

Australian Privacy Foundation

Submission on NOIE Consultation Paper on Control of Spam

September 2002

Introduction

The Australian Privacy Foundation¹ welcomes the opportunity to make a submission on this important issue and congratulates NOIE on a comprehensive issues paper.

Definitions

There is clearly an issue about the definition of Spam, and of other relevant words such as unsolicited, bulk, commercial and marketing. But attempts to definitively resolve this issue can easily get bogged down. There will always be grey areas at the margins, but we suggest that there would be no dispute about the character of the vast majority of the Spam that most of us would recognize as the main problem.

One of the defining characteristics of Spam, in our view, is its bulk character. It would be difficult and contrary to the public interest to seek to limit one-off unsolicited approaches (unless an individual had quite clearly and expressly made potential users aware of this preference). The general approach to Spam control should define the problem as one of organizations speculatively approaching a significant number of individuals in the hope of transacting with them, without any prior indication that the approach will be welcomed. Specifically excluded from the definition should be any concept of prior relationship (Spam from an organisation I have dealt with before is still Spam), although different standards and controls may well be appropriate for 'prior relationship' Spam.

Where there is room for disagreement, definitions should always be resolved in favour of the consumer. For example, when defining Spam, charities should not be allowed to argue that their appeals are a 'special case' and businesses should not be allowed to exclude promotion of new features. We are concerned that in the context of the ACIF SMS Code, telcos are apparently seeking to argue that much of their Spamming is 'service related' and therefore outside the definition of Spam in that Code.

¹ See <http://www.privacy.org.au>

Regulatory overlap

Spam is a good example of a consumer problem that straddles a number of different laws and regulators. It is essential that there is adequate co-operation between relevant authorities to ensure that all resources are brought to bear on the problem and to avoid inconsistent approaches.

We note that the Spam problem is being separately addressed by at least the Federal Privacy Commissioner; the Australian Communications Authority (draft Guideline on Consumer Information by Internet Service Providers (ISPs)); the Australian Communications Industry Forum (various relevant Codes of Practice), and NOIE. We can also see a significant role for the State Fair Trading agencies and the Australian Competition and Consumer Commission (ACCC) in relation to the Trades Practices Act, and note the agreement between the Privacy Commissioner and the ACCC to co-operate on privacy compliance issues.

As an example of the dangers of this regulatory overlap, we note with concern that the ACIF code of practice on unsolicited SMS marketing expressly takes a different view on the effect of National Privacy Principle 2 from the Privacy Commissioner in his NPP Guidelines (see below). The effect of this is to give telecommunications suppliers more freedom to send Spam without express consent than the Commissioner sees as permissible under NPP2. This inconsistency will presumably be ultimately resolved in the courts, but it is very unfortunate that in the meantime different standards are being officially sanctioned.

We are also disappointed that the early pioneering work by the Internet Industry Association (IIA) on a code of practice covering Spam does not appear to have progressed. While a voluntary code may not have been enough, the starting point of allowing Spam only on an opt-in basis was a good one.

We urge all relevant agencies to co-operate to ensure that all resources are brought to bear on the Spam problem and to avoid inconsistent approaches.

Identifying the Spammer

One of the most serious obstacles to effective control of Spam is the frequent inability of the recipient to identify the Spammer. The marketing names used often bear no relationship to any recognized legal entity, and attempts to contact the Spammer by replying either fail or are allegedly used by Spammers to confirm that they have a 'live' address.

We are attracted to a requirement, already included in the ACIF SMS Code of Practice, to include in the Spam message a "Recognised Identifier" - defined in the Code as a symbol or equivalent which enables the recipient to readily contact the Supplier.

In order to make this requirement effective, it would probably need to be an offence to send a message that did not include a genuine, legitimate and operational name and contact details. Spammers that are Australian businesses subject to the Privacy Act 1988 may have to identify themselves to comply with NPP 1.3 or 1.5 (see below) but this would not apply to small businesses that are exempt from the Act, or overseas Spammers.

We suggest that consideration be given to making it a universal requirement for Spammers to include the name of a relevant legal entity and contact details in every Spam message.

We agree with NOIE that there is an issue concerning who should take responsibility for Spam – the person who actually sends the message or the ultimate beneficiary (a business may employ a specialist intermediary to actually send messages on its behalf). We believe the immediate focus of attention should be on the actual message sender, who should not be able to escape responsibility on the grounds that they are merely providing a service. It may however be necessary to deal with both message sender and client to deal with the problem – for instance where the client holds the prospect list and the message sender is only fleetingly in possession of E-mail addresses or telephone numbers.

Spam under the Privacy Act 1988

Most E-mail addresses and telephone numbers are likely to be ‘personal information’, either because the organisation holding them also stores a corresponding name, or because the identity of the individuals concerned can ‘reasonably be ascertained’ from the address or number (in many cases directly where an E-mail address uses all or part of a name, but otherwise indirectly through ‘who-is’ or reverse directory² searches).

Obligations of the Spammer

If the Spamming organization declares direct marketing as a primary purpose for which it collects and holds the addresses (NPP2.1 - likely to be quite common), or if it is a secondary purpose but one which the individual might reasonably expect (NPP2.1(a) - unlikely but depends on circumstances); then there is no requirement for it to offer an opt-out opportunity - this requirement only applies where the marketing is a secondary purpose beyond the reasonable expectation of the individuals concerned, and where seeking consent is impracticable.

The Privacy Commissioner’s final NPP guidelines suggest that on-line marketers should generally find it practicable to seek consent (thereby qualifying under NPP2.1(b)) – and the Commissioner’s advice on consent suggests that at least notice and an opt-out

² While the Telecommunications Act prohibits directory publishers from providing reverse search (number to name) capability, it has proved difficult to stop such products from being available and in any case there is nothing to stop individual businesses from reverse searching their own corporate databases.

opportunity will be required – perhaps not express opt-in consent. In this respect the practical consequences are similar to what would be required under NPP 2.1(c) with the important distinction (we suggest) that the notice and opt-out opportunity would have to be given in advance of the first purposive use, rather than as part of it, as would be allowed under 2.1(c). It would be helpful for the application of the NPP2.1 and its various exceptions to unsolicited direct marketing be clarified.

Even where an organization can justify use of E-mail addresses for SPAM as either a primary purpose or a reasonably expected secondary purpose, they still have obligations under NPP1 to ensure that individuals are notified of intended purpose. This notice can either be by the Spamming organisation (NPP1.3 - if the addresses are collected directly from the individuals) or by some other third party, such as the source of addresses (NPP1.5). Unless the Spamming organisation notifies individuals directly, it must be able to show that it has taken reasonable steps to ensure that the individuals have been notified by someone else. The most obvious ways for a Spamming organization to do this is to contractually require the source to notify or to warrant that it has notified individuals of all the relevant details.

It is not yet clear how detailed the NPP1.3 and 1.5 notices will be required to be, particularly in terms of specifying the form of use, ie: will ‘direct marketing’ be sufficient or will collectors need to distinguish E-mail or SMS Spam from postal or voice telephone marketing? Clear guidance on this from the Privacy Commissioner would be helpful.

Another related issue is the extent to which it is reasonable to rely on notices by an original collector satisfying the NPP 1.5 obligation of a subsequent user. Of particular concern is the ability of such notices to adequately convey the information specified in NPP1.3 (a) and (c), which are very specific. A collector may be able to describe classes of disclosure and broad purposes sufficient to satisfy its own NPP 1.3 obligations, but we suggest that generic descriptions will not necessarily satisfy NPP1.5 – which requires reasonable steps to make individuals aware of the specific identity of the third party indirect collector, and how to contact it. Again, clearer advice from the Privacy Commissioner would be helpful.

Obligations of organizations which are the source of the email address

An organization that is the source of email addresses used for Spam will have independent obligations under the Act as well as, in many cases, contractual obligations to carry out notification imposed on it by Spammers in order for the Spammer to satisfy NPP1.5.

In some cases, the immediate source of email addresses used for Spamming may themselves have obtained them from another source. But there should always be a traceable chain back to an organization that has made the ‘original’ collection. If this was from the individuals concerned, then the collector has the NPP1.3 obligation to notify,

and also an NPP1.2 obligation to collect 'fairly' which will help to prevent 'covert' collection such as from web-sites without clear notice

NPP1.3(d) (and the equivalent notice obligation under NPP 1.5) requires a collecting organization to give the individual information about 'usual' disclosures. A pre-formed intention to disclose email addresses to third parties for Spamming purposes would almost certainly be a 'usual' disclosure requiring notification, no matter how infrequently the addresses are actually disclosed. There will however be no need to name the organizations to which the addresses are disclosed – generic descriptions will suffice and the Commissioner's guidelines give the example description 'list renters' (but see above for the implications of generic descriptions for the subsequent user).

Organisations intending to disclose email addresses for Spamming need to be aware that the NPP 2.1(c) exception is not available for disclosure – only for internal use. This means that E-mail addresses and SMS numbers can only be *disclosed* for marketing use if it is a primary purpose, reasonably expected secondary purpose (2.1(a)), or with consent (2.1(b)).

Publicly available information – E-mail and telephone directories

Much unsolicited telephone marketing draws on the telephone numbers published in directories.

To date, there have been few public directories of either mobile telephone numbers or E-mail addresses. This suggests that most Spam SMS and E-mail makes use of prospect lists derived from other sources – mostly non-public lists compiled from previous transactions.

Since public directories of mobile telephone numbers and E-mail addresses are likely to emerge, it would be sensible to establish some binding principles to ensure that they do not become a source of Spam. There is a very simple solution which publishers of fixed telephone directories have been shamefully reluctant to embrace despite repeated requests from consumer organizations. This is to ask those whose numbers or addresses are to be included to express a preference as to receipt of unsolicited communications, and to indicate this preference in the published directory.

Directory publishers, like individual businesses, should be free to offer as wide a range of options as they like (yes/no to sales Spam; charity appeals, survey research etc), but the default minimum should be no unsolicited approaches of a 'bulk' character at all.

We suggest that publishers of directories of contact details (telephone and fax numbers, postal or e-mail addresses) should be required at a minimum to ascertain the preferences of any individuals included concerning receipt of Spam (however defined), and to indicate this clearly against each entry in the directory. The default indication, in the event of non-response, should be 'No Spam'.

We note that the Privacy Commissioner is currently consulting on the collection and use of publicly available personal information, and his findings will be relevant to your review, although the scope of his proposed information sheet is limited in that it will deal only with the privacy law as it currently stands.

We suggest that the Privacy Commissioner issues more detailed advice on the application of National Privacy Principles 1 and 2 to unsolicited direct marketing, covering obligations of both Spammers and data sources.

Taking action under the Privacy Act or other Australian laws

One of the inherent problems with Spam is that the level of harm or irritation caused by any one Spammer will rarely be sufficient to justify an individual spending the time and effort required to bring a complaint and see it through. And yet the cumulative damage, cost and inconvenience caused by the overall level of Spam is enormous.

This makes it a classic case where action is required by an organization acting on behalf of all recipients. Under the Privacy Act 1988, this could either be a person or organization bringing a representative complaint, or an own-motion investigation by the Privacy Commissioner. Given that the problem is well known and perpetrators relatively easily identified, Spamming would seem to be a potential breach of privacy principles which the Commissioner is best placed to take up without any need for a specific complaint. The only result that an 'own-motion' investigation cannot deliver is compensation, but this is not really an appropriate remedy in any case – a determination could still require the remedial action that is everyone's objective.

We suggest that the federal Privacy Commissioner takes on a pro-active role of identifying suitable test cases of Spamming and initiating own-motion investigations into them.

Spamming from other jurisdictions

Many Spam message originate from overseas. Even if the identity of the spammer can be ascertained, it can be almost impossible for an individual to take any effective action. And even if the Spammer's home jurisdiction has a privacy or other relevant law which affords rights to non-residents, it is beyond the capacity of most individuals (and beyond reasonable expectation) to research the other law, find the appropriate complaints body and sustain the effort required to see the complaint through.

Clearly what is needed is practical collaboration between regulators in different jurisdictions to cross refer complaints or other allegations of Spamming and investigate them without requiring input from the initial complainant. It should not be difficult to establish one or more linked web-sites on which recipients of Spam could lodge details of the unwanted messages, with a clearing house function to sort and assemble common

complaints into a target list of high volume or particularly objectionable Spammers. The web sites could also publish these lists (it would be some comfort for recipients to know that they are not alone!), report on investigations and enforcement action and give advice on anti-spamming measures.

We suggest that Australian regulators co-operate with their counterparts in other jurisdictions to urgently establish clearing houses for complaints about Spam, and enter into reciprocal agreements to investigate complaints about Spammers operating in their respective jurisdictions.

The limits of Self help

Current advice to consumers about how to deal with Spam emphasizes caution in giving out E-mail addresses. While we do not argue with this as a 'motherhood' statement, we have serious doubts about the contribution it can make to dealing with the problem. Suggesting that consumers do not give their e-mail addresses to commercial organizations is as unrealistic as suggesting that they only give their telephone number to family and friends. The reality is that an E-mail address is rapidly becoming as essential a communications tool as a telephone number, and consumers should be entitled to give their address (or number) to businesses for a specific purpose as they define it, without having to be concerned that it might be used for unwelcome marketing either by the business itself or third parties.

The role of ISPs

We support many of the proposals in your paper in relation to action by ISPs including improved security; industry white and black lists; availability of filtering products, advice to customers etc. Some of these activities do however raise important issues of censorship and freedom of speech which need to be addressed. These go beyond the scope of privacy concerns and will no doubt be adequately covered in other submissions.

The main area of concern for the Foundation in relation to the role of ISPs is the suggestion that they need to routinely identify users, and that calling line identification should be used more for this purpose (see draft recommendations 2-4). We do not think that these proposals have been adequately thought through. The paper slips into talking about identification of individuals when we have seen no evidence of large scale Spamming by individuals. Most Spammers are organizations and any proposed monitoring should focus on them. What evidence is there that Spammers are blocking transmission of their CLI (presumably as a way of preserving their anonymity?).

As we understand the law, ISPs, as carriage service providers under the Telecommunications Act, are entitled to CLI from carriers irrespective of any block that the user has placed (either on their line or on specific calls). This is recognized in the ACIF CND Code of Practice, which re-iterates the purposes for which CLI can be provided. These are fraud prevention, billing, call management and credit control of

Internet access services. We do not see that this very specific list of purposes would include identification of Spammers, even if Spamming was unlawful and certainly not if it is merely a nuisance.

We understand that a few years ago, some ISPs were seeking to make it a condition of service that users did not block CLI – presumably to allow them to use it for purposes other than those for which they can obtain it without consent. We are not sure whether this is still being attempted, but would argue that if so it might constitute a breach of the anonymity principle of the Privacy Act (NPP8). NPP 8 should not in our view be interpreted as an ‘all or nothing’ obligation – instead it requires organizations to allow individuals (not businesses) as much anonymity as possible. This means that just because an ISP may be able to ascertain a customer’s CLI for one or more of the four permitted purposes, some of which may involve using the CLI to identify the customer, does not authorize them to identify the customer for the purpose of investigating and taking action in relation to alleged Spamming.

Having said that we think the Privacy Act may currently prevent this use of CLI, we are not averse to a proposal to add control of Spam to the list of permitted purposes, subject to conditions – this would be best achieved by amendment of the Telecommunications Act.

We would not see it as being necessary to authorise routine collection of CLI of all users just in case a Spam investigation is required. Rather we would see it as appropriate to allow CLI to be captured for Spam control purposes on a targeted basis on lines being used to transmit Spam. There may in fact be no need to allow the ISPs to access the CLI for this purpose themselves – it would be preferable for complaints to trigger the recording of CLI but only for provision to a third party investigating body (such as the Privacy Commissioner or an Industry Ombudsman). This model could be similar to the proposal for investigation of nuisance telephone calls suggested by consumer groups in the past, with the aggrieved recipient triggering the recording of CLI for referral to and use by the investigating third party, keeping the ISP out of the loop for that bit of information.

There is of course a current debate about the length of time ISPs should maintain traffic records, both for their own purposes and for law enforcement purposes. To the extent that CLI information is collected and kept by ISPs for all dial up access for these other purposes, it would be potentially available for Spam control. Whether or not an automated complaint system was in place, a separate regime should apply to accessing CLI information for Spam control purposes, with appropriate record-keeping, auditing and reporting requirements.

We suggest that the Review clearly spells out the current position regarding capture of CLI by ISPs, works through the argument for the use of CLI in relation to Spam control, and only then, if it is justified, recommend legislative amendments to allow for that use to the extent required, and subject to safeguards.

We further suggest that consideration be given to a user initiated system of recording CLI for Spam messages, with direct referral of the Spam CLI to the relevant third party investigative body.

End.

*Australian Privacy Foundation
C/- Law Faculty
Room 1212 Mathews Building
University of NSW 2052
t. 02 9385 1208
f. 02 9385 1778
For e-mail contact see covering e-mail*