University of Auckland Business Review

By Alexandra Sims and
Gehan Gunasekara

Privacy and the Spam Act in online competitions

Online competitions are a cheap and useful tool for businesses to gain information about potential customers. Organisations using online competitions, however, must comply with a number of legal requirements; two such requirements are the Privacy Act 1993 and the Unsolicited Electronic Messages Act 2007 (the Spam Act). In a study conducted in 2009, 40 competitions were analysed for their compliance with these Acts. The results of the study demonstrate considerable non-compliance as well as some misunderstanding of the requirements of these Acts. This article, in addition to explaining the law, provides best practice guidelines for organisations running such competitions.

Online competitions can be a valuable source of information. They operate as a low cost promotional activity; provide the names and contact details of people that are interested in an organisation's products; and the data collected can be used to build up profiles of an organisation's target market. Online competitions are attractive for organisations ranging from multinationals through to small businesses because they:

- Are cheap and easy to set up, there are no printing and distribution costs;
- Have no data entry costs, the entrant has done all the work by filling out the online form; and
- There is a negligible cost to entrants; there is no need to purchase a stamp so entrants are more likely to enter a competition.

As with all business activities, however, there are laws that affect online competitions. Two such laws are the Privacy Act 1993 and the Unsolicited Electronic Messages Act 2007 (the Spam Act)[1].

While media portrayal of the Privacy Act 1993 has had a bad press over the years, consumers are concerned about privacy. A 2006 UMR Report commissioned by the Privacy Commissioner found that 57 percent of surveyed people were concerned about individual privacy and 27 percent stated they were very concerned, compared to just seven percent who were not concerned at all with their privacy[2]. Brands can be damaged through what may be rightly seen by consumers as a lack of concern over consumers' privacy and the receipt of unwanted emails. Moreover, consumers are no longer likely to keep their annoyance to themselves; nowadays they are more likely to vent their anger in public on the internet through blogs and other forums.

It is also important to appreciate that many of our trading partners have privacy laws that are similar to and in some cases stricter than the requirements of the Privacy Act. This is of concern in a globalised business environment as personal information is increasingly transferable between countries, whether through outsourcing, web-based business or the mobility of individuals[3]. Although the United States has adopted sector-specific rather than over-arching information privacy laws (preferring to negotiate compromises with other trading blocs such as the "Safe Harbor", which allows United States companies to trade in and collect personal information about citizens of the European Union without potentially contravening the strict privacy rules that operate there)[4] information privacy rules across the world are based on internationally-recognised standards, are oriented around a few basic principles, and are therefore remarkably consistent[5]. Complying with the rules in New Zealand will therefore ensure that a business' global reach is enhanced as New Zealand's law is generally regarded as compliant with the trend-setting European Union standard[6].

More broadly, concerns over privacy may slow the general uptake of the internet economy. As a recent Australian Government consultation paper has noted, government can "promote

consumer digital confidence by setting a regulatory framework that encourages businesses to adopt practices that respect user privacy and security"[7].

In addition to brand damage through inappropriate treatment of privacy and email addresses, a breach of the Spam Act can result in large fines (the maximum pecuniary penalty payable to the Crown is $200,000 for individuals and $500,000 for organisations)[8] and non-compliance with the Privacy Act can result in the Privacy Commissioner investigating a complaint[9], which includes inspecting internal documents and interviewing staff. After the Privacy Commissioner's investigation the matter may be heard by the Human Rights Review Tribunal, which has the power to award substantial damages for breaches of privacy[10].

The practical difficulty with the Privacy Act and the Spam Act is that while they both affect online competitions, the two do not complement each other: their underlying rationales are different. The Privacy Act is permissive and as we shall see, not well understood, as it seemingly has few concrete requirements. In contrast, the Spam Act is prescriptive: organisations must gain consent from contestants before they can send emails promoting their products. Partly as a consequence of this divergence, many more issues need to be addressed in relation to the Privacy Act than arise under the Spam Act and this is reflected in the relative attention given them in the discussion that follows.

In the summer of 2009, we conducted a survey to see how well competitions adhered to the requirements of the Privacy Act and the Spam Act. Few of the surveyed competitions met the minimum requirements and of those that did, improvements can be made. The results of our survey are presented in this paper.

The aim of this paper is twofold. First, it explains the requirements of the Privacy Act and those of the Spam Act as they relate to online competitions; this is necessary as there is some confusion over the Acts' requirements. Second, it provides provide best practice guidelines for the operation of online competitions. A well designed competition does not take any longer to develop than a poorly designed one.

Methodology

We analysed 40 online competitions that were promoted to New Zealand residents. The competitions were selected purely at random during December 2008 and early January 2009 (the first 40 competitions that we found that were current at the time the research was conducted and for which no purchase of goods or services was required as a pre-requisite). The organisations offering the competitions were private sector companies and represented a cross-section of companies ranging from multinationals through to SMEs. The competitions were analysed to see how well they complied with privacy principles 3 and 11 of the Privacy Act 1993 and the requirements of the Unsolicited Electronic Messages Act 2007 (the Spam Act).

The Privacy Act 1993

The online competitions in our sample required contestants to provide at a minimum their names and contact details (although, as will be seen, further information such as contact details of contestants' friends were sometimes also sought). Such information is personal information under the Privacy Act[11]. The collector of the personal information must inform contestants of a number of things (the actual mechanisms for informing contestants are dealt with under the privacy policy section):

Under privacy principle 3 of the Privacy Act, contestants must be informed:

(a) That the information is being collected;

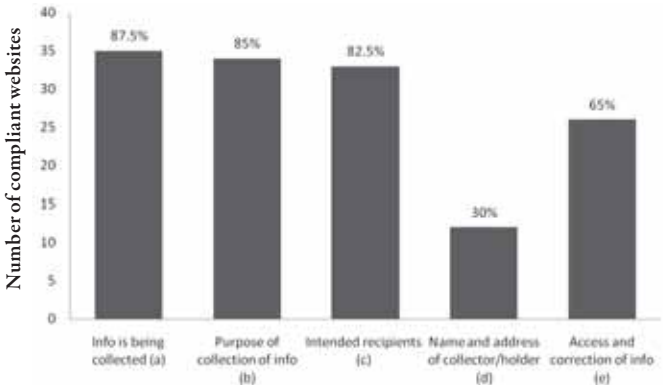
(b) Of the purpose for which the information is being collected (for example, if the organisation wishes to keep the information after the competition has closed and/or if the organisation wishes to send the contestant information about their products at a later date, the contestant must informed about this);

(c) Of the intended recipients of the information;

(d) Of the names and addresses of who is collecting the information and who is holding the information (the collector and holder may not be the same person);

(e) That the contestant has the right to access the information and to correct the information (or if no correction is made then to attach a statement to the information about the requested changes).

As the graph below demonstrates, not all the minimum requirements are being met.



Privacy Act 1993 minimum requirements

It can be observed that there was an extremely low degree of compliance with paragraph (d) of principle 3 and only just over half of the competitions surveyed informed entrants of their right to access and correct information (paragraph (e)). It may be thought unnecessary, in the context of an online competition, to advise entrants of this right but the rights conferred by the Privacy Act may be relevant where say an individual subsequently changes their address or perhaps mistakenly enters a competition.

Furthermore, even though there was on the whole substantial compliance with paragraphs (a) to (c) of principle 3, this is due to a somewhat generous reading of many of the privacy statements that we surveyed. Many were worded in all-encompassing terms, were difficult to find or simply lacked clarity. In this regard one should pay heed to the warning given by New Zealand's first Privacy Commissioner, Bruce Slane[12]:

"I have seen too many purported privacy statements in small print, containing all-encompassing weasel words. These

statements do not fool people but act as a beacon that flashes 'this business has something to hide', even where the business has merely acted on cautious advice."

In addition, some confusion exists as to the requirements of the Act itself. There is a perception that if the collecting agency tells people what it will do with the information, the collecting agency can do what they wish with it. For example, it has been stated that if an organisation wishes to sell, license or give information to unidentified third parties it can do so if it states that "other related organisations may wish to send you relevant marketing information from time to time"[13]. However, with respect, such an interpretation is overly simplistic and is we believe fraught with danger. This is because the Privacy Act contains two inter-connected principles that apply when information is collected.

The first is principle 3, the requirements of which are set out above. This relates to the information that must be made known to the individual whose information is being collected and is quite specific. Vague reference to communicating the details to unidentified third parties for marketing or other purposes does not provide information about the intended recipients as those recipients could be anyone, thus it does not comply with the Act.

Secondly, under privacy principle 11 an organisation, once it holds information about an individual, must not disclose it to anyone else unless one of a number of exceptions applies. The most important exception is where "disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained". It is certainly arguable that reference to communicating information with "other related organisations" in order that they can send the individual marketing information from time to time meets this requirement. However, despite this, we maintain that best practice (see below) is where the recipients of the information cannot be identified with some specificity to request individuals check a box assenting to their customer information being provided to third parties. This is preferable to the practice of asking individuals who do not wish their information to be shared to indicate such preference.

Best practice aside, we maintain that in order to meet the legal requirements of the two relevant privacy principles contained in the Act an organisation should, before passing on information to others, either obtain the contestant's consent (see consent section) or clearly identify the recipients at the outset.

Best practice:

In addition to what the contestant must be told in (a) to (e) on the previous page, there are additional factors which we believe constitute best practice:

- If information is to be sent to third parties who are unidentified request that contestants assent to this by checking a box in the short form privacy policy (see the privacy policy section);
- Organisations are required to have a privacy officer. Contact details for a privacy officer should be provided; and
- If the privacy policy states that the organisation may send promotional material and other advertising to the contestant via snail mail, then organisations should offer contestants the ability to opt out of receiving subsequent advertising from that organisation. That can be done by including a tick box with the wording, "I do not wish to receive any further information about [insert company's name] products."

We have seen the bare minimum of what contestants need to be told under the Privacy Act and we have outlined what additional features constitute best practice, the question now is how the information is communicated to the contestants.

The privacy policy

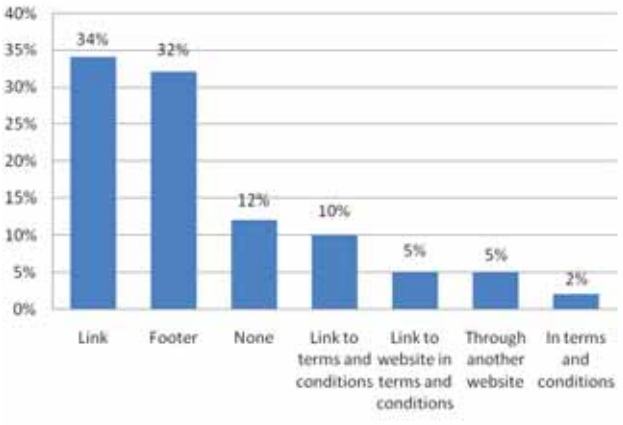
The usual way to inform contestants of the information which is required under the Privacy Act is through a privacy policy or statement, albeit as we shall see below, 12 percent of competitions failed to make any statement about privacy. The lack of a privacy policy or statement in these competitions is of extreme concern and amounts to a clear breach of the Privacy Act.

On the other hand, the fact that 88 percent of websites surveyed did have some type of privacy notice is encouraging and marks an advance from previous surveys. For instance a survey conducted in 2006 by the Privacy Commissioner's Office of 50 public and 50 private sector websites chosen from the largest employers listed in the online Kompass database[14] found that overall only 56 percent had a notice of some type relating to privacy, and of the 50 private sector websites 52 percent had no privacy notice of any kind.[15] Indeed, although a quarter of both public and private sector websites had means for job applicants to apply online – thus collecting personal information – only 58 percent in each case had a privacy notice[16].

However, in the case of our survey the legal position for online competitions is unambiguous; whereas there is no requirement that websites generally must contain a privacy statement, when personal information is collected through them (as is the case with online competitions) the requirements of the Privacy Act must be met. It is difficult to see how they can be in the absence of a privacy notice.

Of those organisations in our survey which did use privacy policies nearly half (48 percent) had specific policies for competitions, while the remainder had general privacy policies. Of the organisations which did mention privacy, contestants were informed of the privacy factors in a variety of ways:

- A privacy policy was embedded as a direct link on the competition form;
- A link to a privacy policy was included on the footer of the competition page, but it was the general privacy policy for the website and may or may not be directly for that competition;
- A privacy statement was included in the terms and conditions of the competition;
- A privacy policy governed the competition but it was found on another website;
- Link to privacy policy in the terms and conditions.



Location (if any) of privacy policy/statement

Other ways are possible for communicating the privacy policy, for example, a privacy policy could be included on the page of the competition, so that the contestant could read the policy without navigating away from the page. Alternatively organisations can use what is called a layered privacy statement.

Layered privacy statements

In a layered privacy statement the key parts of the privacy statement are contained on the competition page, with a link through to the full privacy policy. A key part of a privacy statement would be any unusual terms, for example, that the organisation collecting the information may pass on that information to unknown third parties or that information that was being collected was being held on a server located overseas. At the minimum, the competition page ought to provide a link to the condensed privacy notice or "privacy notice highlights" page (this is discussed below).

Increasingly, layered privacy statements are the method preferred by privacy authorities in New Zealand[17] and overseas. Experts and privacy authorities worldwide have found that current privacy notices are less than successful, being so long and complex that individuals are no wiser by reading them.[18] The OECD Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy has issued a report highlighting that a privacy notice is an obvious way to disclose an organisation's privacy policy and practices and that "short, simple, and understandable privacy notices are a useful addition to a complete notice, and better enable individuals to make informed decisions about their personal information"[19].

A layered notice may have two or three layers: the first layer can be very short providing only the identity of the data controller and contact details, layer two being a condensed notice covering no more than a page and including subheadings dealing with the purposes of information collection, its use and sharing and rights to access the information as well as how to contact the agency. Where there are only two layers, the competition page should contain a link to the full privacy notice.

The third layer should contain the full notice and this should cover all the agency's practices and policies regarding the handling of personal information, including those relating to the competition. It is common to include advice and assistance concerning cookies and so forth. This notice should also contain references to any relevant legislation (for example in some countries different statutes and rules apply depending on whether the agency collecting the information is in the public or private sector). In addition, any specific legislation that applies, such as that relating to the privacy of children[20], can be referred to in this third layer notice.

Furthermore, both international agencies and private sector agencies have formulated freely downloadable step-by-step guides and privacy statement generators to assist organisations to develop privacy statements.[21] These resources, however, cannot and should not be a substitute for coherent and pre-determined information handling practices within organisations. Privacy statements, layered or otherwise, will only work and be compliant where they reflect the actual practices within the organisation and staff and management receive proper training regarding them.

Providing a layered privacy notice then should not be an overly burdensome exercise. As the Australian Law reform Commission has stated, "the oft-repeated slogan...'privacy is good business' – that is, consumer trust is a *sine qua non* of engagement with such services as e-commerce and internet banking"[22]. We would go even further and say the uptake of online competitions and the like would be greatly enhanced if entrants have the security of reading a (brief) privacy statement on the competition page itself, with a link to the organisation's full privacy statement. If specific practices are intended with regard to the information gathered about competition entrants then this should either be highlighted in the condensed notice (layer 2) or there should be direct link from the competition page through to the relevant portion of the full notice which deals with competitions.

By contrast, including the privacy policy in the terms and conditions is not best practice. It signals to contestants (an organisation's current or potential customers) that the organisation is not interested about privacy and is more interested in limiting its liability.

Lastly, drawing up a full privacy notice is not itself difficult: as we have seen there are many tools to facilitate this. It should be noted that where an organisation primarily or solely conducts business within New Zealand the requirements of the Privacy Act are far simpler than the rules that operate in overseas jurisdictions. For example, we do not have to contend with overlapping federal and state legislation, as occurs in Australia; the same rules apply to public and private sector organisations and unlike in Australia the Privacy Act in New Zealand does not exempt categories of personal information, such as that relating to "small business operators" or "employment records".[23] Thus the twelve information privacy principles (IPPs)[24] apply to practically all organisations in New Zealand and contain broad principles relating to the collection, use and disposal of personal information. It should be relatively straightforward to incorporate them within an organisation's privacy statement.

Best practice:

Hiding privacy statements in terms and conditions is not advised. The optimal way is to:

- Have a specific privacy policy for competitions; and
- Use a layered privacy policy on the page of the competition.

Consent

Some organisations (five percent) saw it as desirable for contestants to signal their acceptance of the privacy policy. In general, the Privacy Act does not require that contestants positively accept or assent to the terms of an organisation's privacy policy, its main emphasis being that contestants have been informed as to the uses to which their information will be put. However the Privacy Act does require specific consent from the individual if the organisation wishes to act in certain ways: these include collecting personal information from someone other than the data subject (principle 2(2)(b)), the notification requirements when collecting information (principle 3(4)(a) – relevant if for example an individual joins an organisation or a competition on an ongoing basis where it is practicable to dispense with the notification requirements for each subsequent entry) and where the collector wishes to use the information for purposes other than that for which it was obtained (principle 10 (b)).

Thus consent is imperative if an organisation intends to pass on the personal information which it has gathered to third parties which it cannot name at the time of the competition. Consent can be gained in various ways. The best way is to include a tick box on the competition page stating "I understand that my personal information may be passed onto reputable third parties who we do business with". Alternatively, there could be a statement in the privacy policy that information will be passed onto third parties and the contestant is asked to tick a box stating that they agree to the terms of the privacy policy. However, for the latter to qualify as consent, the privacy policy would need to be included at a minimum in a link next to the tick box.

Other Privacy Act breaches

The primary focus of our investigation into compliance with the Privacy Act hinged on the degree to which privacy notices were transparent regarding their use and disclosure of information: we did not, for instance, concentrate on other Privacy Act requirements such as the need to keep personal information secure (privacy principle 5) and the requirement that personal information not be kept for longer than is required for the purposes for which it is to be used (privacy principle 9). This is because compliance or non-compliance with them could not reasonably be ascertained solely by reference to the privacy policies we surveyed.

Despite this limitation of what could be analysed, the survey of the competitions did raise the very real possibility that breaches of these principles may be taking place. In the first instance, not a single privacy notice advised contestants of the length of time that the information supplied would be held; for example, whether it would be retained beyond the duration of the competition itself. There is, of course, no requirement to advise contestants thus and a well-drafted privacy notice is as we have seen likely to be specific as to the intended uses for the information.

More disturbingly, however, we discovered that several companies (16 percent in our survey) were using competitions not only to gather information about contestants but also to obtain personal information about their friends (asking for instance for their names, email and phone numbers). The practice of obtaining information about contestants' friends amounts to a clear breach of privacy principle 2 which stipulates that where personal information is collected about an individual it must be collected directly from the individual concerned. Although a number of exceptions apply (including where the individual has consented to information being collected from someone else) none are relevant here; it cannot be argued that compliance is not reasonably practicable since it is possible to have contestants forward a link to the competition to their friends instead.

Furthermore, 16 percent of the privacy policies included in the survey stated that they may collect information about contestants from third parties, again violating privacy principle 2. It could, no doubt, be argued that contestants had agreed to this (see the consent section) but as we have seen, only five percent of those in our survey included the practice of having contestants signify acceptance of the privacy policy. Unless this was indicated in the privacy highlights of the layered privacy notice or attention was specifically drawn to it, we think that the purported consent is not a valid defence in these circumstances. Although modern information technology allows businesses to cross-check personal information with that held by other companies to build up customer profiles, mine information and perhaps even engage in predictive behavioural modelling of potential customers, such practices if engaged in are likely to fall foul of the Privacy Act.

The Spam Act

One purpose of many online competitions is to gain contact details of potential customers. If an email (apart from one notifying the contestant that they are a winner of the competition and emails associated with delivery of the prize) is sent to a contestant that promotes or acts as advertising for the goods or services of an organisation, that email will be caught by the Spam Act. To avoid breaching the Spam Act the organisation must obtain consent from the contestant[25]. Thus the Spam Act is the opposite of the Privacy Act as the Privacy Act does not require consent (apart from the specific instances we have highlighted earlier). Therefore, complying with the minimum standards of the Privacy Act will not in itself be sufficient to comply with the Spam Act.

For the purposes of online competitions, consent can be express or implied. Express consent is simply defined as "express consent, whether given by the relevant electronic address-holder or any other person who uses the relevant electronic address"[26]. Inferred consent is "consent that can reasonably be inferred from...the conduct and the business and other relationships of the persons concerned"[27]. Entering a competition by itself does not amount to inferred consent.

Express consent can be gained easily by including a line of text near the "submit" or "enter" box which can be ticked. That box should contain wording along the lines of "I would like to receive emails updating me on products and services offered by [insert name of organisation]". Of the surveyed competitions, 52 percent contained similar wording with an accompanying tick box and thus would have gained express consent.

Of concern were those competitions that did not have a box which could be ticked. Three explanations are possible. First, it may be that organisations believe consent has been obtained, because in the privacy policy or in the terms and conditions there is a statement that the company may from time to time

contact the contestant, and that the contestant agreeing to the terms and conditions by ticking a box which says "I agree to the terms and conditions" and/or "I agree to the privacy policy" constitutes consent to the receipt of emails. Secondly, there may be a statement in the privacy policy that emails may be sent to the contestant advising them of new products and promotions of the organisation. Thirdly, in the absence of any statement about the sending or contacting at a later date, organisations may argue that a person merely by entering the competition and providing their email address is consenting to the sending of emails to them about that organisation's products at a later date.

Although the point has not yet been tested in court, practices short of including a specific tick box consenting to the receiving of emails are risky. There is a good chance that such tactics will not constitute consent and organisations should avoid the practice. For example, while the second explanation above may meet the requirements of the Privacy Act, the Spam Act's requirements are higher. Moreover, if the contestant's details were passed onto an unknown third party and that third party began to email the contestant, it is difficult to see how consent could have been given to this unless a box had been ticked stating that the contestant wished for that organisation and others to which the information had been passed on to send emails to the contestant.

Conclusion

Some organisations go to great lengths in their construction of online competitions and adopt many features which we identify as best practice. However, for every organisation that is doing well, there are many who are not and who risk breaching the law. The poorly performing organisations are damaging not just their own reputations, but online competitions and consumer confidence in the internet economy in general.

Online competitions have operated below the radar, but given their increased use and in the light of our findings it is hoped that more attention will be paid by the public and by the authorities to issues of privacy and spam created by such competitions. Members of the public are entitled to, and should, complain to the Privacy Commissioner[28] when online competitions fail to meet the requirements of the Privacy Act. There is a regulatory framework and it should be policed to ensure that consumer confidence in the internet economy is enhanced rather than damaged.

Best practice checklist for online competitions:

- Privacy policy has been designed for competitions;
- Privacy policy is not contained in the terms and conditions of the competition;
- Information required by privacy principle 3 is provided;
- Personal information is not sold, licensed or given to third parties (but, if wish to pass on information to third parties, then tick box asking contestant's permission to do this is provided on the competition page);
- Layered privacy policy with key terms on the page of the competition with link on the competition page to the full privacy policy;
- Do not ask for information about individuals who are not contestants and if it is intended to obtain information about contestants from third parties clearly signpost this in the privacy policy;
- Privacy officer's contact details are provided;
- If you wish to contact contestants by email in the future, provide a tick box on competition page which states "I would like to obtain information via email about [insert company's name] products in the future"; and
- Be honest and sincere – some organisations claimed they valued the contestant's privacy, but then went on to state in the fine print that personal information may be sold or licensed to third parties. If companies really did value privacy, they would not be passing personal information on to third parties, so leave out platitudes to privacy if there is no intention to respect it.

References

1 Other laws are, for example, the Fair Trading Act 1986: competitions cannot be misleading or deceptive.

2 Privacy Survey 2006 (http://www.privacy.org.nz/assets/Files/24153322.pdf).

3 See generally Gunasekara, G. N. (2007). The "Final" Privacy Frontier? Regulating Trans-Border Data Flows, *International Journal of Law and Information Technology,* 15(3), 362-393.

4 United States Department of Commerce, *Issuance of Safe Harbor Principles and Transmission to European Commission,* 65 Fed Reg 45666 (2000).

5 Most rules originate from the Organisation for Economic Development and Co-operation (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980 (www.oecd.org).

6 *Necessary and Desirable: Privacy Act 1993 Review, Report of the Privacy Commissioner on the First Periodic Review of the Operation of the Privacy Act* 1998, at p. 9.

7 Digital Economy Future Directions, Consultation Paper (Australia Government, Department of Broadband, Communications and the Digital Economy, Draft 18 December 2008) (http://www.dbcde.gov.au/__data/assets/word_doc/0005/94190/Consultation_Draft_-_DEFDP_-_17_Dec_2008_final.doc).

8 See s45(3) and (4) of the Unsolicited Electronic Messages Act 2007 .

9 Privacy Act 1993, s 66 – 69.

10 Privacy Act 1993, s82 – 85 and 88; see Gunasekara, G. N. and Dillon, E (2008). Data Protection Litigation in New Zealand: Processes and Outcomes. *Victoria University of Wellington Law Review,* 39(4), 457-486.

11 Personal information is defined as any information about an identifiable individual, see Privacy Act 1993, s 2.

12 "Privacy protection: A Key To Electronic Commerce" Address by Privacy Commissioner, Bruce Slane, New Zealand Law Conference, Rotorua, 9 April 1999 (http://www.privacy.org.nz/privacy-protection-a-key-to-electronic-commerce/?highlight=fai).

13 See (2008) *Sales and Marketing Law*. Auckland: CCH, p.262.

14 Business Profiles of New Zealand's Top 100 Companies (http://www.kompass.co.nz/business-profiles/nz_top_100.php)

15 Privacy Commissioner, *New Zealand Website Privacy Notices: a first look,* March 2006 (http://www.privacy.org.nz/assets/Files/96683381.pdf).

16 Ibid.

17 See http://www.privacy.org.nz/effective-website-privacy-notices.

18 The Center for Information Policy Leadership *Multi-Layered Notices Explained: A White Paper prepared for the APEC Data Privacy Subgroup,* Seoul, Korea, 23-24 February 2005 (http://aimp.apec.org/Documents/2005/ECSG/DPM1/05_ecsg_dpm1_003.pdf).

19 The Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy *Making Privacy Notices Simple: An OECD Report and Recommendations,* 24 July 2006 (http://appli1.oecd.org/olis/2006doc.nsf/43bb6130e5e86e5fc12569fa005d004c/a56f6b2f04871d3fc12571b5003dac3f/$FILE/JT03212212.pdf)

20 For instance in the United States see the Children's Online Privacy Protection Act of 1998, Pub. L. no. 106-170, 15 U.S.C. §§ 6501-6506 restricts the use of information obtained from children under 13 by Internet web sites.

21 See, for instance, the OECD Privacy Statement Generator (http://www.oecd.org/document/39/0,2340,en_2649_34255_28863271_1_1_1_1,00.html) and The Center for Information Policy Leadership *Ten steps to develop a multilayered privacy notice,* (http://www.hunton.com/files/tbl_s47Details percent5CFileUpload265 percent5C1405 percent5CTen_Steps_whitepaper.pdf)

22 *Australian Privacy Law and Practice,* Report 108, Vol. 1, May, 2008, 152.

23 Privacy Act (Cth) 1988, ss 6 C and 7 B (3) respectively.

24 Privacy Act 1993, s 6.

25 In addition, when consent has been obtained and an email is sent, that email must contain accurate sender information and a functional unsubscribe facility: ss 10 and 11 of the Unsolicited Electronic Messages Act 2007.

26 Ibid, s (4)(1)(a)(i).

27 Ibid, s 4(1)(a)(ii).

28 See http://www.privacy.org.nz/introduction-to-complaints.