the communications council

ONLINE PRIVACY GUIDELINES

November 2007

MEMBER GUIDELINE

The Communications Council recommends members refer to the Australian Direct Marketing Association's (ADMA) Code of Practice for guidelines on privacy issues - www.adma.com.au

INTRODUCTION

Why online privacy guidelines from The Communications Council? Long gone are the days when agencies and their clients relied solely on broadcast, one-way, push media. Digital media means interactivity and one-to-one communications whether we're advertising and communicating on the Internet, wireless devices or interactive TV. As advertisers we're now dealing with two-way communications and consequently data collection which opens up the world of privacy. Around the world, online privacy is a highly topical and important issue. The debate over government regulation of online privacy is rapidly evolving from a question of 'whether' to a question of 'when'. A rash of privacy bills have been introduced and some have even been passed in Europe, Asia and North America but there is no single global standard. The Communications Council online privacy guidelines are in accordance with the Australian Privacy Amendment Bill. This Bill provides National Privacy Principles and is considered a light-touch privacy bill. Importantly it allows (and encourages) industries to draw up their own privacy's codes to address their specific industry's privacy considerations. The Communications Council online privacy guidelines are provided to members to provide guidance on this important issue. As well as, to assist in the development of business-wide actions towards an environment of industry regulation, trust between advertisers and consumers, and to foster the protection of consumer's privacy.

What do these guidelines cover?

- Adopting and communicating a privacy policy covering the collection and use practices regarding personally identifiable information (data used to identify, contact, or locate a person).
- Giving users choice and consent over how their information is used and shared.
- Giving users access to their personally identifiable information and the ability to update it, remedy any inaccuracies or withdraw the permission to use it all together.
- Putting data security, quality, and access measures in place to safeguard, update, and correct personally identifiable information.
- Responsible use of marketing communications via email and other personal messaging devices ie. Mobile phones, pagers, PDAs.
- Compliance with international laws and principles when involved with trans-border data flows.
- Responsible interactive marketing to children.

How and when to use these guidelines?

These guidelines are provided as guidance and as a checklist for the development of any and all interactive advertising campaigns, customer relationship marketing campaigns and for web sites.

The Guiding Principles Behind These Guidelines

Never before have consumers been empowered with more information, choice and alternative

sales channels, changing forever their expectations of brands, the purchase experience and customer service. The Internet provides the ability to deliver on consumer's expectations of a highly relevant and personal brand and shopping experience. At the same times, the tools that make this all possible also raise serious concerns for consumers about their privacy.

To be successful in the interactive marketplace advertisers must build trust with consumers. The Communications Council fundamentally believes that 'consumer privacy is a right and not a privilege' and that consumers should not have to work to protect their privacy, but rather marketers should have to work to earn their trust and seek permission to use these new tools to develop more personalised and ultimately one-to-one relationships.

The Guidelines

1. Adopting and Communicating a Privacy Policy

a. Friendly, easy to understand language, clearly explain how the information tracking and capturing technology you employ works. Even your privacy policy is the voice of the brand.

b. The privacy policy must state clearly:

I. What information is being collected and all of the methods of how this information is collected. For example, via a registration process, via a purchase, entry in a sweepstakes/contest or a feedback form or click stream information.

II. The full details and contacts details of the organisation collecting the information and whom to contact within the organisation with privacy related questions or concerns.

III. How the information is used or may be used in the future

IV. With whom the information may be shared. And whether there is a law requiring that the information be collected. For example, third-party distribution. In the event information is being disclosed to third parties, the policy should make reference to what information is disclosed, why this disclosure takes place, and the relationship of the organisation to the third party.

V. What choices are available to the consumer regarding identification, collection, use and distribution of the information and how to exercise these choices. And what consequences, if any, of an individual's refusal to provide information.

VI. How consumers can access the personally identifiable information they have actively given to you and how they can correct any inaccuracies or withdraw permission to use the information all together.

VII. How consumers will be informed of any future changes in the privacy policy.

VIII. The kind of security procedures that are in place to protect the loss, misuse or alteration of information and what steps the organisation takes to ensure data quality and access.

IX. A statement of the organisation's commitment to data security.

X. What accountability mechanisms the organisation uses. For example, measures such as internal or external reviews, or privacy audits that the organisation takes to assure compliance with their privacy policy.

XI. All sites using a third party ad server provide information regarding the privacy policy and practices of that third party ad server. This should be done via a link to the ad server company's privacy policy.

c. Communicating your privacy policy.
Post privacy policies prior to the collection of personal identifiable information, as well as ensuring policies are provided to users at the time of collection of such information.

d. A prominent link on your home page or main ad and on any form, page or device that collects personal identifiable information. This link clicks through to the detailed privacy policy.
e. In addition, a link to the Privacy Statement should be referenced as a link in the web site footer throughout the web site.

f. An organisation must provide notification of when their privacy policy was last amended by posting an "as of" date at the top of the policy to reflect the last time it was changed.

2. Giving Users Choice and Consent Over How their Information is Used and Shared

a. Use opt-out for personally identifiable information to be used for marketing purposes within the 'environment' in which it is captured ie. the web site, iTV ad, the WAP mobile phone/PDA

b. Use opt-in for personally identified information to be used for marketing purposes beyond the 'marketing environment' in which it was captured ie. information captured on a web site and then used in an email or to a WAP mobile phone/PDA or to a third party requires opt-in.

c. Use opt-out for click stream data to be linked to personally identifiable information that has been captured and will be used within the same 'marketing environment'.
Cookies and Log Files

d. The organisation's privacy policy should make reference to the use of technologies such as cookies and log files, and explicitly state what this technology is, what information it collects and how this information is used by the organisation. The policy should also provide site users with guidance on how they can opt-out of the use of this technology.

e. Users should be made aware they can opt-out of a site linking click stream data with an individual's personally identifiable information. The organisation should take steps to educate site visitors about how and why they can opt-out.

3. Giving Users Access to their Personally Identifiable Information

a. Organisations should take responsible steps to provide users with the appropriate processes or mechanisms to access personally identifiable information they have provided to the organisation in order to correct inaccuracies in material information, such as account or contact information. In addition, these processes and mechanisms should be simple and easy to use, and provide assurance that inaccuracies have been corrected. These processes should be documented in the privacy policy.

b. Organisations must not adopt commonwealth assigned identifiers.

4. Putting Data Security and Quality, and Access Measures in Place

a. An organisation must take reasonable steps to put data security and quality, and access measures in place to safeguard, update, and correct personally identifiable information.

b. An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

5. Responsible Use of Marketing Communications via Email and Other Personal Messaging Devises

a. Responsible use of marketing communications via email and other personal messaging devises ie. Mobile phones, pagers, PDAs involves:

I. Only use opt-in 'lists'

II. Provide the opportunity to easily opt-out in every communication

III. Either full company details and contact information or a link to these details

IV. Marketing communications should be identified in a way that allows recipients to readily recognise them as marketing messages/solicitations

6. Trans-border Data Flows

a. Any organisation involved in the flow of personally identifiable information should attempt to ensure that the recipient country has privacy laws similar to the Australian National Privacy Principles.

b. Any organisation involved in the flow of personally identifiable information (PII. with European-based countries should attempt to ensure they are in compliance with the European Union's privacy laws. See www.cdt.org/privacy/eudirective for details.

c. Any organisation that provides personally identifiable information to third parties must verify that the third party is governed by the European Directive.

7. Responsible Interactive Marketing to Children

We recommend that advertisers ensure that children obtain their parents' permission before they give any information about themselves or their family while on-line. This information includes personally identifiable data, ie address, phone number, parents' jobs and working hours, credit card details.

a. For children under 14 years of age

I. Where the personal information collected would enable someone to contact a child offline, the advertiser obtain prior parental consent, regardless of the intended use of the information.

II. Where the personal information is publicly posted or disclosed to third parties,

the advertiser obtain prior parental consent.

III. Where collection of an email address is necessary for a child's participation at a site, such as to notify contest winners, the advertiser must provide notice to parents and an opportunity to remove the email address from the site's database.

b. For children above 14 years of age

I. Web sites provide parents with notice of the collection of such information and an opportunity to remove the information from the site's database.

II. Advertisers obtain permission from the child or parents before releasing information to a third party.

III. Advertisers disclose why this information is being requested. Advertisers indicate what use is being made of the collected information; how it is stored, whether the information is intended to be shared, sold or distributed outside of the collecting advertiser company.

IV. Advertisers disclose if the information required is optional in language children can understand, eg "You don't have to answer to play the game".

V. Email addresses are solicited on secure sites only. Recipients are given the opportunity to discontinue mailing by return email. If a secure site is not yet available, advertiser to make reasonable effort, in light of the latest available technology, to ensure that parental permission is obtained.

VI. Advertisers who communicate with children through email remind and encourage parents to check and monitor their children's use of email and other on-line activities regularly.

VII. If a site offers the opportunity to order or purchase a product or service, either through a 'click here to order button' or other on-screen means, the ordering instructions to clearly and prominently state that a child must have a parent's permission to order. XI. Advertisers install a clear mechanism allowing the child or parent to cancel the order.

VIII. Advertisers give recipients the opportunity to discontinue mailings by return email.

Definitions

Opt-in requires a consumer to actively provide consent for a particular action to occur. For example, "tick here to receive our monthly enewsletter". Note: pre-ticked boxes are not opt-in.

Opt-out requires a consumer to actively request that a particular action not occur. For example, "tick here if you do not want this web site to use data collected from your surfing habits on this site to be used to provide a more personal web site experience". Marketing Environment is the place where the information capture (overt or covert. took place, for example, a specific web site, a mobile phone, an interactive TV ad or kiosk etc. Actively provided information is information a users has overtly provided to a company by filling in shopping form, voting in a poll, enrolling as a member, entering a contest etc.

Other

a. These guidelines are not intended to apply to proprietary, publicly available or public record information, nor to supersede obligations imposed by statute, regulation or legal process.

b. Complaints should be directed to the Federal Privacy Commissioner:

GPO Box 5218
Sydney NSW 2001

Privacy Hotline 1300 363 992
privacy@privacy.gov.au

Please also refer to the National Privacy Principles:
www.privacy.gov.au/publications/npps01.html