

Annual Report 2001/2002

January 2002

Contents

1. President's Report "Issues for 2002" (by Sandra Davey)
 2. Annual report - Year 2001 (by Lynne Spender)
 3. Privacy - Resources for Members (by Matthew Hall)
- (i) Article from Phillips Fox - "A new era of private sector privacy protection"
(ii) Compliance Checklist
(iii) National Privacy Principles
4. Example Privacy Policy Statement (prepared by Sandra Davey)
 5. Draft AIMIA Privacy Policy (prepared by Lynne Spender)

1. President's Report - "Issues for 2002"

Sandra Davey reports on 2001 and outlines AIMIA's prime achievements and issues

- We need to capitalise on the momentum we have in Canberra - and make an effort to brief Senator Richard Alston - submission on datacasting - 25 February
- The Export Access Program finishes this year and a new program is to be announced - we know that AIMIA will be part of it but that there will be significant changes to the structure of the program
- The website - our credibility depends on the new website and improved services for members

Our focus needs to be on:

membership - the content industries are changing and there are new members for AIMIA in the areas of education; the creative industries (publishing, illustration, design, communications etc); interactive TV and broadband as well as in companies like Ericsson which are focusing less on technology and more on content. AIMIA should have a membership drive of some sort if we are to bring in enough income from subscriptions to fund the national office and support the states

- website development - a must for 2002 - the brief for the new site will solve some of the current problems where there is little contact between states and where we currently do not have the human or website resources to support special interest groups
- issues of privacy, security, intellectual property (copyright and DRM) as major issues for the industry
- finances - our support from the NSW state government (\$15 000 pa contribution to rent of National Office) is not guaranteed - we need to do some lobbying in NSW to ensure that this support continues
- outreach in areas where AIMIA membership is low - Tasmania, WA, and the Territories. (Hopefully SA will start to improve with Evon's energy)

by Sandra Davey

2. Annual Report - 2001 THE YEAR THAT WAS not as bad as it might have been

At the AIMIA Meeting where plans were made for the 2001 year, members talked about the upcoming federal election and determined to have a policy presence in Canberra during the year. We also discussed the possible negative impact on the industry of what is now referred to as the 'dot.com' (or dot.bomb) crash'. And we were pretty accurate in defining these as the major issues for the year

1. Policy

Early in 2001, National President Colin Griffith and Executive Director Lynne Spender circulated to members a draft submission on issues relating to the Industry. With input from members of the National Committee, this evolved into a paper on digital content, which was submitted in Canberra and to various state agencies. Issues raised in the paper were discussed with DCITA, the Office of the Prime Minister, the Arts Minister and the Opposition.

This resulted in some attention being paid to the content industries and during the year. In the lead up to the election:

(iv) Senator Alston's office announced a \$2.1 million broadband content fund to be administered by the AFC with first round funding being available after 30 June 2002

(v) a cluster study of the industry, managed by the National Office of Information technology was announced The first report from the cluster study - to which Colin Griffith was appointed as an adviser and which we hoped would provide a clearer picture of the industry in Australia - is imminent

(vi) AIMIA participated in the development and presentation of the inaugural OzEculture Conference in Melbourne

(vii) a digital round table was convened with AIMIA representatives invited to discuss issues for the industry with the Minister, colleagues and advisers from DCITA

On the basis of the positive relationships developed with state and federal governments, AIMIA will be lobbying this year for:

- a bigger and more permanent digital media fund (an extension of the broadband content fund)
- changes to the datacasting rules to encourage the takeup of broadband and the growth and development of a viable Australian content industry
- research scholarships/fellowships for people working in the interactive media industry
- direct financial assistance for AIMIA to undertake industry related research and projects

2. Services to Members

During the 2001 year, AIMIA members were provided with free copies of the National Magazine 'Webhead' as well as a free weekly emailing of Internet Watch Magazine, provided by Slattery IT Consulting. Members in Victoria, NSW and Queensland were invited to attend regular meetings and briefings organised for them by their state committees and IDOs, supported by National Office. The appointment of a part-time Industry

Development Office in South Australia in the latter part of the year means that SA members now also have access to local AIMIA events and to being part of a visible interactive media community.

During 2001, fortnightly Newsletters were dispatched from National Office with local, national and international news and information, including discounted fees for approved conferences and exhibitions. States with IDOs also received news bulletins aimed specifically at the local industry. Thanks to the NSW, QLD SA and VIC governments for the financial support they offered during the year. NSW government assisted with rent for the National Office, As well as housing the Queensland Industry Development Officer in their Milton offices, Queensland supported a research project and report into the Games Industry. The

Business Centre in South Australia offered financial support for a series of events in South Australia, and Multimedia Victoria was generous in its support of the Annual Awards being held in Melbourne.

AIMIA National Office organised the sponsorship, marketing and judging for the Annual Industry Awards and provided the contact point for thousands of telephone and email inquiries linking members to each other and referring members and their services to the public. Staff at National office manage the organisation fulfilling corporate, insurance and other legal requirements.

AIMIA has been aware for several year that our website needs urgent attention and but the fund have not been available to either dramatically upgrade the old site or to develop a new one. During 2000, the national office liaised with members who have agreed to assist with the development of stage 1 of a new site, which is now being organised. The site will eventually abnew site

The AIMIA Export Access Office, administered through the National Office, recruited another 30 clients onto the EA program, assisting them with information and resources to launch their products offshore.

3. AIMIA membership

In spite of the global downturn, membership at AIMIA remains at just under 500. We have lost a number of corporate members in the dot-com crash - and gained a number of new student members, thanks to the efforts of various state committees who worked hard during the year contacting students and educational institutions to cement connections between industry and training/education bodies. This has meant a shortfall in funds from membership and means that we need a concerted effort this year to rebuild our membership. We are relying on membership fees to support the new AIMIA website, which will in turn provide a better service for our members.

What we have lost (and we lost quite a few) we have gained through the export access program and the efforts of the staff and at events. There is still much room for us to follow up people who attend events and 'convert' them into members

Thanks to:

AIMIA staff and IDOs

All committee members and their hard work during the year

Nicola and Michelle at Mendleson

Brainwaave for acting as our ISP

Rob Clemente for assistance during the year - premises/staff (Thanks to Kathy Speakman and Jodie)

Peter Higgs and IPR for generosity and forbearance (and photocopier)

Michael Buffham for the weeks of work he did for AIMIA and the Awards

Libby for being herself

Colin for being an excellent President and a pleasure to work with

Lynne Spender

Executive Director

3. PRIVACY - Resources for members

(i) A NEW ERA OF PRIVATE SECTOR PRIVACY PROTECTION

Mathew Hall reports on the new privacy laws and issues that affect our members

In a recent survey conducted by the Office of the Privacy Commissioner Internet retailers were perceived as the least trustworthy organisations regarding the protection and use of personal information, scoring 1.98 on a scale of 5, (with real estate agencies and market research companies rating above them slightly).

The same survey also found that 'respect for, and protection of, my personal information' was, overall, the aspect of service that mattered most to the largest proportion of consumers rating above quality of product, efficiency, price and convenience.

While the benefits of sound privacy practices are obvious, most private sector organisations are now required by law to maintain certain minimum privacy standards.

The new privacy laws

New private sector privacy laws commenced on 21 December 2001.

However, it is never too late to comply. The Privacy Commissioner has indicated that he will "not be taking a heavy-handed approach to enforcement. His office will be working with - not against - business ... to ensure realistic and mutually agreeable outcomes" and increased compliance over time.

Do the privacy laws apply to your organisation?

All private sector 'organisations' must comply with the Act. An 'organisation' is an individual or entity (including an unincorporated association or trust) that is not:

a small business operator (ie. organisations with a turnover of under \$3 million are generally exempt - see below for further details)

a registered political party

a Commonwealth government agency that is already required to comply with the Information Privacy Principles in the Privacy Act

a State or Territory authority

a body performing government functions, which has been prescribed as a State or Territory instrumentality

an individual acting in the course of his or her own personal, family or household affairs

Is your 'small business' exempt from the application of the new privacy laws?

A **small business** is an organisation that, during a financial year, has an annual turnover of less than \$3 million. As a general rule, most small businesses are exempt from the new privacy laws.

However, the NPPs will apply to small businesses that:
are related to a company with an annual turnover of more than \$3 million
elect to opt in
provide a health service (broadly defined to include any activity intended or claimed to "maintain or improve" an individual's health, and so would include gyms and health clubs), to individuals and hold health information (except in an employee record)
disclose personal information about another individual to anyone else for a benefit, service or advantage; or
are a contracted service provider to a federal government agency

Most of these small businesses have an additional 12 months to comply with the new privacy laws (making the compliance date 21 December 2002). However, if the small business provides a health service to individuals and holds health information it must comply from 21 December 2001.

Even if you do not have to comply, you may find that many clients or others with whom you deal will require you to comply (or to warrant that you will comply). Also, developers need to be aware of the regime when considering any design and functional elements of multimedia products.

What do the new privacy laws do?

The new law establishes a set of 10 privacy principles, the National Privacy Principles (NPPs), that provide the minimum standard for privacy protection.

The NPPs:

- (a) set out rules relating to the collection, use, disclosure, quality and security of personal information
- (b) require organisations to be open about their information-handling policies
- (c) grant individuals a right to access the personal information an organisation holds about them, and to deal anonymously with organisations where practicable
- (d) require organisations to take steps to ensure that personal information they hold is accurate, complete and up to date, and that its security is maintained
- (d) prohibit an organisation from adopting as its own identifiers of individuals, identifiers assigned by government agencies (such as tax file numbers)
- (e) limit the transfer of information to organisations outside Australia to those in countries or circumstances that can guarantee individuals the same privacy rights as they have in Australia
- (f) require a higher standard of protection for the collection and use of "sensitive" and "health" information. Sensitive information includes information about an individual's racial or ethnic origin, political opinions, religious beliefs and sexual preferences.

Personal Information

NPPs protect '**personal information**'. This is broadly defined as information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual (a "natural person") whose identity is apparent, or can be reasonably ascertained, from the information or opinion.

Information about companies or other entities is **not** covered by the regime.

Privacy Codes as an alternative

The new law also allows industry bodies to have and enforce their own tailored privacy codes in place of the NPPs.

However, each code is subject to the Privacy Commissioner's approval and must provide privacy standards that, overall, are at least the equivalent of the obligations in the NPPs.

What is not covered by the new privacy laws?

There are some limited exemptions under the law. Information about companies is not covered. Also, employee records, media organisations and registered political parties are exempt. These exemptions are detailed and complex. If you think that you may be covered by an exemption you need to obtain further detailed advice.

Privacy Policies & Collection Statements

The NPPs require organisations to establish two documents regarding the organisation's information handling and privacy practices:

- a Collection Statement making a number of specified disclosures in relation to its collection of personal information (as a general rule, all forms that an organisation use to collect personal information must include this statement), and
- a written Privacy Policy, a high-level policy document which must be made available to anyone who asks for it - eg by placing it on the organisations website.

If the uses or disclosures of personal information an organisation makes are limited, the Collection Statement and Privacy Policy may be combined into one document.

What happens if an organisation does not comply with the new privacy laws?

The new law gives the Privacy Commissioner extensive powers to investigate complaints and to make determinations, including for the payment of compensation. These are enforceable in the Federal Court and the Federal Magistrates Court.

It is very important that all private sector organisations (with the exception of some small businesses) review their existing collection, use, storage, and disclosure practices with respect to personal information, to ensure compliance with the Privacy Act and client requirements.

(ii) COMPLIANCE CHECKLIST

The first step an organisation needs to take is to appoint a privacy officer to co-ordinate a uniform approach to the Privacy Act.

To prepare for implementation, the organisation then needs to:

- undertake a data audit to determine its data collection and supply chains
- review existing practices and procedures for collecting, using, storing, disclosing and accessing personal information
- formulate and implement a privacy policy that clearly sets out its policies on the collection, handling and use of personal information
- formulate a collection statement providing the information required by the new Act
- develop and implement mechanisms for ensuring quality and security of personal information
- implement organisation-wide training on the handling of personal information
- update all standard contracts for arrangements with third parties which involve the disclosure of personal information
- consider whether there is a need for an industry code and complaint mechanism

For further information contact:

Matthew Hall

Ph: 9286 8527
Email: matthew.hall@phillipsfox.com

Rachel Burleigh
Ph: 9286 8233
Email: rachel.burleigh@phillipsfox.com

Phillips Fox Lawyers
Ground Floor
255 Elizabeth Street
SYDNEY NSW 2000

(iii) National Privacy Principles

The National Privacy Principles, under the commonwealth Privacy Act ("NPPs") specify the minimum standards for the collection, use and disclosure of personal information by private sector organisations. In summary, the 10 NPPs require that:

Collection of personal information must be fair, lawful and not intrusive. Therefore, individuals must be well informed and told the collectors name, purpose for collecting the information and that they can get access to their information.

Use and Disclosure of personal information must only be for the primary purpose that it was intended for (or for strongly related secondary purposes). Therefore, individuals must consent to the use of their personal information or any other purpose other than the provision of a health service, for example consent will be required for marketing purposes. An opportunity must be provided for individuals to opt out of and particular use of their information.

Data quality must be accurate, complete, and up-to-date when collected and used.

Data Security must ensure personal information is safe from misuse, loss or unauthorised access.

Openness must be provided and the collector must have a policy document available to individuals to outline its information handling practices. Upon request, the collector must take steps to inform individuals what sort of information it holds, for what purposes and how it collects, holds, uses and discloses that information.

Access to and correction of personal information must be made available on request by an individual.

Anonymity should be provided by the collector whenever it is lawful and practical to do so.

Transborder data flow are only allowed where the foreign recipients has similar privacy restrictions imposed.

Sensitive information must not be collected unless the individual has consented, or in some special circumstances (such as public health and safety). Note sensitive information includes information about an individual's health.

Transitional Provisions

All NPPs will apply to personal health information collected after 21 December 2001. Some business operations will have a further 12 months within which to comply. However, not all of the NPPs will apply to person information that is collected before that date.

In summary, the NPPs that will apply to information collected prior to 21 December 2001 are:

NPP3 - Quality - obligation to ensure that the information stored and used b the collector is complete, accurate and up to date;

NPP4 - Security - obligation to keep this information secure;

NPP5 - Privacy Policy - obligation to provide privacy policy on request;

NPP6 - Access and Correction - obligation to provide access to this information and correct it if shown to be inaccurate. However, you do not need to comply if it can be demonstrated that to do so will impose an unreasonable burden or lead to an unreasonable expense.

NPP7 - Government Identifiers - obligation not to use government identifiers; and

NPP9 - Transborder Data - may not transfer this information overseas unless they have similar privacy obligations

imposed.

One issue that needs to be addressed is the extent to which existing data needs to be quarantined from new data. The Act is silent on the point. However, we are of the view that if an existing record is updated or added to, after 21 December 2001, it no longer has the benefit of the transitional provisions. All of the privacy principles will apply at that time.

You will need to develop a mechanism to identify these types of updated information, so as to ensure compliance. The alternative is to accept the obligations to comply with all NPPs in respect of all personal information that you hold.

4. Example Privacy Policy Statement

Note: You are welcome to use this policy upon which to base your own. Insert your name/company name where applicable.

Privacy Policy

At xxxxx, we see the protection of your privacy to be of the highest importance and we have made our site cookie-free so you can access and browse without disclosing any personal information. We do not automatically log personal data/information, nor do we link information automatically logged by other means with personal data about specific individuals.

When you look at our site, our Internet service provider (ISP) makes a record of your visit and logs the following information for statistical purposes:

- your server address
- the date and time of your visit to the site
- the pages accessed and documents you downloaded
- the site that directed or referred you to us eg. a search engine
- the type of browser you used
- your top-level domain name (eg. .com, .au, .gov, .uk etc).

No attempt will be made to identify you or your browsing activity except, in the unlikely event of an investigation, where a law enforcement agency may produce a warrant to inspect our ISP's logs.

We will only record your email address or other details you provide if you send us a message to request more information when using our contact form.

Your details will only be used for the purpose for which you have provided them and will never be added to any mailing list. We will not use or disclose them to anyone without your consent.

Our Privacy Policy and our approach to privacy adheres to the Australian Government's National Privacy

Principles contained within the new Privacy Amendment (Private Sector) Act 2000.

If you have a question about our Privacy Policy, or would like to gain access to information we might hold about you, please contact us.

You can obtain more information on Australia's approach to privacy from the Australian Privacy Commissioner's website.

5. AIMIA Privacy Policy statement

AIMIA believes that an individual's right to keep personal information private is very important. We are committed to protecting your right to privacy and ensuring the accuracy and security of any of our members personal information.

How we collect your information

We collect your information directly from you when you join AIMIA as a member or when you register with us for an event or activity or you nominate for our Annual Industry Awards. We collect only your contact details, financial details insofar as you provide them to pay your membership or other fees and any other information that you volunteer. We do not collect sensitive information relating to your health, personal or political affiliations.

How we use your information

We use your personal information :

- provide you with information about the industry
- provide you with services offered by AIMIA

Where you have given consent, we may provide your contact details to potential clients or business partners.

Who will use your information

Your personal information is used only internally for purposes associated with membership records unless you register your details or we have your consent to make details available on the AIMIA website or in the AIMIA Directory of Members. We may ask your consent to provide sponsors with your contact details if you are shortlisted for the AIMIA Industry Awards.

Security of Information

We are committed to keeping data you supply confidential unless you give us permission to make it available under certain circumstances. We do not for example, make available any financial information we may have about you. We will not retain information for any longer than is required except to comply with legal obligations. We will, with your assistance, keep your information accurate and up to date. You will be invited at least twice in each year to update your information with AIMIA.

Access to your information

You can access your information held with us. You can correct the information on the website via your membership password or you can request that we make available any other records we hold. We will correct any errors and update the records if they are inaccurate or out of date.

Resolving your privacy concerns

If you have any privacy concerns relating to records at AIMIA, you can contact the office staff by phone or you can email or write to us at [AIMIA National Office](#).