australian privacy foundation
po box r507 royal exchange sydney nsw 1225
ph (02) 9231 4949 fax (02) 9262 3553

22 March 2001

Ms Jo Lim
Secretariat
auDA Model Competition Advisory Panel
Australian Domain Administration
GPO Box 1545P
Melbourne VIC 3001

Submission to the auDA Model Competition Advisory Panel

To the auDA Competition Model Advisory Panel

I am writing to you on behalf of the Australian Privacy Foundation in respect of your call for submissions to the Competition Model Advisory Panel. We believe that the proposed changes to domain name registration procedures raise serious privacy issues for both Australian and international Internet users. In particular, we would suggest that auDA must take steps to ensure that the public accessibility of personal information through the Whois protocol is restricted and monitored such that it can become neither a threat to individuals' privacy, nor a disincentive for the use of the Internet in general.

While the auDA *Stage 3 Report for Public Consultation* does make some brief mention of privacy concerns, it provides only the most minimal consideration of the nature of the threats to the security of personal information involved in maintaining the public registries and deals only briefly with how such threats might be addressed in any final stipulation. Such concerns must be taken into account in order to preserve users' rights to privacy and choice when applying for domain names.

The need for a cogent and coordinated response in regards to the management of the personal information maintained by the registries is all the more vital in light of the fact that such databases are likely beyond the scope of the recent changes to privacy legislation that come into effect in December 2001 with the commencement of the *Privacy Amendment (Private Sector) Act 2000,* because of the exclusion of personal information which is published already in a generally available publication. The management of information stored in a Whois database is therefore beyond the scope of legislative control. For this reason, it is imperative that auDA take reasonable steps to ensure the protection of users' personal information in order to avoid exposing them to unreasonable and irremediable abuses.

The ability to obtain and maintain a domain name is an increasingly critical part of Internet usage. It is among the most basic facilities enabling individuals and groups to interact in the online environment, and provides an excellent opportunity for the free exchange of ideas and debate. Such freedom of communication is a basic right that should not be made contingent on willingness to supply personal information. By requiring organisations and companies to release sensitive personal information to the public as a condition of obtaining a domain name, auDA would, in effect, be forcing user's to choose between their right to privacy and their right to communication.

As recently seen in the US with Verisign's decision to sell domain name registration information to marketers, publicly accessible Whois protocols are somewhat of a double edged sword for Internet users. On the one hand, they ensure that companies and individuals who operate web sites are accountable for the content of such sites, ensuring a degree of consumer protection. On the other hand, however, they can act as disincentives for individuals and small organisations to register domain names as many people would be unwilling to make their personal information freely available. This is especially the case where an individual may operate from home and may therefore be forced to place his or her home address and phone number with the registry.

Only a few months ago, the furore over the inclusion of personal information in the Australian Business Register highlighted a similar issue in Australia. The reforms to the taxation system made it essential to obtain an Australian Business Number (ABN) for business to business dealings. Over 3 million applications for ABNs were received in the second half of 2000, although Australian Bureau of Statistics figures indicate that there are only 1.1m businesses in Australia – suggesting most ABNs were for individuals. The ATO had not taken into account the extent to which individuals would obtain ABNs, and the fact that ABN records would contain a substantial amount of personal information. Legislation relating to the ABN established a publicly available Australian Business Register, including information on the holders of ABN drawn from the ABN registration forms, and in addition the Tax Office was planning to make available records of registration-related information to a private sector business information database which would then charge for access. Although the ABN registration booklet mentioned that some ABN information would be publicly available, the details of this availability were not clear and applicants were not informed of this on the pages where they entered information. After a substantial public reaction, and intervention by the Privacy Commissioner, the Treasurer agreed to legislative amendments and the Tax Office agreed to limit the amount of information available publicly, and give individuals the option of limiting disclosure of their information if this disclosure could present a danger to them.

In light of such conflicting concerns, it is important to understand the extent of the threat posed by the proposed restructuring of the domain name registration system, and the potential for significant improvement in terms of the protection of personal information. One particular area of concern relates to the ways in which independent 2LDs, acting as registrars, might be allowed to use the information they collect from registering parties. The Verisign example demonstrates that consumers and companies are extremely concerned about registrars transferring or selling their information to other organisations, a fact that has been continually demonstrated by consumer surveys. The American example of Verisign has even more resonance in the Australian context as a result of the fact that, unlike Verisign, the current AUNIC registry has no privacy policy whatsoever.

These problems exist at present and should be rectified by whichever model the Panel chooses to adopt. To this end, the Foundation believes that by allowing bulk access to registry data as a means of cost recovery, even where spamming is expressly prohibited, would unreasonably compromise a registrant's privacy. A reasonable compromise would be to provide registrants with the opportunity to 'opt in' to such arrangements, so that the bulk access lists contain only the details of those who consent to the release of their information. This scheme has an added benefit for those seeking bulk access, in that they can ensure that their target audience is limited to those groups most keen to receive marketing information.

Moreover, a dedicated 'opt in' approach to the release of personal information would have the benefit of ensuring that individual privacy is not sacrificed, yet stop short of a situation of registrant anonymity that would compromise consumer protection. While it is certainly necessary for registries to collect contact information for technical and administrative contacts so as to ensure that criminal and fraudulent activities can be traced to individuals, there is no reason why such information needs to be publicly available.

Publicly accessible information should be restricted to:

- the domain name
- the Internet Protocol address
- name of the registrant

While the personal and contact information for individuals should only be available to government authorities (such as the police, ACCC, the Courts, ASIO, etc) where it is required for:

- criminal investigation and law enforcement
- trademark and cyber-squatting disputes
- consumer protection

Again, an 'opt in' provision would allow those who are comfortable with the release of their information to provide contact details, yet allow a certain degree of anonymity which may be essential where members of registrant organisations risk prejudice and persecution.

Under Proposal 4.3A some further degree of protection would probably be required as the multiplicity of registrars allows for the possibility of greater abuse. Nevertheless, such problems could be overcome were auDA to prescribe certain standards that 2LDs must apply in protecting personal information. Under paragraph 4.3.32 of the *Report for Public Consultation*, the Advisory Panel suggests that auDA might mandate technical standards with which all registrar 2LDs must comply. We would submit that in addition to these standards, a set of personal information protection standards should be adopted to ensure that such information is not misused.

Such standards should (at the very least) require the following:

- that each 2LD have a privacy policy detailing:
  (a) what information is collected;

  (b) how information is used; and

  (c) when information will be disclosed to third parties.

- that each 2LD provide a means by which registrants can gain access to the registries information about them and rectify any errors.
- that each 2LD adopt a high level of security in dealing with personal information so that it is safe from hackers and software failures.

A related issue relates to the way in which the collected information is made publicly available. Currently, registries such as AUNIC fail to give clear notification to potential registering parties that the personal information they provide in the registering process will become publicly available through the Whois protocol. This prevents organisations and individuals from making informed choices as to the provision of their personal information and potentially exposes them to greater level of public exposure than that to which they would ordinarily give consent. This also breaches basic fundamental privacy principles which have been accepted internationally since the OECD promulgated its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980, and which are embodied in laws throughout the world. Whether Proposal 4.3A or 4.3B is adopted, it is essential that registrars be required to provide clear notification of what information will be publicly available thereby allowing potential registrants to make informed choices.

In summary then, the Australian Privacy Foundation recommends the following:

- That auDA adopt mandate a set of procedures to ensure the protection of personal information applying to all registries.
- That these procedures include the adoption of privacy policies by all registries as well as a requirement that registries notify registrants as to how their information be used.
- That auDA continues to collect all the information it currently collects but that only the domain name, IP address and registrant's name be in the public domain.
- That auDA allow registrants to 'opt in' to further disclosure so that those who choose to release their personal information can to do so.
- That auDA allow a small number of specified government agencies access to all registry information for criminal investigation, trade mark and consumer protection purposes.
- That auDA allow all registrants to 'opt in' to any purchasable bulk access arrangement so that only the details of users who consent to the release of their personal information are publicly available.

It is imperative that the auDA considers not simply the interests of e-commerce and trading sites, but also that of public interest groups, small organisations and individuals for whom the release of personal information may represent a considerable compromise of their right to privacy. Such concerns can be balanced against the need for registered information about domain name registrants by requiring that only the essential information about a registrant is publicly available, and by allowing these groups to determine their own level of exposure beyond this basic level. This would not prevent contact information from being accessed by government authorities for legitimate criminal investigation and consumer protection purposes, yet would nevertheless preserve both the registrants' right to communicate and their right to privacy. In the longer term, it would help us to realise the tremendous benefits which the Internet can bring to our democracy.

Yours Sincerely

Tim Dixon
Chairman, Australian Privacy Foundation