Internet Society of Australia
A Chapter of the Internet Society
ABN 36 076 406 801

C/- Maddocks, Level 7, 140 William Street
Melbourne, Victoria 3000
Accounts: P.O. Box 351, Glenorie NSW Australia 2157

To: Jo Lim, Chief Policy Officer

auDA

By email: jo.lim@auda.org.au

Friday, 11 September 2009

# INQUIRY INTO DOMAIN RENEWAL, EXPIRY AND DELETION POLICY

The Internet Society of Australia (ISOC-AU) welcomes this opportunity to comment on the auDA Inquiry into Domain Renewal, Expiry and Deletion Policy.

ISOC-AU's fundamental belief is that the Internet is for everyone. We provide broad-based representation of the Australian Internet community both nationally and internationally from a user perspective and a sound technical base. We also consistently promote the availability of access to the Internet for all Australians., ISOC-AU has a direct interest in the outcomes of the arrangements that will underpin the provision of the NBN, because the Internet is a central driving factor in the demand for broadband.

The overriding objective of the Society is to give expression to the needs and wishes of individuals, groups, or organisations that have a common interest in the viability of the Internet in Australia, so that all Australian users of the Internet may continue to benefit from, and contribute to, its applications, technologies, and evolution. Our submission, therefore, is made from the perspective of the users of the Internet, drawing on the strong technical base of understanding of our ISOC-AU membership. In particular, users include the individuals, groups and organisations that are impacted by the auDA Name Policy Framework.

In our view, Domain Names should be viewed as a public resource to be managed in the interests of Internet users including individuals seeking access to Internet sites and registrants providing those sites.

The Society's response to the Inquiry's individual Terms of Reference are as follows:

## 1. DELETE PERIOD

Term of Reference:
*Whether the current 30 day pending delete period for expired domain names (ie. where the registrant has not renewed their domain name) is appropriate.*

Registrants may choose, for whatever reason, not to renew their domain name. Domain names can, however, also be deleted through error, including the following:

- Registrant mistake – failure to renew (due to clerical error, failure to receive a renewal notice or change in Internet service provider

- Registrar mistake including those caused by registry/systems-related confusion (this is addressed in the Registrar Accreditation Agreement, but the procedure is not mandatory)
- Deletions arising from the actions of domain name hijackers

The consequences of mistaken deletion of a domain name can have serious consequences for the registrant. Therefore, it is critical that registrants are given timely notice of a pending expiry of their domain name and additional notice when the domain name has expired and is pending deletion.

The Redemption Grace Period, introduced by ICANN in 2002, allows 30 days in which an expired domain name is not made available. Clearly, the auDA 30 day period is in line with ICANN policy and appears to allow sufficient time for a registrant to reclaim a domain name that may have been deleted in error. The 30 day period, however, can only be seen as adequate if the registrant is given adequate notice of the pending deletion of their domain name. It should also be noted that, in the case of telephone numbers, a disconnected number is put into quarantine for between six to twelve months before it can be reallocated, except in particular circumstances such as reallocation to the number owner.[1]

Because the Registrar Agreement requires that registrars update registrant information in the Registry's registrant database (clause 11.2), registrars (and their resellers) should have current contact information for their registrants, hopefully avoiding instances where incorrect registrant contact information is used.

*Recommendation:*

*That the auDA Domain Name Supplier's Code of Practice be amended to require that registrants are given a minimum period of notice (at least two weeks) before their domain name has expired, and an additional notice when their domain name is pending deletion, including information in both notices of how the registrant can renew their domain name.*

## 2. 'DOMAIN PURGE' PROCEDURE

Term of Reference:
*Whether the current "domain purge" procedure (ie. where domain names are purged from the registry at a random time between 10.30am and 5.00pm AEST on the next business day after the pending delete period ends) is effective.*

ISOC-AU has no comment to make on the auDA 'domain purge' procedure.

## 3. "DROP LISTS'

Term of Reference:
*What action (if any) auDA should take in relation to unofficial domain drop lists, and the domain-catching services being provided by some accredited registrars and other industry participants.*

The auDA Domain Name Suppliers' Code of Practice has, as one of its objectives: '…preventing practices that undermine the reputation of the industry and interests of registrants and customers'. (clause 2.1(e). Some of the comments made to this inquiry suggest that 'drop lists' are seen as unfair and should not be allowed.

[1] ACMA, *Numbering Plan 1997*, Divisions 9 and 10.

What 'drop lists' do is effectively deny potentially eligible registrants the opportunity to obtain a domain name when it becomes available. It has been suggested that, to address this issue, people should be able to register an interest in a particular name and when it becomes available, the name be allocated on a first come, first served basis. The difficulty with the suggestion is that people may be reluctant to highlight their interest in a particular name, for commercial reasons. The ICANN Safety and Security Advisory Committee (SSAC) highlighted difficulties with having a public list where individuals can express interest in a particular domain name.

*SSAC begins with a premise that checking the availability of a domain name can be a sensitive act which may disclose an interest in or a value ascribed to a domain name. SSAC suggests that any such domain name availability lookups should be performed with care. Our premise is that a registrant may ascribe a value to a domain name; that unintended or unauthorized disclosure, or disclosure of an availability check by a third party without notice may pose a security risk to the would-be registrant; and that availability checks may create opportunities for a party with access to availability check data to acquire a domain name at the expense of the party that performed an availability check, or to the benefit of the party that monitored the check.*[2]

Recommendation:
*That auDA explore ways in which it can maintain a publicly available list of names that have entered the pending expiry period. Applicants can then be judged on, first, their close and substantial connection with the name, and, for those meeting the eligibility requirements, allocation on a first come, first served basis.*

# 4. OTHER POLICY ISSUES

### *Domain Name Renewal*

*In our submission to the auDA Domain Name Policy Framework inquiry, we suggested that domain names be able to be registered for periods of one, two or three years. We continue to support this recommendation.*

# 5. OTHER ISSUES

## 5.1. *Code of Practice Review*

The auDA Domain Name Suppliers' Code of Practice says that the Code will be reviewed on an 'ongoing' basis. However, the date of the Code is stated as 2004. Either the date of the Code does not reflect any 'ongoing' process of Code review, or it has not been reviewed since 2004. Given recent changes to the ICANN Registrar Accreditation Agreement, and the many advisories issues by the ICANN SSAC, it would be timely to review the Code of Practice within the next year.

Recommendation
*That auDA commence review of the Domain Name Suppliers' Code of Practice within the year 2010.*

[2] SAC22: *SSAC Advisory on Domain Name Front Running*, October 2007, p. 2.

## 5.2. *Registrar Point of Contact*

Under the gTLD agreements, registrars are required to provide a point of contact. In the ICANN's view, there should be an additional requirement for a point of contact for dealing with instances of DNS abuse. The recent SSAC Advisory on Registrar Abuse Points of Contact emphasises the importance of this issue.

*Inquiries involving alleged abuse or criminal activities typically require timely if not urgent response. For example, inquiries that will lead to the suspension of a domain name used in a phishing attack, in support of an illegal activity (hosting of child pornography or illegal sales of prescription pharmaceuticals) are ideally processed within hours. In the case of a "double flux" attack, minutes of delay provide an attacker with sufficient time to divert his attack vector to other domain names he has registered or domains over which he has obtained unauthorized control.*[3]

*And the SSAC inquiry into registrar points of contact found:*

a) *Not all registrars voluntarily publish public contact information on their web sites,*
b) *Not all of the published contact information is accurate or complete,*
c) *Personnel who are reached via certain published contact information may be unable to handle abuse inquiries or may be unfamiliar with escalation procedures that would put an investigator in touch with a suitable (e.g., technical) contact, and*
d) *Not all registrars publish a separate abuse contact, and*

In the SSAC's view, while a public contact may only be available during specific business hours, an abuse contact should be available 24 x 7.[4]

Recommendation
*That the Suppliers' Code of Practice be amended to require registrars to provide an easily accessible point of contact and, for instances of abuse or criminal activity, abuse contact information available to relevant authorities on a 24/7 basis.*

## 5.3. *Registrar contact of Registrants*

We have suggested above that registrars contact registrants, particularly in relation to a pending expiry of the registrant's domain name. However, a recent advisory from the SAC suggests caution in the way registrars communicate with their registrants.

As the Advisory suggests:
*Phishers have broadened their reach beyond merchant and financial institutions and into domain registration service providers. Registrars and resellers must acknowledge that they are phishing targets in response. SSAC recommends that registrars (and resellers) exercise care and follow antiphishing best practices when composing correspondence to customers.*

*SSAC specifically recommends that registrars use the following practices when communicating with their registrants:*

[3] SAC 038 *Registrar Abuse Point of Contact*, 29 February 2009, p. 2
[4] Ibid.

1. *Only include information necessary to convey the desired message in customer correspondence. Do not include customer account numbers, identities, and (generally) registration information.*
2. *Avoid using hyperlink references in correspondence with customers. Warn customers against clicking on hyperlinks included in any correspondence, in text or image fashion. Include statements in the message bodies of correspondence you send such as, "To protect against phishing, please type the following web address into the address bar of your web browser" or "Do not trust links in email. Always type a web address into your browser's address bar.*
3. *Raise awareness that registrars are targets for phishing attacks. Provide (or expand existing) FAQ pages to call attention to registrar impersonation phishing, the threats these phishing attacks pose, measures you are taking to deter phishing and measures your customers can take to detect and avoid falling victim to such attacks. Explain the type of information you will include in email correspondence and in particular, identify the types of information that you will never include in correspondence so that customers have a basis for assessing whether correspondence they receive is legitimate or suspicious.*
4. *Provide a means for a customer to report suspected phishing attacks, either directly, or in cooperation with an organization that encourages submission of suspected scam and fraud emails and maintains a repository of phishing emails.*
5. *Consider implementing a form of email non-repudiation of origin for customer correspondence, such as a digital signature.5*

Recommendation:

*That the Suppliers' Code of Practice be amended to provide registrars with guidance on how to more safely communicate with their registrants and customers.*

We will be happy to provide any further comments on issues raised by this Inquiry


Tony Hill
President
Internet Society of Australia
President@isoc-au.org.au

Holly Raiche
Executive Director
Internet Society of Australia
ed@isoc-au.org.au


[5] SSAC 028 *Advisory on Registrar Impersonation Phising Attacks*, May 2008, p. .10