Law Enforcement Recommended RAA Amendments and ICANN Due Diligence

Detailed Version

Introduction: Below are: 1) suggested amendments to the RAA and; 2) due diligence recommendations for ICANN to adopt in accrediting registrars and registries. Both are supported by the following international law enforcement agencies:

- Australian Federal Police;
- Department of Justice (US);
- Federal Bureau of Investigation (US);
- New Zealand Police;
- Royal Canadian Mounted Police;
- Serious Organised Crime Agency (UK)

The amendments are considered to be required in order to aid the prevention and disruption of efforts to exploit domain registration procedures by Criminal Groups for criminal purposes. The proposed amendments take account of existing EU, US, Canadian and Australian legislation and those countries commitment to preserving individual's rights to privacy. These amendments would maintain these protections whilst facilitating effective investigation of Internet related crime.

I. Proposed Amendments to the RAA (May 21, 2009 version)

1) The RAA should not explicitly condone or encourage the use of Proxy Registrations or Privacy Services, as it appears in paragraphs 3.4.1 and 3.12.4. This goes directly against the Joint Project Agreement (JPA) ICANN signed with the United States Department of Commerce on September 25, 2006 which specifically states "*ICANN shall continue to enforce existing (Whois) policy*", i.e., totally open and public WHOIS, and the September 30, 2009, Affirmation of Commitments, paragraph 9.3.1 which states "*ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information*." Lastly, proxy and privacy registrations contravene the 2007 GAC Principles on WHOIS.

   If there are proxy and/or privacy domain name registrations, the following is recommended concerning their use:

a. Registrars are to accept proxy/privacy registrations only from ICANN accredited Proxy Registration Services;[13]

b. Registrants using privacy/proxy registration services will have authentic WHOIS information immediately published by the Registrar when registrant is found to be violating terms of service, including but not limited to the use of false data, fraudulent use, spamming and/or criminal activity.

2) To RAA paragraph 5.3.2.1, language should be added to the effect "or knowingly and/or through gross negligence permit criminal activity in the registration of domain names or provision of domain name WHOIS information…"

3) All Accredited Registrars must submit to ICANN accurate and verifiable contact details of their main operational and physical office location, including country, phone number (with international prefix), street address, city, and region, to be publicly disclosed in ICANN web directory. Address must also be posted clearly on the Registrar's main website. Post Office boxes, incorporation addresses, mail-drop, and mail-forwarding locations will not be acceptable. In addition, Registrar must submit URL and location of Port 43 WHOIS server.

4) Registrars must publicly display of the name of CEO, President, and/or other responsible officer(s).

5) Registrars with multiple accreditations must disclose and publicly display on their website parent ownership or corporate relationship, i.e., identify controlling interests.

6) Registrar must notify ICANN immediately of the following and concurrently update Registrar website:

a. any and all changes to a Registrar's location;
b. changes to presiding officer(s);
c. bankruptcy filing;
d. change of ownership;
e. criminal convictions ;
f. legal/civil actions

[13] ICANN to implement accreditation system for Proxy Services using the same stringent checks and assurances as provided in these points, to ensure that all proxy services used are traceable and can supply correct details of registrant to relevant authorities.

7) Registrar should be legal entity within the country of operation, and should provide ICANN with official certification of business registration or license.

8) Resellers must be held completely accountable to ALL provisions of the RAA. Registrars must contractually obligate all its Resellers to comply and enforce all RAA provisions. The Registrar will be held directly liable for any breach of the RAA a Reseller commits in which the Registrar does not remediate immediately. All Registrar resellers and third-party beneficiaries should be listed and reported to ICANN who shall maintain accurate and updated records.

9) Registrars and all associated third-party beneficiaries to Registrars are required to collect and securely maintain the following data[14]:

(i) Source IP address

(ii) HTTP Request Headers

(a) From

(b) Accept

(c) Accept-Encoding

(d) Accept-Language

(e) User-Agent

(f) Referrer

(g) Authorization

(h) Charge-To

(i) If-Modified-Since

(iii) Collect and store the following data from registrants:

(a) First Name:

(b) Last Name:

[14] Anti-Phishing Working Group (AGWG) "Anti-Phishing Best Practices Recommendations for Registrars", October 2008

(c) E-mail Address:

(d) Alternate E-mail address

(e) Company Name:

(f) Position:

(g) Address 1:

(h) Address 2:

(i) City:

(j) Country:

(k) State:

(l) Enter State:

(m) Zip:

(n) Phone Number:

(o) Additional Phone:

(p) Fax:

(q) Alternative Contact First Name:

(r) Alternative Contact Last Name:

(s) Alternative Contact E-mail:

(t) Alternative Contact Phone:

(iv) Collect data on all additional add-on services purchased during the registration process.

(v) All financial transactions, including, but not limited to credit card, payment information.

10) Each registrar is required to validate the following data upon receipt from a registrant[15]:

(1) Technical Data

(a) IP addresses used to register domain names.

(b) E-mail Address

(i) Verify that registration e-mail address(es) are valid.

(2) Billing Data

(a) Validate billing data based on the payment card industry (PCI standards), at a minimum, the latest version of the PCI Data Security Standard (DSS).

(3) Contact Data

(a) Validate data is being provided by a human by using some anti-automatic form submission technology (such as dynamic imaging) to ensure registrations are done by humans.

(b) Validate current address WHOIS data and correlate with in-house fraudulent data for domain contact information and registrant's IP address.

(4) Phone Numbers

[15] Anti-Phishing Working Group (AGWG) "Anti-Phishing Best Practices Recommendations for Registrars", October 2008

(i) Confirm that point of contact phone numbers are valid using an automated system.

(ii) (ii) Cross validate the phone number area code with the provided address and credit card billing address.

11) Registrar must provide abuse contact information, including the SSAC SAC 038 recommendations below[16]:

- Registrars must prominently publish abuse contact information on their website and WHOIS.

  1. The registrar identified in the sponsoring registrar field of a Whois entry should have an abuse contact listed prominently on its web page. To assist the community in locating this page, registrars should use uniform naming convention to facilitate (automated and rapid) discovery of this page, i.e., http://www.<registar>.<TLD>/abuse.html.
  2. Registrars should provide ICANN with their abuse contact information and ICANN should publish this information at http://www.internic.net/regist.html.

- The information a registrar publishes for the abuse point of contact should be consistent with contact details currently proposed as an amendment to Section 3.16 of the RAA. Each contact method (telephone, email, postal address) should reach an individual at the Registrar who will be able to promptly and competently attend to an abuse claim; for example, no contact should intentionally reject postal or email submissions.

- Registrars should provide complainants with a well-defined, auditable way to track abuse complaints (e.g. a ticketing or similar tracking system).

12) ICANN should require Registrars to have a Service Level Agreement for their Port 43 servers.

[16] ICANN SSAC SAC 038: Registrar Abuse Point of Contact, 25 February 2009

II. Proposed ICANN Due Diligence on current and new gTLD Registrars and Registries

a. ICANN to conduct enhanced due diligence on all Registrars and Registries (including but not limited to owners, officers, board of directors) ICANN accredits, or has accredited, to include, but not limited to:

- criminal checks;
- credit checks;
- financial history and solvency;
- corporate/company structure and ownership.

For example: Dunn and Bradstreet, Lexis-Nexis, Clear, World-Check, etc.

b. Such due diligence shall be documented by ICANN, in detail, in a written report that can be provided upon request to appropriate auditors.

c. ICANN should provide complainants with well-defined and auditable way to track complaints against Registrars and Registries.

i. ICANN should publish annual detailed reports of reported complaints.

d. ICANN should conduct WHOIS compliance audits , at least once a year, and publish results on:

i. Port 43
ii. WHOIS accuracy