Communication from Registrar Stakeholder Group

Summary of Law Enforcement – Registrar – Registry Meeting

Brussels, Belgium
24-25 February 2011

From

ICANN Registrar Stakeholder Group

FINAL OFFICIAL COMMUNICATION AS PUBLISHED 17 MARCH 2011

Introduction

In recent years, representatives of international law enforcement agencies (LEAs) have become active in the ICANN community, participating in discussions about combating improprieties facilitated in part through the domain name system (DNS). As a result of those discussions, LEAs have made proposals for policies and/or amendments to contracted party agreements they believed would assist them in more efficiently addressing improper activity.

The Registrar Stakeholder Groups (RrSG) proactively opened a dialog with LEAs to learn more about how the DNS is used for criminal activity, and to inform LEAs about operational and legal considerations relating to LEA proposals. This dialogue began in earnest during the 38th ICANN meeting in Brussels in June 2010, and was followed by a meeting in Washington, DC in September 2010.

While contracted parties and LEAs agreed that the Washington meeting was informative and productive, additional discussion was needed to consider regulatory and legal obligations of contracted parties in Europe and the Asia-Pacific region, as they sometimes conflict with those of US-based operators.

LEAs and contracted parties thus met in Brussels to continue discussions. Generously hosted by the European Commission, the meeting included international LEAs, contracted parties, government officials, and representatives from European and American Regional Internet Registries (RIPE NCC and ARIN).

Summary

The Brussels meeting agenda included:

- Review of LEA recommendations on due diligence in accrediting registrars
- Review of registrar standard operating procedures
- Case examples from EU law enforcement agencies
- Presentations regarding online crime from representatives of ccTLDs, including .gg, .na, .be and .uk.
- A review of the Internet landscape following the introduction of new gTLDs
- A discussion of the recent voluntary collaborative model used to address the sale of illegal pharmaceuticals over the internet (includes registries, registrars, payment providers, shipping companies, search providers, law enforcement, and the US government)

Statements of agreement by meeting participants

<u>Crime and improper activity under the DNS are significant and growing problems that continue to evolve rapidly</u>
Regrettably, crime facilitated through the DNS is a serious issue, and criminal activity develops and changes very quickly. Addressing and reducing criminal behavior demands collaboration and flexibility from a variety of different segments of the Internet ecosystem.

<u>Collaboration to address online crime must focus on objectives and the most practical method to achieve them</u>
While there have been specific proposals—namely, proposed amendments to the Registrar Accreditation Agreement (RAA)—the parties agreed that proposed collaboration should be focused on steps that would be most effective and rapidly deployed, whether or not this included new policy or amending contracts.

Contracts may or may not be the most practical or efficient method
Parties agreed that contracts between ICANN and contracted parties are not policy tools, but at times may represent an effective method for registrars and registries to assist LEAs in their efforts. It is important to consider that amendments to contracts may not be immediately effective (depending on the term of the agreement), so there likely are alternative methods to reach objectives that can have impact sooner.

Consider the entire Internet ecosystem
As cybercriminal activity evolves, the community should consider the entire Internet ecosystem in addressing crime to find the most effective path to solutions. This includes ICANN and its contracted parties, but also ISPs, hosting providers, search engines, payment processors, shipping firms, and others.

ICANN should add more rigorous due diligence to of its accreditation process
Additional diligence in evaluating applicants for registrar accreditation, at minimum, is a good practice and may offer assistance in evaluating who is well suited to provide domain name services and collaborate in online crime prevention.

ICANN must maintain a robust compliance program
For contractual and policy matters that are binding to contracted parties or others, ICANN must consistently and effectively enforce compliance with the terms of their agreements, and terminate accreditations, where appropriate.

Policy or contract amendment proposals must responsibly consider resource and financial costs of implementation, and how costs will be borne
Without considering the burden of implementation, proposed policies will needlessly be slowed by affected parties questioning how costs will be borne and by whom.

Review of LEA proposals

To organize specific discussions about how contracted parties and LEAs can collaborate toward addressing online offenses, participants examined LEAs' proposed RAA amendments. Each issue was thoroughly reviewed to identify the objective of the proposed amendment, hoped-for outcomes, and available paths toward the objectives.

Following is a list of the proposals, noting that further discussion and revisions are needed:

Proposal No. 1

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;
   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.

Summary of Discussion

There was agreement that accreditation of privacy/proxy services has value to consumers. The issue needs further research and discussion in order to understand how ICANN (particularly ICANN staff) would define accreditation parameters, pursue accreditation, educate the community, and seek to accredit current providers of such services.

Proposal No. 2

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…"

Summary of Discussion

There is agreement that language be added to provide notice of the illegal behaviour to the registrar and an opportunity to cure by the registrar would be necessary. Also, paragraph 5.3.2.1 of the RAA may not be the appropriate place for this amendment.

Proposal No. 3

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.

Summary of Discussion
Again, there was general agreement that this amendment is not objectionable. At least two alternatives are possible:

- Make the amendment more directly stated: "Registrars must provide a valid physical address for legal service, as well as a valid phone number."
- Amend section 3.16 of the 2009 RAA to specify that a physical address must be provided.

Proposal No. 4

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

Summary of Discussion
There was no objection to this, though the amendment needs to be more carefully worded, as the operational reality is that legal issues are often referred to others in an organization.

Proposal No. 5

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

Summary of Discussion
For the purpose of eradicating illegal online behavior, there was little certainty that corporate ladder information would provide data necessary to do so.

Proposal No. 6

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

Summary of Discussion

a. This is agreeable.
b. This is agreeable.
c. There was general agreement that this would be difficult and is an unreasonable ask, as it is asking registrars to, in effect, dissuade their own customers' confidence in their stability.
d. Should be amended to "change in controlling ownership." Note, however, that this may be duplicative since a notifcation to ICANN of a change in "Controlling Interest" is required in the 2009 RAA under section 5.9.2
e. Perhaps corporate criminal convictions could be reported to ICANN, but publishing such data on registrar websites is not reasonable and may violate privacy laws. Furthermore, official findings by non-criminal regulatory bodies could be reported, to ICANN, as well.
f. This is impractical, as most civil actions have little to do with combating online crime.

An ICANN board member was present and indicated that ICANN would not, at present, have the operational capacity to collect and manage this data. This proposed amendment would need more discussion.

Generally, the requirement to publish points c) to f) on the registrar website was seen as unnecessarily harmful to the registrar business without positively impacting the cybercrime issues, while a) and b) were seen as redundant with the current RAA.

Proposal No. 7

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

Summary of Discussion

This is redundant, as ICANN requires this during the accreditation process.

Proposal No. 8

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.

Summary of Discussion

Such an amendment would work if a notice / cure period were added to the provision. There also needs to be additional clarity on the definition of "liability." The "reseller" term needs specificity as registrars employ resellers for multiple services. It was suggested that any liability be limited to cases where action was not taken within a reasonable time period following notification of the registrar.

It was discussed again that ICANN is not equipped to maintain the proposed list of resellers, and would therefore be out of compliance with the RAA.

Proposal No. 9

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

(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:
(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.

Summary of Discussion
Registrars did not question the spirit of what is trying to be achieved here. However there are questions about the details that would be collected. In fact, collection of data is one issue—storage of that data is another, and its transmission is yet another. Data transmission and storage of data not needed to provide the service often run contrary to EU privacy laws. A time limit for data storage would be useful.

Care should be taken with definition of "securely." Credit card data may need to be stored in a separate location. The room was unsure if this can be technically accomplished at a level that LEAs need.

Proposal No. 10

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

(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

(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.

Summary of Discussion
There was broad agreement in the ultimate goal of this proposal but an acknowledgement that the economic, operational and technical challenges would be great. Also, and equally importantly, against what data would registrars validate, and how would it be secured without violating privacy laws?

Proposal No. 11

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

- 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).

Summary of Discussion
There was agreement in the room on this proposal.

Proposed No. 12

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

Summary of Discussion
The difficulty with this proposal is how to define a penalty for not meeting the SLA. There was no objection to the concept, however.

Next Steps: Near-Term

Registrars and law enforcement agree to move forward with the following in the near term:

- Registrars to publish on their websites a valid physical address for receiving legal service
- Registrars to publish a contact for handling abuse complaints
- Contracted parties and law enforcement to continue meeting and discussing additional outcomes and most effective and practical method to achieve them (which may or may not entail RAA amendments)

Next Steps: Longer Term

- Agree with ICANN on parameters for enhanced due diligence for accreditation of registrars
- Develop template process for LEA to document and provide evidence of improper online behavior in the relevant country and according to the applicable national laws on which registrars can reasonably rely and act.
- Create a method for verification of identify of law enforcement contacting contracted parties requesting action.
- Adoption of the CICILE LEA database

A word about process

Registrars have heard that they are resistant to needed changes. However, registrars want to emphasize that they are seeking the most effective means to assist the community without needlessly disrupting their own operational stability.

The most effective step toward getting the assistance of registrars is to approach them and describe a problem and discuss ways to address it. Such a process will intelligently inform everyone involved as to the best path forward, and will prevent frustration by others when registrars helpfully point out the possible operational shortcomings of proposals.

In this instance, dialogue with registrars began following LEA proposals and their endorsement by the GAC and others. Registrars understand the current impatience of the community; however, it is better to directly address the operational issues now, when there is an opportunity to ensure thoughtful and correct execution, than risk further frustration later if policies are not adequately vetted.

Thanks

Registrars, registries and LEAs extend their heartfelt thanks to the European Commission for their hospitality and generosity in providing a forum for the productive and collegial discussions over the past two days.