ONG DERECHOS DIGITALES

ONG Derechos Digitales es una organización no gubernamental cuya misión es promover la defensa y protección de los derechos fundamentales en el entorno tecnológico.

July 19, 2012

Dr. Steve Crocker, Chair of the ICANN Board
Akram Atallah, interim ICANN CEO

For your consideration:

ONG Derechos Digitales is a Chilean independent non-profit organization focused towards the defense, development and promotion of fundamental rights in the digital environment.

The purpose of this letter is to express our concern on the personal data issues related with the draft for a "*Registrar Accreditation Agreement*", dated June 3, 2012; and the negotiation status of the Law Enforcement Recommendations, as reflected in the document called "*ICANN's Summary of RAA Negotiations to Address Law Enforcement Recommendations As of 3 June 2012*", because both contains several provisions that puts information privacy and freedom of expression at stake.

1. Summary

Personal security and freedom of expression have a close relation with privacy. Obligating registrars to provide personal data of the domain holders or administrators without basic limitations, such declaring a legitimate interest or disclose identity of who requests, will give tools to authoritarian governments, Internet bullies and abusive intellectual property plaintiffs to pursue illegitimate objectives, becoming a major deterrent for activists, artists, and startups to use the domain registration system.

2. RAA Analysis

The 3.3 provision, obligating registrars to grant "*Public Access to Data on Registered Names*", is not consistent with the international data protection principles reflected, among other several instruments, in the European Union Data Protection Directive, the OECD Personal Data Principles, and our Chilean Personal Data Protection Law.

The 3.3 provision of the Registrar Accreditation Agreement draft obligates the registrar to provide an interactive web page and a port 43 Whois service providing **free public query** concerning all active Registered Names sponsored by Registrar in any gTLD. The data accessible shall consist, unless otherwise stated by ICANN, the following elements (3.3.1) :

1. The name of the Registered Name
2. The names of the primary nameserver and secondary nameserver(s) for the Registered Name
3. The identity of Registrar (which may be provided through Registrar's website)
4. The original creation date of the registration;
5. The expiration date of the registration;

@| ONGDERECHOSDIGITALES
DIAGONAL PARAGUAY 458, PISO 2
CP. 833 0051 / SANTIAGO DE CHILE
FONO: +56 2. 632 3660
FAX: +56 2. 632 3660
WWW.DERECHOSDIGITALES.ORG
INFO@DERECHOSDIGITALES.ORG

6. The name and postal address of the Registered Name Holder;
7. The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name
8. The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

Also, 3.3.3 states that the Registrar may subcontract its obligation to provide the public access described in Subsection 3.3.1 and the updating described in Subsection 3.3.2, provided that Registrar shall remain fully responsible for the proper provision of the access and updating. Both the personal data disclosure obligation and the subcontracting faculty given to the registrar are **not consisting with basic personal data protection principles, as it mentioned**.

Regarding the first issue -personal data disclosure obligation-, **data referred in numbers 5, 6, 7, and 8 undisputedly falls under the category of personal data, because it is information relating to an identified o identifiable individual**[1]. Once a database holder or controller is able to collect, process and, as in this case, disseminate personal data, it must follow some basic principles, which are common to UE directives, OECD guidelines, and most countries personal data protection laws. Also, the holder or controller has to ensure that third parties will not be able to go against those principles.

Data protection principles mentioned before (following OECD guidelines) are, among others, the Collection Limitation Principle, Purpose Specification Principle, Use Limitation Principle, and Security Safeguards Principle. All of these principles are compromised by the current RAA draft, because it does not contain effective safeguards regarding the way that personal data will be collected and processed by third parties.

In fact, with this provisions any third party will be able to collect personal data about the domains' owners and contacts without restrain, creating problems regarding the core principles of data protection and giving anyone the chance to collect and process personal data of the previously mentioned people without their consent.

Also, the 3.3.5 provision states the following:

"*In providing query-based public access to registration data as required by Subsections 3.3.1 and 3.3.4, Registrar shall not impose terms and conditions on use of the data provided, except as permitted by policy established by ICANN.*"

This provision is given without any consideration to national or international regulations regarding information privacy. The only exceptions in that provision are related with preventing spam and system overload, but they are established in highly narrow terms.

In the 3.3.6 provision, the RAA set conditions to provide bulk access to the data subject to public access, establishing terms and conditions that insufficiently address information privacy issues, providing only spam, automated queries, and a basic "do-not-sell" provision regarding selling and redistribution of data, but lacking any consideration to other privacy problems, as the disclosure, processing, or second uses of personal data.

The only way the RAA refers to national and international regulations, is through the 3.3.8 provision, but only establishing a general rule stating that:

[1] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, defines "personal data" as any information relating to an identified or identifiable individual (data subject), and similarly does the EU Directive on Personal Data Protection, the APEC Privacy Framework, the United Nations Recommendations on Data Protection, and our domestic Chilean Personal Data Protection Act.

"*ICANN may from time to time adopt policies and specifications establishing limits (a) on the Personal Data concerning Registered Names that Registrar may make available to the public through a public–access service described in this Subsection 3.3 and (b) on the manner in which Registrar may make such data available. In the event ICANN adopts any such policy, Registrar shall abide by it.*"

This rule does not contain any real or substantive restriction, and merely refers to possible ICANN policies on personal data.

3. Concrete proposals

- The WHOIS databases system should not have public and massive access to personal data such as names, addresses, phone numbers, e-mails or P.O. boxes. National laws and international treaties protect that data by setting forth high standards to access and processing personal information.
- Those standards are incompatible with public disclosure of personal data by Domain Name registrars. The RAA **shall add provisions regarding the disclosure and second uses of personal data of the domain owners, administrators, and technical contacts**.
- Also, the RAA **shall state clearly that that at least, information will be accessible only by a justified request and providing the identity of the party who's making that request**. **In a ideal scenario, information should be accessible only to public officers through a court order**. Latter information shall be kept on records by the registrar in order to allow access from law enforcement agents or the personal data owner, to take action if somebody incur in some personal data breach or infraction.

Francisco Vera Hott, vice-president
ONG Derechos Digitales