In response to the recent considerations regarding the proposed rules governing companies that provide WHOIS privacy services (as set forth in the Privacy and Policy Services Accreditation Issues Policy document), the **Association for Technology and Internet** (www.apti.ro)**, member of EURALO,** would like to submit the **following comments expressing our firm stance against the proposal, which presents a serious danger to freedom of speech, privacy and even to the rule of law on the Internet.**

As an association promoting free speech, privacy, and freedom on the global Internet we voice the following concerns, **urging ICANN to reject the proposals still in contention** for the following five major reasons:

1. Extra-judicial enforcement at the behest of Law Enforcement Authorities

From the Report on the Conclusion of the 2013 Registrar Accreditation Agreement Negotiations, it is clear that Law Enforcement Authorities (LEAs) have been pushing for measures which are damaging both from a human rights perspective and from a rule of law perspective. To be more precise, in the issue chart on privacy/proxy services, which begins on page 15 of the document, it is said:

- item 1.6 *"Publication in WHOIS in instances of illegal conduct"* states *"Registrants using privacy/proxy registration services will have the contact information of the customer 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"*
- item 6.2 *"Restrict Proxy/Privacy Services to only non-commercial purposes"* states *"If proxy/privacy registrations are allowed, the proxy/privacy registrant is a private individual using the domain name for non-commercial purposes only"*

Both of these items are carried on to this consultation document in sections 1.3.2 and 1.3.3 respectively in the following form:

- in section 1.3.2, under the *"On Disclosure and Publication in relation to Requests by LEA and other Third Parties other than Trademark and Copyright Owners"* heading, the most problematic being item #2 *"Should there be mandatory Publication for certain types of activity e.g. malware/viruses or violation of terms of service relating to illegal activity?"*, which would transform the privacy/proxy service providers into an arm of LEAs and would force them to take measures against clients without the intervention of the courts. This is bound to have serious consequences because this application of extra-judicial authority is going to have a damaging effect on the people's respect for the law and their trust in their registrars and, by extension, in ICANN and the Domain Name System. Item #4 from the same list *"Should a similar framework and/or considerations apply to requests made by third parties other than LEA and intellectual property rights-holders?"* is just as problematic, if not even more so, because it would open the door to expanding

this extra-judicial regime to requests coming from an open list of sources, not just LEAs and the copyright industry.

- in section 1.3.3, item #1 "*Should registrants of domain names associated with commercial activities and which are used for online financial transactions be prohibited from using, or continuing to use, P/P services? If so, why, and if not, why not?"* is the core issue, which is going to be argued against in the following sections of this document.

Furthermore, both these LEAs-requested measures are then exploited by the copyright industry at the expense of everybody else.

2. Vague terms and definitions for commercial websites

The proposed provisions limit the availability of privacy & proxy services to individuals only, denying this service for organizations. We underline there are actors such as political groups, religious organizations, ethnic groups, gender orientation groups, and others engaged in freedom of expression activities which are in immediate need for protection. Consider this example of the transgender community as illustration of one of the situations where privacy protection is highly needed.

Furthermore, we note that the proposal refers to commercial sites. However there is ambiguity regarding the definition of commercial sites. For example would an NGO selling personalized merchandise be regarded as a commercial website? How about a humanitarian website asking for donations? Or a website selling advertisement space? (which has recently been ruled as a commercial site)

Moreover, we strongly believe that the purpose of a registered domain name (commercial or noncommercial) should not be a criteria for establishing rules governing the availability of privacy/proxy services. One of the reasons is that it is not within ICANN's remit to decide what is a commercial activity and what not. Another reason is the fact that such a practice will be unfair and discriminatory for vulnerable groups, organizations and entrepreneurs who wish to exercise their right to freedom of expression on the Internet.

3. ICANN's anti privacy domain registration - the new SOPA

We urge ICANN to resist calls to impose new copyright and trademark enforcement responsibilities. Refusing private domain name registrations for reasons of copyright means giving up to the pressure put by various copyright holder groups such as MPAA, which is well known for its persuasive lobbying activities. In the eye of the public, the adoption of an anti-privacy domain name registration scheme will not only be regarded as a violation of human rights but also as compromising on the core values of the Internet in order to placate the

powerful copyright industry. Consequently, ICANN will lose credibility and trustworthiness and, as it has been witnessed throughout history, appeasement is not a winning strategy anyway.

In addition, we highlight that the arguments of the copyright industry - needing the DNS to shut down copyright infringing websites - are completely inappropriate in the digital society, where the sharing model has become the social norm and where governments adopt strategies for opening up content for various purposes (for reference see the Open Education Resources movement at UNESCO and European Commission initiatives).

Moreover, for example in the United States, the copyright holders can easily obtain a DMCA subpoena for identifying the alleged infringers. For reference, this is a practice which is already used by RIAA (the Recording Industry Association of America).

Furthermore, worldwide, the different intellectual property laws have their own particularities, and enforcement activities pose complicated issues - differing from country to country. For example, specific IPR enforcement activities could lead to interim blocking measures that could prove to have no basis in a court trial (see the case of rojadirecta).

Thus, we emphasize the fact that there are sufficient legal means and competent authorities for copyright holders to exercise their rights. The domain name industry should not be asked to play any part in policing the Internet by being forced to suspend Internet domain names based on accusations of copyright or trademark infringement by a website. **Such measures would impose the same obligations that the highly contested Stop Online Piracy Act (SOPA) contained in 2011.**

We acknowledge the fact that ICANN develops policies for accredited registrars to prevent abuse and illegal use of domain names, but we strongly believe that this is not the way to go. ICANN should not step out of its mandate to judge on content, website blocking or human rights.

4. Privacy and anonymity are fundamental for the open use of the Internet

There are a number of very good reasons why the use of the Internet should optionally remain anonymous or, at the very least, quasi-anonymous, and these reasons largely have to do with protecting freedom of speech or with ensuring data protection of individuals and whistleblowers.

Limiting private domain name registrations is disproportionate and unjustified because the risks to which website owners will be subject to (for example harassment, intimidation and identity theft) are far greater than serving the purpose of identifying few illegal websites - for which there are already several redress mechanisms in place. Moreover, there are certain situations (for example in family and witness protection protection programmes) where privacy

and proxy services represent a useful and justified tool for maintaining anonymity, being thus *in support of law enforcement activities.*

Furthermore, law enforcement statements suggesting that *"if an entity is engaged in legitimate business activities, then a proxy service should not be necessary"* (Chapter 6, subsection C, *Report on the Conclusion of the 2013 Registrar Accreditation Agreement Negotiations*, page 26) does not represent a valid argument since a website engaged in legitimate commercial activities (such as selling parody publications and merchandise in a country under an oppressive regime) may want to opt for proxy services as well. It has also been suggested that criminals use proxy and privacy registrations to hide their identities, however, **illegal uses represent a minority of cases and privacy registrations do not contribute to a wide-spread criminal behaviour**. On the contrary, privacy registrations have a great **potential to bring positive results for society** since sensitive information (for example in corruption cases) can safely be revealed without repercussions. Therefore, such valuable uses of the proxy/privacy registrations should not be left out of considerations.

To underline the importance of privacy/proxy services even more, we highlight the fact that **the vast majority of domain owners are not criminals, so why put *everyone* at risk just for catching *few* perpetrators?** This measure is disproportionate and unjustified and it resembles the deeply flawed reasoning behind adopting mass surveillance decisions. The quotation of the Blackstone formulation is appropriate here: *"It is better that ten guilty persons escape than that one innocent suffer"*, which is a principle closely related to the presumption of innocence, which, in turn, is one of the cornerstones of any fair criminal law system.

This measure will definitely fail any European Union privacy impact assessment test, thus a large proportion of Internet users would be striped unlawfully of one of their fundamental rights.

Moreover, given the differences of the privacy laws worldwide, it should be acknowledged that not all persons have the possibility to turn to national laws for removing personal information from the WHOIS registry (as it is possible under the laws of the European Union member states implementing Directive 95/46/EC).

Thus, on a general note, we underscore the need for greater confidentiality and privacy in the WHOIS directory and ask ICANN not to transform itself into the Internet's police agency. Moreover, we draw attention to the fact that **the lack of clear and efficient privacy oriented rules will contribute to the opposite phenomenon in terms of ICANN's Affirmation of Commitments relating to 'timely, unrestricted and public access' to WHOIS data** since people will start to declare inaccurate or false data upon domain registration (consequently even law enforcement agencies obtaining a warrant or subpoena for receiving registrant data will waste resources on a wild goose chase).

Therefore, privacy protection is not infringing upon the right to receive accurate and complete WHOIS data because the proposed privacy restrictions give birth exactly to the counter-phenomenon, feeding in more false, unavailable and incomplete WHOIS data.

5. The proposal violates ICANN's bylaws and the Internet's core values

The proposal closes up the free and open use of the Internet. Certain categories of people will be left with no guarantees that their message will be delivered without abuses and repercussions. Website owners with less popular content (or presenting dissident views) will fear from becoming easy targets. With their sensitive data displayed in the public registry, more and more people will refrain from making their voice heard online. **Self-censorship is not going to contribute to a free and open Internet.**

Moreover, it is clear from Steve Metalitz' testimony that the US entertainment industry is going to use this data for suspending, blocking or shutting down websites. All of these activities do not correspond to the principles ICANN has set for itself in its bylaws and they do not help promote a safe, reliable, healthy online environment.

6. Conclusion

It is our belief that adopting this policy comes at the cost of human rights, especially freedom of speech and privacy, and that it would be contributing to the fragmenting and the closing down of the Internet, which would be contrary to the longstanding values of ICANN. In other words, by adopting this policy, ICANN would not only prove to have become the puppet of the copyright industry and the aide-de-camp of law enforcement bodies, but would also fail to achieve its mission and goals and abide its own bylaws.

Considering all these issues, we urge you to abandon this initiative and continue to provide full privacy protection to domain name customers.