**Annex 1**

**Statement on the Threats under a ‘Thick’ Whois Model**

**11 February 2013**

This statement is intended to enumerate imminent threats to privacy and data protection if Thick Whois is implemented for all TLDs. It should be read as an annex to the previously submitted NCUC statement. This annex is intended to provide additional clarification to all members of the ‘Thick’ Whois Working Group, the Privacy and data Protection Sub-Group, and the GNSO.

It is noted that the issues surrounding privacy and data protection are difficult and longstanding. To rush thorough their consideration would be counterproductive. The very first consideration to keep in mind is that the WG recommendations to the GNSO Council will initiate a policy requirement of 'thick' Whois for all incumbent gTLDs.

The following ten issues demonstrate the importance and necessity of this discussion:

**Issue #1: This discussion is mandated by the charter of this Working Group.**

The Working Group, as stated in the charter, “is tasked to provide the GNSO Council with a policy recommendation regarding the use of ‘thick’ Whois by ***all gTLD Registries, both existing and future***. As part of its deliberations on this issue, the PDP WG should, at a minimum, consider the following elements as detailed in the Final Issue Report…

Impact on privacy and data protection: ***how would ‘thick’ Whois affect privacy and data protection, also taking into account the involvement of different jurisdictions with different laws and legislation*** with regard to data privacy as well as possible cross border transfers of registrant data?”

**Issue #2: Thick Whois Model has the potential (if not already) to be considered in direct violation of European Union Law.**

Privacy as a human right is firmly rooted in multiple international instruments and recognized in the constitutions and other legal acts of many nations. This annex notes that, at present, the most rigorous regulations on personal data protection are implemented in Europe. Thus, this is the high standard that most become the guiding principle. Regarding the international flow of personal data, the vast divergence between nations requires a suitable compromise.

The 1995 EU Directive on data protection continues to regulate the collection, processing and transfer of personal data within the EU. While the transfer of data is important, the EU has established a mechanism which addresses the export of data. Article 25 (the key article relevant to this issue) stipulates that member states should allow transfer of data to a third country only if that third country ensures an adequate level of data protection. Article 29 Working Party (see attached documents) notes this long lasting issue in their official comments. Since the EU policy has been incorporated in numerous non-EU legal systems, the process may introduce further violation of those laws through a model binding registrars, which in turn could force them to violate national laws or force them out of business.

**Issue #3: A continued, clear violation of article 25 of the EU Data Protection Directive with all of its consequences.**

Should the “thick” WHOIS policy be enforced for all registrars they will be in violation of EU data protection laws and EU states will therefore not be allowed to share data with them. A continued violation of article 25 of the EU Data Protection Directive would bring as a consequence no access to EU data for registrars in states where the “thick” WHOIS contracts are enforceable to avoid the circumvention of national laws.

Thus, a threat of violating EU data protection laws would mean that EU states would not be allowed to export EU data to countries that cannot guarantee equal level of protection.  This in turn, will have an impact of businesses and their customers.

**Issue #4: Thick Whois information is constantly abused.**

This issue is a direct quote from the experts in Article 29 Data Protection Working Party: “The problem of inaccurate contact details in the WHOIS database cannot be solved without addressing the root of the problem: the unlimited public accessibility of private contact details in the WHOIS database. It is a fact that these contact details are being harvested on a large scale and abused for spamming. In other words, the way the system is designed provides a strong incentive for natural persons to provide inaccurate contact details. Regrettably, ICANN has decided not to work on alternative layered access models, such as the OPoC model repeatedly proposed as proportionate alternative by the Working Party.” (See attached document.)

It would be advisable to also incorporate the Whois Misuse Study requested by ICANN and being conducted by the Carnegie Mellon University Cylab expected to have initial results in mid-2013.

**Issue #5: Thick Whois information is a threat to individuals in oppressive nations.**

Who owns the data is as important as who controls it. Setting aside the legitimacy as to why Whois data is public, the transfer of 100+ million entries of data (such as in *.com*) is hardly a simple matter, and one not comparable to *.org* (which originally only transferred 3 million entries) or any other domain. Indeed, the PDP will decide on the fate of people lives. While information is now protected in some cases by national laws, this protection will be lost.

The transfer process would have to be refined to avoid the imminent danger to consumers. There is great risk for potential misuse of this information. In the end, control of transfer must reside with the individual registrant.

**Issue #6: Existing Safe Harbor Agreements are ineffective.**

While there are Safe Harbors Agreements in effect between EU and US, Non-US registrars obliged to abide by a new ‘thick’ WHOIS will not be able to benefit from this arrangement. Their very introduction was a challenging compromise for both parties. Introducing new ways of violating the current data protection arrangement will only intensify the conflicts within this discussion. (See attached document.)

**Issue #7: Beneficial purposes do not in itself legitimize the collection and processing of personal data for other purposes.**

Article 29 Data Protection Working Party has also been clear on this issue, and the following statement sections are quite clear:

“The fact that WHOIS data can be used for other beneficial purposes does not in itself legitimize the collection and processing of personal data for those other purposes. The Working Party finds the proposed new requirement to annually re-verify both the telephone number and the e-mail address and publish these contact details in the publicly accessible WHOIS database excessive and therefore unlawful. Because ICANN is not addressing the root of the problem, the proposed solution is a disproportionate infringement of the right to protection of personal data.”

“This proposed new requirement does not stem from any legal requirement in Europe, but again, is explicitly introduced by ICANN to accommodate wishes from law enforcement. The Working Party strongly objects to the introduction of data retention by means of a contract issued by a private corporation in order to facilitate (public) law enforcement. If there is a pressing social need for specific collections of personal data to be available for law is up to national governments to introduce legislation that meets the demands of article 8 of the European Convention on Human Rights and article 17 of the International Covenant on Civil and Political rights.” (Regarding these international instruments, please see prior NCUC statement.)

“Since the registrars (both within Europe and worldwide to the extent they are processing personal data from EU citizens) are data controllers (responsible for the collection and processing of personal data), the Working Party is concerned that this new obligation will put them in the uncomfortable position of violating European data protection law. The Working Party would deeply regret a situation where data protection authorities were to be forced to enforce compliance…”

“The Working Party has on several occasions expressed an interest in being consulted by ICANN about privacy-related WHOIS issues. We repeat that we are ready to discuss any issue that ICANN feels would be useful in relation to the application of EU and national data protection legislation in respect of WHOIS services and would appreciate it if the relevant ICANN staff would contact the Working Party to ensure that ICANN has a full understanding of the concerns we have expressed.”

This PDP may benefit from contacting the DHS Data Privacy and Integrity Advisory Committee (under the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues) for advice in this matter. The committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. section 451.

**Issue #8: The New Registrar Accreditation Agreement has already accommodated the wishes of law enforcement.**

The new RAA will include robust data retention requirements. In this context, data and privacy protections should be in keeping with ICANN’s plans to set up a Registrar Code of Conduct Process to require certain terms to be followed by all Registrars, regardless of whether they operate within the 2009 RAA or the new one.

**Issue #9: The example of *.name* has to be considered.**

While ICANN has required registrars to make Whois data publicly searchable, for this domain special rules where negotiated by Global Name Registry, the original administrator of the domain, which acquired the right to set up a tiered level of access within "Whois II.

**Issue #10: It must be considered a possibility that *.com* and *.net* may have to remain within the “thin” model.**

These are considerations that must be considered satisfactorily, regardless of what the WG may find, and even if it involves financial considerations.

Finally, this annex strongly suggests that all these issues have to be analyzed in consultation with a panel of experts. All of these considerations, taken together, open up ICANN to considerable liability.