Dear colleagues of the data protection subgroup,

This statement (which I submit as an individual with some input from our colleagues Avri Doria, Amr Elsadr, and Joanna Kulesza, a lawyer from Poland, and expert on European privacy and data protection laws) is intended to address a couple of observations made at our last meeting of March 20, 2013.

The NCUC statements previously submitted clearly showed the threats to human rights that exist within a 'thick' Whois environment. These observations, although acknowledged by the sub-group, have not persuaded most of its members. The ten issues subsequently presented by the NCUC have also been acknowledged, but also found not persuasive, or inapplicable. The reasons given have been based on two observations that I have noticed below. For the record, both observations are erroneous and totally irrelevant. Below I explain why.

Observation #1: There is no known record of a registrar's prosecution under data protection laws in Europe. At first impression, this statement looks easy enough. This observation relies on the old adage that "no news is good news." As we noticed, the data protection laws in Europe (and around the world) are evolving quickly, and in Europe in particular, penalties of heavy fines could be included within the new provisions. Nevertheless, there is a reason why there have not been any prosecutions of registrars. For an answer, we have to look at the numbers:

Of the 21 unrestricted gTLDs, only four have Registrars in Europe (plus one in Hong Kong), and you guessed it, all others are in the USA. This raises interesting questions. Could it be said that a 'thick' Whois environment would potentially eliminate border restrictions under a unified database? Could it be said then, that now US-based Registrars, and others, may be found within the EU jurisdiction for purposes of prosecution? The statement by the new CEO of ICANN, Mr. Fadi Chehade, is illuminating (see attached his letter to the EU Article 29 Working Party).

While I am not oblivious to the needs of law enforcement, the rules are not applied equally around the world. While, for example, it could be said that in the USA, Canada, and Europe, citizens may depend on law enforcement for protection, this is not the case in other parts of the world. This is no secret and has been documented extensively. (See report from Freedom House.)

In short, Mr. Chehade, statement notes that Registrars based in the European Union could be exempt from the Whois verification requirements currently under our discussions; and more important, it seems that the GAC is also in agreement. Thus, in the end, there would not be, apparently, a unified 'thick' Whois database for all registrars. This would bring us back to the first question: what about US-based Registrars? Even if there have not been cases reported yet,

European registrars continue to be bound by European law. Just because they have not been prosecuted yet, does not mean that registrants do not have their rights to privacy as defined by their national laws. The issue is a loss of rights, not of changed practice.

Observation#2: There is no difference to the vulnerability between what is available in 'thin' versus what is made available in 'thick.'

A member of the sub-group stated that in the past, the majority of Whois data had become widely available in cyberspace (and effectively within the reach of spammers and such). If by this statement, we are referring to VeriSign, then this fact would be irrelevant. To follow that reasoning, we would have to assume that the reason why all this Whois data is floating around is not because of VeriSign's thin' model, but potentially likely because of the 'thick' models by which the registrars operate (both in and outside of the USA). To educate all members of the WG, it would be great if we could read an official report that demonstrates the vulnerabilities of 'thin,' the circumstances surrounding the assembly of the report, and the agency that conducted it. I find it difficult to understand, how 'thin' would be more vulnerable than 'thick.' A Whois record contains all of the contact information associated with the person, group, or company that registers a particular domain name. Typically, the record would contain information such as the name and contact information of the Registrant, the name and contact information of the registrar, the registration dates, the name servers, the most recent update, and the expiration date. Why would that be the case in a 'thick' Model that provides more details?

In any case, it seems that most members of the sub-group favor the observation that "there was no difference to the data and its vulnerability between what is available in 'thin' versus what is made available in 'thick.' This particular observation is confusing because its premise is inaccurate. For example, the argument that consumers agree to the "terms" of Whois is not relevant to our discussion. We would have to look at whether consumers have realistic choices in the first place. Agreeing to terms without any other choice (except not doing business in the Internet) is not really a choice. Rather than going down that tangent, why not avoid that problem and instead offer consumers the maximum protection possible from the very beginning? That is, providing a Whois system that ensures privacy and data protection as it is defined in the national and local laws of the registrars. For all other considerations, see comments to observation #1. If privacy cannot be guaranteed, then 'thick' Whois will never be a real choice for consumers.