The EWG Use Cases Seem Fundamentally Flawed:
How are the Use Cases Justified and How do they fit within the Scope and Mission of ICANN and How have these Cases Been Measured Against Due Process and Practices in other Fields?

After years of debating the need to narrow access to the Whois, we in the NCSG are shocked to find an array of "Use Cases" that seem tantamount to giving everyone everything they have ever wanted.

We respectfully submit that we do not understand the Use Cases developed by the EWG: what were the limits set? What rigor in the analysis? How do the "Use Cases" fit within the limited and narrow scope and mission of ICANN? How do the Use Cases fit within traditional practices and protections for the owners and providers of the data?

For example:

a) Why is an individual entitled to find the physical location of a domain name registrant? What law gives an individual the right to track down a Registrant for purposes that may include stalking, harassment and intimidation?

   The physical dangers are very clear, but the benefits are not. The only answer given by a EWG member to date is that Internet users should be allowed to find the locations of the vendors with whom they are doing business. We note that only the smallest of subsets of domain name registrants are engaged in business-to-consumer transactions, and that these interactions with the Amazons, Facebooks, and Estee Lauders of the world are regulated closely by local and national regulators.

   ICANN is neither a business regulator nor a consumer protection agency. The Whois and any related new set of data is not a substitute, replacement or proxy for the work of governments in protecting consumers. Governments can and do mandate what data must be made available on the websites of entities selling goods to the general public. Governments can and do educate consumers to

deal only with entities they know online and that have complied with the legal requirements of disclosure and presentation.

This is content outside the scope and mission of ICANN. We are not a content regulator; we are not a consumer protection organization; and we know something more: that domain names need not be used for websites, but for listservs, for email addresses and more. The vast majority of domain names provide ideas, but not necessarily websites or content for the general public.

Yet, the risks of validating them and making the physical location of all registrants available to any "Individual Internet User" threaten far more than assist, and harm far more than help. They could lead to harassment, stalking, physical harm, psychological harm, and unnecessary threats to ideas and communications. **The Internet users who should be protected here are the Registrants.**

b) Domain Name Research – the availability of Whois data for domain name research seems to have some validity if provided in the aggregate and via some type of statistical sampling without personal data associated. But to allow a Researcher access to "Specified Registrants" with Contact and Specific Historical Data strains credulity, and threatens individual Domain Name Registrants.

c) Legal Actions -- Unfortunately, lawyers are the butt of jokes in many societies around the world. When asked why, lawyers note that they are mocked, but feared. The lawyer code of "zealous advocacy" generally requires the single-minded pursuit of the clients' goals – regardless of the merit, the fairness or even the truth of the matter. Accordingly, lawyers intimidate, threaten, browbeat, and sue (with and without adequate grounds). That is their/our job.

But societies with lawyers protect against their abuses. For example, to attain the identity of a "John Doe" (an unidentified person in a chatroom), lawyers may not merely made an allegation of wrongdoing or breach, he/she must file a lawsuit, show a justified legal claim and affirm they will

not misuse the data/identity when disclosed. If the conditions are met, and the disclosure made, the attorney's actions are monitored by a judge or magistrate for protection of the John Doe.

Similarly, sanctions threaten frivolous lawsuits by attorneys which would sap the time, money and energy, particularly of smaller defendants. Further, due process rules help level the planning field by ensuring that parties large and small, represented and not, have the time and notice needed to prepare and ready themselves for legal steps.

The high reputation of a the members of the Trademark Bar in ICANN notwithstanding, the mere proof of being a lawyer and the mere allegation of a legal problem is never enough to cause a defendant to lose rights, privileges and protections. It cannot be here.

c) UDRP cases?

Obviously a Registrant to a UDRP domain name dispute case must receive notice of the case (and it can be provided by his/her Registrar), but why should his/her name, location and contact information be disclosed? The UDRP is a virtual tribunal in which all proceedings pass by email. Physical locations are irrelevant; identity of the Registrant is irrelevant (except as disclosed through actions online or in other forums).

Domain names can be taken down and transferred without exposing the Registrant to other forms of wrath and retaliation by the trademark owner and the personal wrath of the party seeking the takedown.

d) Business Domain Name and Sale

Some country codes have looked at the purpose of domain name use – and limited access to Registrant information. A potential buyer of domain names is not entitled to any information that the domain name registrant does not choose to provide. By way of comparison, what potential buyer of a house would have the right to come onto the property, harass the home owner and seek the history of repairs to roofs and furnaces ***prior*** to

an indication the homeowner wanted to sell, and before any steps taken by the home owner to entertain the offer of that particular buyer?

Similarly, uninvited potential purchasers of domain names have no rights to Whois data – and certainly no unique rights to data about the Registrant, Registration History, or contact information or anything else. All information can and should come through the Registrant – if and when he/she/it is interested in selling.

e) Abuse Mitigation and Malicious Activities.

For years, registries and independent third parties have been studying malicious activities online and taking down domain names without any need to disclose or even contact the registrant. Such disclosure of registrants should not be routine, but subject to the legal and law enforcement process of investigation, and appropriate subpoenas and warrants.

We respectfully submit that the Use Cases are strained – too much disclosure with too little process and far too little protection for the Domain Name Registrant. Such a "wish list" of uses should not be further entertained by the EWG. A far better alternative is to limit the data in whatever Whois/Directory databases are to follow – provide a contact for technical questions, delete physical location (which can still be found through the Registrar likely subject to the appropriate jurisdictional protections for the Registrant), and delete the numerous additional fields being added.