

August 22, 2013

Jean-Francois Baril
Lead Facilitator
Expert Working Group, gTLD Directory Services
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA
Via E-mail - input-to-ewg@icann.org

Re: EWG Report on ARDS

Dear Mr. Baril and the Members of the Expert Working Group on gTLD Directory Services:

The International Anti-Counterfeiting Coalition applauds the efforts of ICANN and of the Expert Working Group (“EWG”) to grapple with the numerous and substantial deficiencies with the WHOIS database that have developed since responsibility for the database was first assigned to ICANN. The comprehensive evaluation represented by the EWG and its Initial report on a proposed Aggregated Registration Directory Service (“ARDS”) is a quantum improvement over the piecemeal approach adopted thus far by different PDPs and working groups within the ICANN universe.

Several of the EWG’s proposals are welcome and overdue. In particular its proposals for (i) a consolidated, centralized database with robust provisions to ensure data accuracy and currency; (ii) specifications for privacy protection/proxy services and (iii) “next generation” improvements intended to accommodate the expanded environment of multiple gTLDs operating with non-ASCII (IDN) script represent serious proposals which warrant aggressive attention by the ICANN community and its staff.

At the same time, however, the proposal is subject to a central, fatal flaw: the restriction of access to what has hitherto been unrestricted registration data.

While the IACC acknowledges competing privacy interests dictate a renewed analysis of data access, it cannot support steps to restrict access without more clarity on the data to which access will be restricted, the authentication required to secure access to classes of restricted data (specifically registrant data required to address illegal activity online) and, most important, responsibility for enforcing those new protocols.

In particular:

1. Absent specified and enforceable protocols governing circumstances under which non-public registration data can be accessed by interested actors with a legitimate need for data (e.g. trademark and copyright owners seeking to enforce their intellectual property rights), no change to the current levels of access should be made. First, such a change is at odds with commitments made by ICANN concerning its operation of the DNS. Second, past experience demonstrates that a “self-policing” mechanism relying upon the integrity of domain name registrants simply does not work. (A simple comparable is the failure of the .net and .org registries to ensure that

those top-level domains were restricted to the types of registrants initially contemplated combined with the absence of any responsibility for enforcement of those restrictions to ensure that violators would suffer consequences.) For all of the layered analysis in the EWG, the Initial Report is entirely silent on how any authentication process will work and what consequences follow from failure to reveal the robust, authenticated data when authentication has been established.

2. On a related note, the detailed and layered analysis subdividing Internet users into a number of different categories with differing levels of access is far too complex. First, many actors will necessarily fall within more than one category. Is the “gatekeeper” responsible for determining in which capacity a particular user is acting? Second, are so many variations strictly required to secure the privacy concerns at issue? In fact,
3. Restricted data fields often appear to have no correspondence to purported privacy concerns driving restricted data access. As one example, server data can be extremely helpful in an underlying investigation of intellectual property infringement – by drawing links between related businesses and infringing websites using the same server. Similarly, domain name expiration dates are helpful in making an economic assessment about whether to act or to suspend action pending possible domain name expiration. Neither data field implicates the privacy concerns purportedly driving the restrictions on data access described in the Initial Report. Both fields should be made fully and publicly accessible in the absence of any demonstrable privacy rationale for restricting access.

The IACC thanks ICANN for the opportunity to comment on this issue of key concern to its membership. With a membership composed of over 200 corporations, trade associations, and professional firms, and founded over 30 years ago, the IACC is the world’s oldest and largest organization representing exclusively the interests of companies concerned with trademark counterfeiting and the related theft of intellectual property. The members of the IACC represent a broad cross-section of industries, and include many of the world’s best known companies in the apparel, automotive, consumer goods, entertainment, pharmaceutical, and other product sectors. The IACC is committed to working with government and industry partners in the United States and abroad to strengthen IP protection by encouraging improvements in the law and the allocation of greater political priority and resources, as well as by raising awareness regarding the enormous—and growing—harm caused by IP violations.

We would welcome the opportunity to discuss our comments with you further.

Respectfully submitted,
on behalf of the International AntiCounterfeiting Coalition,

J. Andrew Coombs
Chair, Domain Name Working Group
IACC Internet Task Force
J. Andrew Coombs, A.P.C.