CAUCE North America
PO Box 727
Trumansburg NY 14886
E-Mail: secretary@cauce.org
13. Apr. 2011

ICANN
by electronic mail

We appreciate the chance to comment on the ICANN WHOIS Review Team Plan as announced at http://www.icann.org/en/announcements/announcement-04mar11-en.htm

CAUCE NA, as an all-volunteer Internet end-user advocacy organization established in 1998 has moved beyond its original narrow mission of encouraging the creation and adoption of anti-spam laws to a broader stance of defending the interests of individual Internet users. CAUCE NA is led by a combined Board with a cumulative century of experience in the field of Internet advocacy and technology.

Based on that experience, including experience directly engaging with ICANN in a variety of capacities, we would like to offer the following comments on your proposed whois policy review activities.

1. Whois Is A Critical Anti-Abuse Resource

Combatting Internet abuse without access to whois data would, in most cases, be difficult if not impossible. To paraphrase a common cliché, IP addresses and domains don't attack Internet assets, people attack Internet assets. We cannot pierce the veil and map IP addresses and domain names to those people without routine access to the crucial information whois data contains.

If whois were to cease to be routinely available, targets of serious Internet abuse will have no alternative but to employ lengthy legal process to compel disclosure of resource assignment and allocation information. This process is cumbersome, time-consuming and expensive, and benefits no one except the attorneys who will be involved in pressing or defending these actions, and the miscreants who will enjoy weeks, months, sometimes even years of anonymity in which to continue to conduct their abuse with impunity. *This abuse happens at internet speed; a slow response is effectively no response at all.*

2. Whois Needs To Be A True Production Service Offering

Currently whois is offered on something of a "hobbyist" basis, particularly in TLDs that use the “thin” whois model. At one provider it will use one format, while at other times and at other providers, it will use another. This lack of consistent formatting, along with restrictive access policies, makes whois access something that's only suitable for small scale interactive "craft" access rather than being a

production-ready and robust service that's appropriate for the volume of domains and other resources involved in today's domain name ecosystem.

If Internet abusers can script the creation of domains at arbitrary scale, but security teams and anti-abuse researchers are limited to some small number of manual whois queries per day, the abusers can obviously simply out-automate and out-scale us. *This enforced handicap represents bad public policy*.

Other technical ways that whois data access can and should be improved include:

- Whois data should be available via authenticated channels (or in a standardized bulk format) so that legitimate uses aren't thwarted by restrictive rate limits. (Authenticated access can and should be logged and audited to ensure that abuse is not occuring)
- Whois data should be structured in a consistent, standard format amenable to machine parsing. We believe that the *tag:value* form used by thick whois servers meets this requirement, so long as they continue to use a restricted and consistent tag vocabulary, and the definitions of each tag are available to the public — perhaps as an IETF RFC.
- Whois data should be aggregated and distributed from a central location using the “thick” model, rather than being distributed across hundreds or thousands of providers on a distributed "thin" model. This ensures both consistency and availability.

3. Whois Is a Community Resource

While law enforcement officers play a critical role in mitigating online crime, they are too few in number and too poorly funded to mitigate all online abuse. Much online abuse is handled by other entities, ranging from non-sworn government administrative agencies (such as the Federal Trade Commission here in the United States), to non-governmental organizations such as CAUCE NA or Spamhaus, to agents of aggrieved private parties seeking to protect their company's assets (including facilities, trademarks and intellectual property being used online in illegal ways).

If whois access were narrowly restricted to sworn law enforcement officers only, the "thin blue line" of law enforcement, important though it may be, will not be sufficient to maintain the status quo. *The security and stability of the Internet will be negatively impacted, with an associated loss of public trust and transparency.*

That said, we would not object if sworn law enforcement officers or civil investigators were offered *expanded* access to whois data, such as a routine ability to view an unfiltered version of whois data that is not encumbered by obfuscating private or proxy registration mechanisms — provided such access is authenticated, logged and audited to protect against arbitrary abuse and misuse.

4. Whois Data Must Be Meaningful

We have seen examples of whois data services that are present in name, but effectively of no value. For example, consider the data for chase-online-banking.com:

```
Domain: chase-online-banking.com
Registrar: Eurodns S.A.
```

```
Registrant:
Company:
Name: I P Freely
Address: 123 blowme lane
City: tacoma
Country: UNITED STATES
Postal Code: 98409


Administrative Contact:
Company:
Name: I P Freely
Address: 123 blowme lane
City: tacoma
Country: UNITED STATES
Postal Code: 98409
Phone: +012589636541
Fax:
Email: maiybs@gma.com

Technical Contact:
Company:
Name: I P Freely
Address: 123 blowme lane
City: tacoma
Country: UNITED STATES
Postal Code: 98409
Phone: +012589636541
Fax:
Email: maiybs@gma.com


Original Creation Date: 2011-04-04
Expiration Date: 2012-04-03


Status:
clientTransferProhibited
```

This entire WHOIS entry is *transparently* fraudulent. There is no “blowme lane” in Tacoma WA, no North American phone number starts with 01, and even if the zero were corrected as a typo, there is no 258 area code. The e-mail address is invalid, and even the simplest attempt to send a confirmation message would have revealed that mail to it is rejected.

If we see abuse involving that domain, which we have, there is no way to find an appropriate security or abuse contact.

It is nominally whois data, but it provides no information whatsoever about who or what that domain actually is. *This shows what whois can devolve to, if we as a community allow it to degrade without objection.*

We acknowledge that whois data, like any data, can potentially be abused. Not all whois data is equally at risk, however. For instance, we do not believe that an entity engaged in Internet commerce should have the same right to anonymity online that a political or religious dissident might require, and in fact, the customers of the Internet have a compelling right to know with whom they're doing business. *We therefore urge ICANN to eliminate whois anonymity as an option for corporations and other non-natural persons controlling Internet resources.*

5. Improvements To WDPRS and Whois Accuracy

When missing or inaccurate whois information is detected, users have the option of reporting that inaccuracy via the Whois Data Problem Reporting System (http://wdprs.internic.net/).

Unfortunately that system is operationally cumbersome, requiring domain-by-domain reporting via a web form, followed by email confirmations, even in cases where hundreds or thousands of domains share the same inaccuracies and the same registrar.

We understand that ICANN has a bulk WDPRS submission facility currently used by only a small number of high-volume reporters. That service should be made available, with suitable registration or other safeguards to deter abuse, to any entity submitting multiple WDPRS reports.

We also believe that the information WDPRS receives is not being appropriately leveraged to identify and address ongoing abuse. While WDPRS complaints may result in the correction of *individual* erroneous whois records, ICANN does not use that data to identify systematic problems, including potentially rogue ("bulletproof") registrars who make no effort at maintaining accurate whois data whatsoever — and may even treat whois inaccuracy and other violations of ICANN's rules as a competitive advantage.

Moreover, why is ICANN not sharing the substance of the community WDPRS reports it receives with community stakeholders? If there was more transparency about the reports received, consumer confidence in whois data accuracy would improve and we could even imagine a "PhishTank"-like model where community members could help to verify the reports that have been made via WDPRS.

We also believe that the costs associated with correcting erroneous whois data, particularly in the case of grossly and obviously inaccurate whois data, should be passed along to the registrar that has allowed that data to be accepted. Even the simplest of automated screening would easily allow many bogus point of contact data elements to be flagged at the time of domain registration; other types of online businesses have been doing this for years. Currently some registrars do not care if they accept bogus whois point of contact data, but if there were financial consequences to large amounts of invalid WHOIS, that could change.

Registrars that exhibit a clear and ongoing pattern of routinely accepting or failing to correct obviously bogus whois information should be subject to notice and breach proceedings under the registration agreement.

6. Adequacy of the "Key Definitions"

The Review Team also asked for feedback on the adequacy of the definitions it proposed at http://www.icann.org/en/announcements/announcement-04mar11-en.htm

In our opinion, the following adjustments would strengthen those definitions.

As written, definition 4.1 (Law Enforcement) does not distinguish between sworn law enforcement officers with criminal law enforcement powers (such as sworn federal law enforcement officers, sworn state police officers, sworn county sheriffs, and sworn municipal police officers here in the United States), and other entities incidentally included in an overly broad definition, including judges,

lawyers, prosecutors, private security officers, administrative investigators and even parking enforcement officers (so-called "meter maids") whose responsibilities include "maintenance, co-ordination, or enforcement of laws, multi-national treaty or government-imposed legal obligations."

We believe "law enforcement officers" should be defined more narrowly to be only those individuals who have:

1. been sworn or commissioned as a law enforcement officer by a government agency of competent authority;
2. who are charged with upholding the general criminal laws of an applicable jurisdiction, including having power of arrest;
3. typically have received specialized peace officer training (e.g., here in the United States such courses are typically offered by the Federal Law Enforcement Training Center ("FLETEC") or a similar program offered by one of the individual states, such as as Oregon's Department of PublicSafety Standards and Training Academy ("the DPSST Academy");
4. and who normally receive tangible official signs of their role such as a police uniform or official credentials (a badge and/or ID card).

In adjusting this definition, we do not mean to imply that ICANN should exclude non-sworn government officials from the scope of its work -- even though those government officials are non-sworn, they play an important role in enforcing applicable law via civil processes. They simply require a different label (such as "civil enforcement officer" or "administrative enforcement agent").

For example, here in the United States, while FTC investigators are not sworn law enforcement officers, they play an important role in compelling fair business practices using the civil enforcement powers at their disposal. They're just "investigators" and not "law enforcement officers" within the customary meaning of that term of art.

We also believe that ICANN should explicitly consider whether "law enforcement" includes those who may be members of national intelligence services, or a country or multinational organization's military services, recognizing that in some countries (such as the United States), there may be as many as seventeen agencies and organizations involved in collecting and processing national security-related intelligence information (see http://www.intelligence.gov/about-the-intelligence-community/).

Definition 4.2 (Applicable Laws) appears to concentrate primarily on laws related to "the collection, use, access, and disclosure of personally identifiable information." That focus would be appropriate if whois policy issues turned solely on matters related to registrant privacy.

CAUCE NA believes that any whois study *must* recognize the applicability of all criminal and civil laws on whois policy, and the impact of whois policy on those laws in turn.

Such laws would include, but not be limited to:

- laws against child exploitation and online "child pornography"
- laws making it illegal to attempt to obtain financial information without authorization by means of deceit or artifice ("phishing")

- laws forbidding the creation and distribution of viruses and other malicious computer software
- laws prohibiting the online sale and distribution of narcotics and other controlled drugs
- laws forbidding the advertising and delivery of copyright and trademark infringing products such as "knock-off" watches and pirated software, music and movies
- laws forbidding fraudulent schemes such as advance fee fraud schemes, penny stock "pump-and-dump" scams, products making baseless promises of weight loss or body enhancement
- laws regulating the collection of email addresses and distribution of bulk commercial email

Only when personal privacy rights are weighed against the full set of criminal and civil laws designed to protect a jurisdiction's citizens, can we achieve an appropriate balance between protecting privacy and protecting citizen's property and persons from all applicable risks.

In many cases the protection of property and persons from malicious actors is best served by *access to* whois information, rather than by withholding that information from interested parties.

Thus, that balancing process requires a more inclusive definition of "applicable laws" in CAUCE's opinion.

Defintion 4.3 ("Producers and Maintainers of WHOIS DATA") comingles a variety of parties and roles in ways that fail to adequately recognize important differences in perspectives and interests. For example, 4.3.A, "Producers" is defined as "The individuals or organizations supplying contact data for inclusion into WHOIS data." While that's seemingly a simple entity -- typically the person registering a domain -- in reality, things are less clear.

For example, whois data producers may include:

- the true or ultimate registrant
- a proxy registrant acting on behalf of the true or ultimate registrant
- a registrar or hosting company, perhaps listed as a default "technical" point of contact for all domains they register on behalf of the true or ultimate registrant
- a registration services provider acting on behalf of a registrar as an independent contractor or as the registrar's agent

These roles may change over time as well. For example, an engineer who may have initially registered a domain on behalf of an employer may change roles or change employers, yet still be carried on a registration as the point of contact for that domain, simply because the relevant data has never been verified and updated.

We might attempt to clarify all this by referring to an "initial producer" of whois data, or a "primary producer" of whois data, or a whois data "producer of record," depending on our emphasis, but any of those titles are only an approximation given the actual underlying practice.

We are also confused by the definition of "Data Controllers," particularly the trailing sentence

fragment: "May or may not be directly involved in these functions." While that tautologically covers all possible cases, and in fact all persons, it does little to illuminate what's intended in this case, and is so overly inclusive as to render the definition of "Data Controllers" effectively meaningless.

More substantively, the sundry roles lumped into the "definition" of "Data Controllers" should be explicitly teased apart unless there is some compelling reason to throw them all into the same vague stew. Those who may work in the IETF to define the whois protocol (thus defining what data may be collected), have little to do with those who may work in ICANN to "govern" how that data may be used, or the judges who may "require its release." Don't lump them all together.

7. Determining The Extent to Which Whois Policy Is Effective, and Meets the "Legitimate Needs of Law Enforcement," and Assessing The Extent to Which "Consumer Trust" Is Being Promoted

Finally, we are not persuaded that the articulated program of work will substantively meet the defined purposes of:

- assessing the extent to which WHOIS Policy is effective,
- meeting the legitimate needs of law enforcement, and
- promoting consumer trust.

If you have a grand program of work, but it doesn't meet those goals, you're wasting your time.

If ICANN wants to know these things, we recommend that it collect hard data on these topics using generally accepted technical market research and statistical methods. Simply asking for comments from the "usual suspects" (particularly when scant feedback is often provided) will not give a true understanding of what's happening in the real world.

Given the technical nature of the questions involved, ICANN should formally poll experts knowledgeable in the areas involved, as well as law enforcement agencies with officers who specialize in cyber crime, and organizations that represent consumer interests. This engagement needs to be *proactive* on ICANN's part, and not merely represent a willingness to listen to comments that may happen to trickle in from particularly motivated respondents who happen to comment.

Thank you for the opportunity to comment on this work, and we stand ready to address any points about which you may have questions or need further information.

Sincerely,
/signed/
CAUCE North America