

ISPCP

The ISP and Connectivity Provider Constituency

The ISPCP is pleased to submit this statement on WHOIS, in response to the “Staff overview on the activities of the Whois Task Force and the Whois Working Group”.

Firstly we would like to thank the ICANN staff for this report, which contributes to presenting a complex debate in a summarized and organized fashion.

The ISPCP has followed the debate on WHOIS, throughout the proceedings involving both the WHOIS Task Force and the WHOIS Working group, with close interest and active participation. The issues that have been debated and re-debated over several years tend to expose some rather inevitable conclusions:

- Registrant data is not validated, and thus any registrant can furnish false information for WHOIS purposes.
- Thus in a significant percentage, the concerns on privacy refer to inaccurate data sets, since no validation is conducted on the information submitted.
- Validation of data has not been attempted partly because of the stated costs borne by registrars.
- Registrants concerned about personal data privacy, have the option of buying the service of “private registration” (proxy service) from a registrar, thus concealing their own registrant data. Registrants can also find “shelter” for their data privacy under their own national laws, in many instances, by registering a domain in their own ccTLD registry.
- The “OPOC” solution does not, in its current form, address the substantial concerns raised by the ISPCP and broadly throughout the Internet community, including who gets access to registrant data, OPOC responsibilities and other practical details.
- There has not been a sufficient review of other possible alternatives such as the “special circumstances” proposal or “tiered access” models both of which limit some but not all access to Whois data.
- These proposed models would benefit from the same in depth discussion awarded to the OPOC solution, and may bear more productive results.
- The discussions of the WHOIS Working Group served to highlight considerable input, from sectors normally involved with pursuing and counteracting cybercrime activities, which invariably use websites to “trap” their victims, and thus require immediate investigative action. The ISPCP believes cybercrime, is a very significant threat to Internet users (including domain registrants) and has a substantial negative impact to the security and stability of the Internet. Cybercrime, in its many varied forms, including predatory behavior against minors, financial and consumer fraud and identity theft pose a very real and direct threat to individual privacy and to national sovereignty when a primary tool used for detection and prevention of such crimes is removed from legitimate users and law enforcement authorities.
- The discussions of the WHOIS Working Group failed to come up with consensus solutions to some basic and practical concerns:

- How can quick and efficient response to anti-cybercrime data gathering be ensured from an OPOC?
- What parties have access to the hidden data?
- Who decides which parties have access to the hidden data?
- Who pays for the costs involved in providing access to hidden data?

Finally, there are various issues pertaining to an implementation of the OPOC model, as reflected in the Staff report, that are far from achieving consensus support.

In this context, the ISPCP believes that promoting a GNSO resolution to move OPOC to an implementation phase, is not appropriate and fails to consider the very broad set of concerns raised by the community at large. .

Thus we would like to re-state certain considerations that our constituency has submitted in the past, namely:

ISPCP Uses of Whois Data

1. to research and verify domain registrants that could vicariously cause liability for ISPs b/c of illegal, deceptive or infringing content.
2. to prevent or detect sources of security attacks of their networks and servers
3. to identify sources of consumer fraud, spam and denial of service attacks and incidents
4. to effectuate UDRP proceedings
5. to support technical operations of ISPs or network administrators

The members of the ISPCP constituency continue to depend on WHOIS for the actions listed above, and in the course of our last meetings, have expressed their concerns on potential changes that could hinder their ability to perform these actions in a timely and effective manner.

Public statements, including this one on whois, are developed through a bottom-up, participant-led process. In the case of this statement, the ISPCP has used its long-established drafting and editing process for drafting, editing and vetting the document.