

[whois-comments]

[<<< Chronological Index >>>](#) [<<< Thread Index >>>](#)

EPIC Supports Formulation 1

- *To:* whois-comments@xxxxxxxxxx
- *Subject:* EPIC Supports Formulation 1
- *From:* Marc Rotenberg <rotenberg@xxxxxxxxxx>
- *Date:* Mon, 13 Feb 2006 16:35:42 -0500

Dear ICANN,

We respectfully request that the views of the Electronic Privacy Information Center (EPIC) be considered in the ICANN evaluation of the "Preliminary task force report on the purpose of Whois and of the Whois contacts 18 January, 2006." We understand that the formal deadline for comments expired 8 February 2006. We received no formal notification of this proceeding, and only recently learned from our colleagues in the NCUC that just one comment was provided in support of the privacy of Internet users. Therefore, we ask that you consider our views so that your decision about this important matter well be informed and that, whatever decision you reach, will be based on sufficient information.

We write to express our firm support for "Formulation 1," as this has been put forward in the Task Force Report. This is almost precisely the description that EPIC and Privacy International have presented in the leading report on privacy developments around the globe, Privacy and Human Rights ("PHR 2004"). In the following text, we excerpt the conclusions from that report on WHOIS and underscore the key findings. Further, we draw attention to the growing concerns about identity theft and the likelihood that a WHOIS policy that makes personal information widely available will put the privacy and security of Internet users at substantially greater risk.

[The report may be cited as <Marc Rotenberg and Cedric Laurant, "Privacy and Human Rights: An International Survey of Privacy Laws and Developments" (EPIC and Privacy International 2004)>, available online at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-82586&als\[theme\]=Privacy%20and%20Human%20Rights&headline=PHR2004](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82586&als[theme]=Privacy%20and%20Human%20Rights&headline=PHR2004), available for sale at <http://www.epic.org/bookstore/phr2004/>. the excerpts below may be found in the print edition at pages 133-37.]

PHR2004 recognized the important role that the Internet plays in promoting many beneficial services.

WHOIS

In the first quarter of 2004, more than 4.7 million new domain names were registered. This brings the total number of registrations to an all time high of 63 million domain names.[521]

Registrants include large and small businesses, individuals, media organizations, non-profit groups, public interest organizations, political, and religious organizations, and support groups. These domain name registrants share their services, ideas, views, activities, and more by way of websites, e-mail, newsgroups, and other Internet media. Registrants are required to provide information in the registration process, which is then made publicly available.

PHR2004 further discusses the central role of the ICANN in establishing the registration procedures, as well as many policy issues, for Internet users.

The Internet Corporation for Assigned Names and Numbers (ICANN), a private-sector corporation that coordinates policy for the Internet,[522] has established contractual arrangements with the registries that manage the top-level domains and the registrars that sell the domain names to the registrants. ICANN requires public disclosure on the Internet of domain name registrants' contact information (such as mailing address, phone number and e-mail address), administrative contact information, technical contact information, domain name and servers, and other information.[523] This information is referred to as "WHOIS" data. Its public availability has generated concerns over privacy protection.

PHR2004 expresses concern that the ICANN has not acknowledged the right of individuals, such as human rights advocates, to maintain anonymous web addresses.

Under ICANN's WHOIS policy, Internet users are unable to register for a domain anonymously. The WHOIS database broadly exposes domain name registrants' personal information to a global audience, including criminals and spammers.[524] Anyone with Internet access has access to WHOIS data, including stalkers, corrupt governments cracking down on dissidents, spammers, aggressive intellectual property lawyers, and police agents without legal authority.[525] Even those speaking out for human rights cannot conceal their identity. While it is true that some registrants use the Internet to conduct fraud, most domain name registrants do not, and many have legitimate reasons to conceal their identities and to register domain names anonymously. For example, political, artistic and religious groups around the world rely on the Internet to provide information and express views while avoiding persecution. Concealing actual identity may be critical for political, artistic, and religious expression.[526]

PHR2004 acknowledges that WHOIS data can be used for both good and bad purposes, but most importantly concludes that "the WHOIS database was no originally intended to allow access for such a variety of purpose." The original purpose of WHOIS, as PHR2004 makes clear was "to allow network administrators to find and fix technical problems with minimum hassle in order to maintain the stability of the Internet."

WHOIS data lends itself to both good faith and bad faith uses, and investigating fraud is only one of many uses of WHOIS data.[527] There now exist various automated data mining procedures that provide bad-faith users with access to large amounts of personal data at a time, rather than just individual queries. Web-based WHOIS services now have to complicate their access procedures, for

example, requiring users to enter number codes before they can retrieve information. The WHOIS database was not originally intended to allow access for such a variety of purposes. The original purpose of WHOIS was instead to allow network administrators to find and fix technical problems with minimal hassle in order to maintain the stability of the Internet.

PHR2004 further notes that requiring accurate data without safeguards for privacy needlessly puts individuals at risk.

ICANN's WHOIS policy requires that registrants provide accurate WHOIS information, or otherwise forgo a domain name.[528] If a domain registration is assumed to have inaccurate information, registrants are contacted and given a very limited amount of time to address the problem. Data entered at registration may change in the real world and registrant may forget to update it. They may lose their domain if they are unable to respond quickly to any attempts to contact them. Privacy experts have noted that a policy requiring accurate WHOIS data and then publicly disclosing the data creates serious implications for free speech.[529]

The ICANN WHOIS policies conflict with national privacy laws, including the EU Data Protection Directive, which require the establishment of a legal framework to ensure that when personal information is collected, it is used only for its intended purpose. At a recent ICANN meeting, George Papapavlou, a representative from the European Commission stated that if the original purpose of the WHOIS database is purely technical, the rights of access to and collection of that information pertain solely to that original purpose.[530] Speaking at the "Freedom 2.0" conference held by EPIC in May 2004, Vinton G. Cerf, the President of ICANN, confirmed directly that the original purpose of WHOIS was indeed purely technical.[531] As personal information in the directory is used for other purposes and ICANN's policy keeps the information public and anonymously accessible, the database could be found illegal according to many data protection laws including the European Data Protection Directive.[532]

As the PHR2004 report explains, the collection of information for a technical purpose would not provide justification for other uses. Such a conclusion would violate the laws of any country with a modern privacy regime.

Under European law, technical users would be the only ones with a legitimate claim to the information. While intellectual property lawyers and law enforcement officials claim the WHOIS database must retain all its current data in its public form as a resource for investigations, the fact that the WHOIS database was originally created for technical purposes makes it clear that such claims to the database would be inconsistent with its original purpose.

In 2003, ICANN's Generic Names Supporting Organization (GNSO) began a policy development process identifying three issues, access, data and accuracy, and creating task forces to study and make recommendations on each. EPIC is serving on one of the WHOIS task forces. The outcome of the WHOIS Policy Development Process will have a significant impact on privacy, civil liberties, and freedom of expression for Internet users.[533] Civil liberties groups and the Non-Commercial Users Constituency[534] of ICANN

have urged ICANN to limit the use and scope of the WHOIS database to its original purpose, which is the resolution of technical network issues, and to establish strong privacy protections based on internationally accepted privacy standards. This limitation would entail restricting access to the data, minimizing data required to only that needed for technical matters, and not penalizing registrants for protecting their personal information by entering inaccurate personal data elements.

The task forces have drafted reports[535] on WHOIS policy in these three areas, yet it is unclear whether the recommendations will improve privacy protections. Some of the recommendations entail more privacy risks than safeguards. At the same time, some of the better recommendations, including some restrictions on access and data required, may not be accepted by the GNSO Council and the ICANN Board should they decide to rule on the policy development. After three years, this policy development process, including the establishment of previous task forces, has not made any strides in the protection of privacy and the current problematic policy remains.

PHR2004 also notes that the prospect of developing policies for access to WHOIS data could particularly contradict the practices that are likely to be enforced for ccTLDs in jurisdictions where there are clear privacy laws.

While ICANN has considerable authority over the development of WHOIS policies for the generic top-level domains (gTLDs), such as .com, .org, and .net, it is unclear whether ICANN will be able to exercise similar control over the country-code top-level domains (ccTLDs), such as .uk and .de, which may choose to follow national policies. Significantly, country code Top Level Domains are moving to provide more privacy protection in accordance with national law. For example, regarding Australia's TLD, .au, the WHOIS policy of the .au Domain Administration Ltd (AUDA) states in section 4.2, "In order to comply with Australian privacy legislation, registrant telephone and facsimile numbers will not be disclosed. In the case of id.au domain names (for individual registrants, rather than corporate registrants), the registrant contact name and address details also will not be disclosed." In addition, aUDA does not allow bulk access to WHOIS data, which ICANN's gTLDs do.[536] It is unclear what, if any, indirect effect the GNSO WHOIS policy development will have on the policies of ccTLDs.

The ICANN WHOIS policy process has continued for several years, yet has failed to resolve the privacy risks faced by Internet users that result directly from ICANN's own data practices.

We concluded in 2004 that the ICANN WHOIS policy has "failed to resolve the privacy risks faced by Internet users that *result directly from ICANN's own data practices.*" (emphasis added).

This last point is critical: It is ICANN that is placing the privacy and security of Internet users at risk by collecting and making publicly available personal information that need not be collected and certainly should not be disclosed.

We have learned in the United States over the last few years about the extraordinary risks to personal privacy that result from the improper disclosure of personal information.

Identity theft has emerged as the #1 crime in the US. According the US Federal Trade Commission, almost 250,000 ID theft complaints were received by the FTC in 2004. The FTC reports that approximately 10 million Americans each year fall victim to identity theft. The FTC estimates that the annual cost is \$53 b to the US economy. Moreover, the FTC found that prosecutions are rare as police investigations are costly, time-consuming and easily stymied.

Has the ICANN given any serious consideration to the likelihood that it may exacerbate dramatically the risk of identity theft for Internet users if it makes personal information widely available to anyone with access to the WHOIS database without any consequences for how that information is used??

The wisdom of privacy laws has become increasingly self-evident over the last several years. Those countries that have limited the disclosure of personal information have simply not experienced the same level of criminal conduct as have those countries that make this information widely available.

ICANN has every reason to adopt Formulation 1 from the Preliminary Task For Report of January 2006:

- (1) It is consistent with the original purpose of WHOIS data
- (2) It is consistent with the privacy laws of many countries
- (3) It is consistent with the best practices of the ccTLDs that have addressed the WHOIS issue
- (4) It will help safeguard the privacy and security of Internet users

We urge the ICANN to adopt this sensible approach to a very serious issue.

(Further information regarding WHOIS Privacy may be found at the EPIC page, <http://www.epic.org/privacy/whois/>)

Thank you for your consideration of our views.

Sincerely,

Marc Rotenberg
Executive Director
EPIC

[<<< Chronological Index >>>](#) [<<< Thread Index >>>](#)

[Privacy Policy](#) | [Terms of Service](#) | [Cookies Policy](#)