

VIA EMAIL

July 5, 2004

Comments regarding the Whois Task Force 1 Preliminary Report

Dear Sir or Ms.:

After reading the Task Force 1 Preliminary Report on Restricting Access of WHOIS data for Marketing Purposes, we have a number of comments regarding its findings and policy recommendations.

Comments on Task Force 1 Preliminary Report

1. Comments on Summary of Findings

A. Comments on Finding 1

The task force report notes that mechanisms for controlling data mining activities are “insufficient to prevent data mining of the WHOIS database for marketing purposes.” We agree with this finding. In the report, we note that we did not find a thorough discussion of what constitutes those marketing uses and abuses. This information should be added to the report.

B. Comments on Finding 3

The report states in Finding 3 that the “requestor of WHOIS information should be required to identify itself to the WHOIS provider ... along with the reasons for which it seeks the data.” We agree with this finding. We, however, strongly disagree with the position advocating that keeping an audit trail is sufficient in preventing abuse of WHOIS data. An audit trail is an unacceptable alternative to registrant notice.

C. Comments on Finding 7

The task force found that “a cost benefit analysis and a feasibility study should be done when considering any changes in WHOIS requirements.” We agree with this finding. However, we are wondering why the task force did not also call for a study of the marketing abuses of the WHOIS data. We believe this omission is a substantial one and needs to be added to the findings. Marketing abuse of WHOIS data can be substantiated and quantified through a number of technical means.

II. Comments on Task Force 1 Policy Recommendations

A. Comments on Recommendation 2, “Value of WHOIS Data”

This recommendation states that if only non-sensitive WHOIS data is displayed, then since that data has little value, it “is less likely to be data mined, and has little effect on privacy rights.” We recognize that some categories of WHOIS data are more sensitive than others. We support tiered access to WHOIS data for this reason. However, some of the WHOIS data that Task Force 1 cited as data of little value includes technical contact name, phone number, and email (See footnote 16 of the report). In the case of an individual registrant who has purchased a domain and is hosting a Web site at home, a private individual is the technical contact. The technical contact information in that situation is of great importance to privacy rights, and has value. Even in a remote domain hosting situation, a registrant would likely put their own name as the technical contact.

We understand that the outcome of this discussion will depend on Task Force 2’s recommendations as to what constitutes sensitive and non-sensitive data. However, it is important to note that access to information deemed non-sensitive still needs to be controlled. This will be particularly true for any information that is personally identifiable, for example a person’s name, a personal email address, or a home phone number.

B. Comments on Recommendation 4, “Identification of Requestor and Notification to Registrant.”

We agree with the task force recommendation that at a minimum, requestors of WHOIS data should be required to identify themselves to the WHOIS provider and state their purposes for accessing the data. Some constituencies recommended identification via an audit trail. An audit trail does not constitute notice, therefore, we do not support using audit trails as a sole identification mechanism. We strongly support notice for each registrant whose data is requested.

Task Force 1 requested comment on a proposal that stated only a limited number of purposes should be allowable for accessing WHOIS data deemed sensitive. The proposal further stated that the reasons be provided in a multiple choice list.

We agree that only a limited number of purposes should be allowable for accessing the WHOIS information deemed sensitive. The WHOIS database was created to be used just as a technically-oriented directory. Now, however, the WHOIS database has become a defacto information source for many uses, such as lawsuits and telemarketing. These uses are inappropriate and can in some cases work to circumvent due process.

Extremely limited WHOIS information could be used to satisfy the "technical and operational purposes" the WHOIS database was created to satisfy. This information could potentially include Web administration details, but need not contain personal information about the registrant such as home address and phone number.

It is our position that access to sensitive WHOIS information should not be granted unless there are valid technical reasons for access, or a subpoena has been delivered for that information.

The report mentions that a multiple choice list of options might be appropriate in this situation of granting access to sensitive information. We would need to see more details in order to be able to comment on the merits of a multiple choice list.

C. Comments on Recommendation 6 (b)

We disagree with the statement that "if only non-sensitive data is displayed, there is little reason to change anything with respect to Port 43" for reasons already stated. We agree that Port 43 access should be available solely to Registrars for the purpose of carrying out domain transfers.

D. Comments on Recommendation 7, "Automated access to WHOIS"

We do not support bulk access to the WHOIS database.

E. Comments on Recommendation 8, "Approval Process for Automated Searches to prevent data mining"

The recommendation for the creation of a "white list" is a negative in the context of the WHOIS database. The potential for abuse of the mechanisms described in Recommendation 7 by those who gain entry on to the list is substantial. Again, access to sensitive data in the WHOIS database is not a right. And access that is beyond the scope of access for technical purposes should be given only by following due process procedures of the host countries of the registrant.

Sincerely,

Pam Dixon
Executive Director
World Privacy Forum

Beth Givens
Director
Privacy Rights Clearinghouse