

VIA EMAIL

June 8, 2004

Comments regarding the WHOIS Task Force 2 Preliminary Report

Dear Sir or Ms.:

After reading the Task Force 2 Preliminary Report regarding the WHOIS database, we have a number of comments in response to the report recommendations on WHOIS data collection and display.

#### 1. Comments on Notification and Consent Recommendations

The Task Force 2 Preliminary Report noted that lengthy domain name registrar/registrant agreements could discourage a thorough reading by registrants. To remedy this, the task force found that registrant disclosures regarding access to WHOIS data should be "set aside from other provisions ....by way of a bigger or bolded font, a highlighted section, simplified language, or otherwise made more conspicuous" (Task Force 2 Preliminary Report, Section 2.1).

These findings are positive, but the actual recommendations of the task force do not go far enough (Sections 1.4, 3.1). Many non-commercial registrants do not know that their home phone numbers, email address, and street addresses may be made public. Because of the potential for abuse of personally identifiable information after it is published in the WHOIS database, we recommend that registrant notification of WHOIS publication be made in a window separate from and in addition to the regular registration agreement.

In other words, registrants must click through a separate window containing only the notification language prior to registration. The notification language in the separate window should be brief, clear, in a large font, and highlighted. This would constitute a much more meaningful electronic notification than simply using larger font in a document that registrants typically do not read anyhow.

We also believe that specific, detailed, and timely notification must be given to registrants each time their personal information is accessed. This notification could take the form of an email. The notice to registrants should contain the name and contact information of the entity that accessed the registrant's information, and whenever possible it should cite the specific reason for access.

Additionally, it is reasonable to request that the recommendations be expanded to include a provision for all domain name registrants to obtain a full reporting of

what entities have accessed their registration information upon their (the registrants') request. This provision relates to the OECD Fair Information Principles of openness and user participation. Registrant requests would not be unduly burdensome to fulfill if access to registrants' personally identifiable information was limited, clearly defined, and a log of accessors was maintained.

## 2. General Comments on Recommendations Regarding Publication of WHOIS Data

We understand -- deeply so -- that the WHOIS database must be focused both on privacy and on reducing fraudulent activity. It is the experience of our organization that registrants have had problems with stalking, identity theft, and fraud after giving accurate, truthful WHOIS data to a registrar. It is also our experience that those individuals and organizations who are committing fraud and other crimes upon individuals regularly give untrue or misleading WHOIS data. So the victims who have told the truth are harmed, but the individuals committing fraud on others escape unscathed for their untrue registration data.

We therefore believe that the recommendations should address this particular situation, among the other situations noted in the Task Force 2 Preliminary Report. Strict controls on the publication of personal data must be implemented as part of the solution to the victimization of registrants.

### A. Comments on Section 3.5 (a)

We support tiered access to registrant data.

### B. Comments on Section 3.5 (b)

The Task Force 2 Initial Report recommended in section 3.5 (b) that "Registrants should have the option to direct that some or all of their protected data be displayed to the public." The language in this recommendation is troubling given that it does not specify that if this option is employed, that it would be applied only as a strict opt-out for registrants. Registrants should never be automatically opted-in by a registrar to this publication choice.

We have seen that registrars often opt registrants in to various uses of WHOIS data by means of small, hard to find, automatically checked boxes at the bottom of pages. This sort of auto-opt in would likely continue unless strong opt-out language is adopted regarding the publication of registrant information.

We urge Task Force 2 to consider that registrants may be human rights workers, and that the personally identifiable information sought for simple business use in one context may in fact be used to bring great harm upon individuals who did not

realize that due to a nearly invisible checked box on a page, that registering a domain name put them at risk.

### C. Comments on Section 3.5 (d)

This section says "Those seeking access to protected information should identify themselves in a verifiable manner. Once identified, the user would be issued a portable credential, rather than needing to re-verify their identity on a registrar-by-registrar ...basis." We agree that authentication of users seeking to access protected registrant information is a positive step.

We strongly oppose the idea of a portable credential that could be used for "bulk access" to registrar data, however. We believe that strictly limited access must be granted on a registrar- by- registrar basis only. Because no mass-authentication system is foolproof against fraud, granting access to the data on a registrar-by-registrar basis institutes an immediate safeguard against those who are able to gain access to the registrant data fraudulently. Instead of being able to gain access to a large number of registrants immediately, a person seeking to harm registrants would have a higher barrier and would have more likelihood of discovery if bulk access is denied.

### D. Comments on Section 3.5 (f)

The Task Force recommended that "Registrars and registries should continue to have full access to the WHOIS data for technical and operational purposes." This access needs to be defined more closely and also needs to be limited. We are seeing that identity theft and fraud are often committed by those who work in positions that provide access to detailed customer data. The WHOIS data held by registrars is not an exception to this trend. Therefore, WHOIS data should be managed as private customer information with internal safeguards and access controls in place within each registrar.

The Task Force 2 recommendations need to do more to identify what specific information a registrar may access. It should not be a given that registrars may access all registrant information. For example, extremely limited information could be used to satisfy the "technical and operational purposes" noted in the recommendations. This information could potentially include Web administration details, but need not contain personal information about the registrant such as home address and phone number.

## 3. Comments on the Purpose of the WHOIS Database

In paragraph one of the preliminary report, the task force defined the WHOIS database as a "directory service to Internet users." The task force rightly said in

the same paragraph that the WHOIS database was no longer used just as a technically-oriented directory, but as a defacto information source for many uses, such as lawsuits and telemarketing. Later in the report, the task force recorded that "One topic the Task Force addressed and did not answer was the purpose of the database" (Section 2.5).

The purpose and definition of the WHOIS database is a core issue that needs to be addressed. We urge Task Force 2 to undertake the hard work of resolving this central issue. Without firm, clear lines of understanding of basic WHOIS database purposes, "mission creep" related to the WHOIS database will continue to occur, and recommendations will continue to sidestep the core issues of who really owns the data, and how or if that data may be accessed and used by third parties.

By sidestepping the core issue of the purpose of the WHOIS database, the task force has unnecessarily relegated itself to correcting the periphery while allowing the central question at hand to remain problematically unarticulated.

#### 4. Comments on Perceived Omissions in the Task Force 2 Preliminary Report

We wonder why more effort was not made by the task force to document the systematic abuses of WHOIS registrant data that are occurring. Section 2.5 (d) notes that abuses were presented to the task force, but were not documented.

We strongly urge Task Force 2 to fully document these abuses and quantify the type and frequency of their occurrence. Documentation and quantification of this type will allow a genuinely informed approach to be made to the data abuse issues facing registrants, registrars, and all stakeholders. It is important to keep in mind that as time goes on -- if history is any indicator -- abuse of registrant data will likely increase, and the crimes committed using it will likely grow more serious in nature.

Without clear and factual documentation of WHOIS abuses, it will be challenging for the task force to put forward the most clear and appropriate set of solutions possible.

Sincerely,

Pam Dixon

Pam Dixon  
Executive Director  
World Privacy Forum

