Comments of the Electronic Frontier Foundation
To ICANN's WHOIS Task Forces 1 and 2, July 5, 2004

The Electronic Frontier Foundation ("EFF") is a member-supported nonprofit organization devoted to protecting civil liberties and free expression in the digital world. With over 12,000 dues-paying members and over 50,000 mailing-list subscribers, EFF leads the global and national effort to ensure that fundamental liberties are respected in the digital environment. EFF has members all over the United States and around the world, and maintains one of the most-linked-to Web sites in the world, <http://www.eff.org>.

EFF has watched recent discussions of WHOIS and changes to WHOIS policies with growing concern. Our concerns as a civil liberties organization are based in both privacy and free speech interests. We commend the Task Forces for steps in the right direction to account for privacy interests, but find that even the strongest of those recommendations are insufficient to protect freedom of speech and anonymity online. To address the broad range of free speech concerns, ICANN would have to address not only limitations on display of WHOIS information, but limitations on the information required to be collected in the first place.

The continuing importance of domain names

Domain names are tools of online speech for individuals, associations, and companies; they facilitate communications on web pages, in email, over chat, via newsgroups, bulletin boards, and weblogs. Although it is possible to speak online without registering a domain name (either by using a bare IP address or by using a subdomain or service for which someone else has registered the primary domain name), many online speakers benefit from registering their own domain names.

A domain name can be a more stable identifier than an IP address or hosted email address, which may change when the user switches Internet service providers,[1] and more memorable than a string of digits.[2] Registering a domain name directly gives greater control than relying on the privacy practices and stability of a third-party host, whose ownership or business interests may change over time. EFF believes that domain names' speech-facilitating qualities should be available to all, without demanding the tradeoff of important privacy and anonymity rights.

A domain name may serve as a persistent pseudonym, by which anonymous speakers can participate in dialogues, accept comments, and respond to critics. While hosted services may enable such pseudonyms, those services provide less stability than direct domain name registration. They do, however, show how anonymity can foster ongoing commentary. For example, liberal political commentator "Atrios" has

---

[1] Many individual Internet users get only dynamically assigned IP addresses from dial-up, cable-modem, or DSL providers. Even larger entities do not own the netblocks they use. *See* ARIN Service Agreement, ¶9:

> Applicant acknowledges and agrees that the numbering resources are not property (real, personal or intellectual) and that Applicant shall not acquire any property rights in or to any numbering resources by virtue of this Agreement or otherwise.

<http://www.arin.net/library/agreements/rsa.pdf>.

[2] *See* RFC 1034, <http://www.ietf.org/rfc/rfc1034.txt>.

maintained a pseudonym for more than two years on the Eschaton weblog.[3] The poster of "Unlimited Freedom" has espoused a politically conservative intellectual property position with the aid of a cryptographically signed identity on Invisiblog.[4]

The imperfections of hosted services may be seen in the example of Domains-By-Proxy and the Re-Code.com website. Domains-By-Proxy revealed the name of its "anonymous" registrant as soon as the registrant's conduct was challenged, without any determination that the challenger had a legal cause of action.[5]

Privacy

What we describe as the "privacy" interest concerns principally the amount and nature of information publicly disclosed about a domain name registrant. Some online speakers are willing to be identified as registrants of a domain name but do not want personally sensitive information such as telephone number, home address, or email address published to the world as a consequence. For these registrants, the Task Forces' recommendations to permit the display of sensitive information only to those requesters who identify themselves and demonstrate justification for their access to the data would provide substantial benefit.

For registrants concerned with privacy as described here, WHOIS would be improved by limiting display of sensitive data, recommendations Task Force 1 describes as "Identification of the Requestor and Notification to the Registrant" (III.C.4 para. 1, recommendations of Noncommercial, ALAC, Registrars, and Registries) and Task Force 2 describes as "tiered access" (3.5, provided access were granted on a per-use basis). If would-be users of WHOIS information were required to identify themselves and the purpose of their data use at the time they sought a domain name registrant's sensitive

---

[3] *See* Eschaton, <http://atrios.blogspot.com/>, and archives, <http://atrios.blogspot.com/atrios_archive.html>.

[4] *See* <http://invisiblog.com/1c801df4aee49232/>.
Invisiblog explains its anonymity service in its FAQ:

> q: Who needs that much anonymity?
> a: Here are some examples of bloggers and web publishers whose life or liberty has been threatened, or could be endangered in the future:
>
> - Salam Pax, a pseudonymous blogger claiming to be from Iraq, who posted a diary during the recent war. He has not posted since March 24; some suspect he was captured by Iraqi secret police before US forces reached Baghdad. Journalist Paul Boutin was able to trace Salam's emails to an ISP in Lebanon.
> - Iranian blogger and journalist Sina Motallebi was arrested on April 19, and faces charges over the content of his weblog and interviews given to foreign media groups.
> - Tunisian web journalist Zouhair Yahyaoui was arrested and imprisoned for publishing political commentary on his web site. Authorities allegedly used torture to force Yahyaoui to reveal his access passwords.
> - Cuba recently imprisoned 75 dissidents and democracy activists, including a number of online journalists, for writing articles critical of the government. Many of them were turned in by informers amongst colleagues and even family. Some of their associates continue to publish on the web.

<http://invisiblog.com/info/faq/#3>.

[5] *See* <http://wendy.seltzer.org/blog/archives/2003/04/11/proxy_fight_domainsbyproxy_update.html>.

information, the reciprocity of disclosure would provide some accountability for the data user and potential recourse to the domain name registrant if the data were misused.

Among the alternative positions set out in the Task Forces' reports, both timely access to requesters' information and per-use authentication are critical to protecting privacy.

1) The registrant must get timely access to requesters' information. The registrant may be in the best position to know whether the requester of WHOIS data has a legitimate purpose or is using the request for improper harassment, for example. For the same reason that data users assert a need for timely response to their WHOIS queries, registrants should be able to follow-up expeditiously on improper requests for their sensitive information. While there may be some latitude to delay (not dispense with) notification when necessary to permit a law enforcement investigation, that exception must not be permitted to swallow the rule of timely notification.

2) Authentication must be per-use rather than per-person or per-entity. Someone who claims legitimate access to some WHOIS information should not thereby get access to the information of all registrants of all domain names. The intellectual property attorney investigating registration of domain names claimed to infringe a client's trademarks, for example, has not shown a need to access information on unrelated domains and registrants. Per-use authentication puts all data requesters on equal footing with one another and with domain name registrants.

Anonymity

Other speakers do not want their online speech connected with offline identities. They may be concerned about political or economic retribution, harassment, or even threats to their lives. Whistleblowers report news that companies and governments would prefer to suppress; human rights workers struggle against repressive governments; parents try to create safe spaces for children to explore; victims of domestic violence attempt to rebuild their lives where abusers cannot follow.[6] For all these individuals and the organizations that support them, secure anonymity is critical. These speakers' interests are not addressed by the reciprocal disclosure of tiered access proposals, but by limiting the data collection that is required of them.

The tradition of anonymous speech is older than United States, where founders Hamilton, Madison, and Jay wrote the Federalist Papers as "Publius" and "the Federal Farmer" spoke up in rebuttal. The U.S. Supreme Court has repeatedly recognized rights to speak anonymously derived from the First Amendment. *See McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995) ("anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent"); *Talley v. California*, 362 U.S. 60 (1960):

[6] It should be clear that our concern is not about protecting the anonymity of lawbreakers, but to protect lawful speech. Those inclined to break the law are unlikely to abide by ICANN's WHOIS accuracy requirements in any event, and other forensic methods will be more reliable to determine their identities.

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. . . . Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes.

Id. at 65.

Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views.

> Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society.

McIntyre, 514 U.S. at 357 (citation omitted). Fears that their identity may be uncovered, and that they may be persecuted on account of their speech, may prevent minority speakers from speaking at all.

In the United States, at least, the right to anonymous speech is protected well beyond the printed page. Thus the Supreme Court struck down a law requiring proselytizers to register before going door-to-door, even where the town had claimed an interest in preventing physical crime supported its law. *See Watchtower Bible & Tract Soc'y of New York, Inc. v. Village of Stratton*, 536 U.S. 150, 166 (2002). Requiring registration to speak through domain names online does not fit this tradition.

Red herring arguments for full WHOIS display

As important as domain names are to speech, domain name WHOIS is much less important than many commenters claim in solving technical or law enforcement problems. Far from complicating troubleshooting, law enforcement, or consumer protection, a privacy-protective WHOIS makes it more likely that information that is provided will be accurate, if registrants do not have to resort to the "self-help" of deliberate inaccuracy.

Further, domain name WHOIS will rarely provide a reliable identifier of the source of spam, "phishing," or denial of service attacks. Substantially more can be learned about network attacks from the ARIN IP address WHOIS, identifying the owners of the network addresses in question and tracing through them to the users at the time of the incident.

Nor does anonymous registration hinder law enforcement. If law enforcement (civil or criminal) show that a domain name is being used in illegal activity, they can obtain an order changing or terminating the domain name resolution even if they cannot yet determine the registrant's identity. Thus the Freedom network from Zero Knowledge allowed its users to use the Internet anonymously. It did not know users identities, but if they spammed or engaged in other harmful activity, they were deleted and lost their payments, without ever being identified. Likewise with domain names, the offending activity can be stopped while law enforcement investigates.

Conclusion:

The protection of rights to anonymous speech and privacy requires more than the steps proposed by any of the WHOIS Task Forces. The Task Forces' recommendations to eliminate sensitive data from public display and to require authentication of purpose from WHOIS data requesters before granting access to those data are important progress, but only a beginning of an answer to half the question.

To address the interests of free speech and anonymity, ICANN should limit ICANN-required data collection to that necessary to resolve a domain name – nameservers and some technical contact information (an email address, for example). Registrars should be free to determine for themselves and in the market whether to collect additional data without displaying it publicly. This limitation on mandatory data collection would simultaneously improve accuracy of the information collected, reduce incentives for and harm from datamining, and preserve freedom of speech and privacy.