PRIVACY ISSUES REPORT:
The Creation of A New Task Force is Necessary For an Adequate Resolution of the Privacy Issues Associated With WHOIS

Statement for the Record of
The Non-Commercial Constituency

Prepared by
Electronic Privacy Information Center (EPIC)
And
Ruchika Agrawal, Non-Commercial Constituency Representative on the WHOIS Task Force

Before the
GNSO Council

March 10, 2003

Contents

Executive Summary

There are various types of domain name registrants – from individuals, who may have legitimate reasons for anonymous speech, to Internet scam artists. Furthermore, anyone with Internet access – from individuals, law enforcement, to scam artists – can access WHOIS data of domain name registrants for any reason and use the data in any way. Finally, WHOIS data consists of personally identifiable information.

This report questions whether it makes sense to impose a rule that requires all domain registrants to make their WHOIS data globally, publicly accessible as is dictated by current WHOIS policies and practices. This report takes into account the issues of privacy, free speech, and fraud.

The report mainly focuses on the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines as a well thought-out solution to challenging questions about international consensus on privacy and data protection that directly implicate WHOIS policies and practices. The OECD Privacy Guidelines serve as a basis for a sensible WHOIS policy. A serious discussion on privacy and WHOIS should begin with the framework set out by the OECD Privacy Guidelines.

A new task force must be formed to further evaluate and resolve the privacy issues associated with WHOIS policies and practices. Such a task force should consider the following recommendations:

> **Recommendation 1:** Personal information, beyond that necessary for contacting system administrators about network or security problems, should not be included in the globally, publicly accessible database. International privacy standards, such as the OECD Privacy Guidelines, should apply to the collection and use of WHOIS data.
>
> **Recommendation 2:** Anonymous registration of domain names should be provided and should not be burdensome to Internet speakers who are engaging in political or religious speech.
>
> **Recommendation 3:** A study that considers whether the availability of WHOIS data contributes to consumer fraud, such as identity theft, should immediately be undertaken.
>
> **Recommendation 4:** Accuracy of WHOIS data should not be enforced until privacy issues are adequately resolved and appropriate privacy safeguards are implemented.

We look forward to the GNSO Council's balanced approach in creating a new task force that will undertake a full and fair evaluation of the privacy issues associated with WHOIS.

1 Introduction

A meaningful discussion on privacy issues associated with WHOIS policies and practices must be preceded by answers to the following questions:

- What is WHOIS data?
- Who are the domain name registrants? That is, whose WHOIS data is exposed?
- Who has access to WHOIS data?
- Does "one size fits all" make sense? That is, does it make sense to apply one rule (to require globally, publicly accessible WHOIS data) to the various types of domain name registrants and to the various types of individuals that access WHOIS information?
- Does the current WHOIS policy and recommendations of the WHOIS Task Force comply with international laws and guidelines?
- What are the implications of WHOIS data on privacy and free speech?
- What are the implications of WHOIS data on consumer fraud?

We will begin by answering the first three questions in turn, and then consider the remaining questions as appropriate.

2 Understanding WHOIS[1]

The WHOIS database, originally intended to allow network administrators to find and fix problems with minimal hassle to maintain the stability of the Internet, now exposes domain name registrants' personally identifiable information to spammers, stalkers, criminal investigators, and copyright enforcers.[2] Whether WHOIS policies and practices should facilitate this exposure is a topic that deserves careful consideration.

2.1 WHOIS data consists of personally identifiable information.

WHOIS data consists of domain name registrants' contact information (including registrant's mailing address, email address, telephone number, and fax number); administrative contact information (including mailing address, email address, telephone number, and fax number); technical contact information (including mailing address, email address, telephone number, and fax number); domain name; domain servers; and other information.

For example, a WHOIS search for epic.org reveals:

Through .ORG Registry (and subject to registry's terms of use)	Through epic.org's Registrar (and subject to registrar's terms of use)
Public Interest Registry (PIR)	**Tucows**

[1] See Appendix A for the Internet Corporation for Assigned Names and Numbers' (ICANN's) requirements for the collection and disclosure of WHOIS data.
[2] Marc Rotenberg, "Review of Ruling the Root," EPIC Alert 9.14[7] (July 25, 2002)

Domain ID:	D313895-LROR
Domain Name:	EPIC.ORG
Created On:	18-Apr-1994 04:00:00 UTC
Last Updated On:	28-Feb-2002 19:08:44 UTC
Expiration Date:	19-Apr-2004 04:00:00 UTC
Sponsoring Registrar:	Tucows, Inc (R11-LROR)
Status:	OK
Registrant Name:	CONTACT NOT AUTHORITATIVE
Registrant Street1:	Whois Server:whois.opensrs.net
Registrant Street2:	Referral URL:http://www.opensrs.org
Name Server:	NS.2RAD.NET
Name Server:	NS.PEREGRINEHW.COM
Name Server:	NS2.2RAD.NET

Registrant:
Electronic Privacy Information Center
Rotenberg, Marc rotenberg@epic.org
1718 Connecticut Ave NW
#200
Washington, DC 20009-1146
US
202 483 1140
Fax: 202 483 1248

Domain name: EPIC.ORG

Administrative Contact:
Rotenberg, Marc rotenberg@epic.org
1718 Connecticut Ave NW
#200
Washington, DC 20009-1146
US
202 483 1140
Fax: 202 483 1248

Technical Contact:
Hoofnagle, Chris hoofnagle@epic.org
1718 Connecticut Ave NW
#200
Washington, DC 20009-1146
US
202 483 1140
Fax: 202 483 1248

Registration Service Provider:
Intercosmos Media Group Inc. dba directNIC.com, support@directnic.com
504 679 5173
http://www.directnic.com
This company may be contacted for domain login/passwords, DNS/Nameserver changes, and general domain support questions.

Registrar of Record: TUCOWS, INC.
Record last updated on 06-Feb-2003.
Record expires on 19-Apr-2004.
Record Created on 18-Apr-1994.

Domain servers in listed order:

	NS.2RAD.NET NS.PEREGRINEHW.COM NS2.2RAD.NET

Note that the second column provides more information, which was obtained in two steps: (1) a WHOIS search through PIR, as the shared domain registry, revealed epic.org's registrar as Tucows and then (2) a WHOIS search through Tucows provided additional information, including epic.org's registrant's mailing address, administrative contact, technical contact, creation date, and expiration date. Through one website (accessible via http://www.betterwhois.com), a BetterWhois search would reveal the same information as in the second column.

As another example, a WHOIS search for farber.net reveals:

Through BetterWhois
Registrant: David Farber (FARBER6-DOM) 216 Good Hope Road Landenburg PA,19350 US Domain Name: FARBER.NET Administrative Contact: Farber, David (DF188) farber@CIS.UPENN.EDU David Farber 216 Good Hope Road Landenburg, PA 19350 (610) 274-8292 Technical Contact: Administration, Domain (AD8810-ORG) dns@DCA.NET DCANet 1204 West Street Wilmington , DE 19801 US (302) 654-1019 Fax- (320) 426-1568 Record expires on 16-Apr-2009. Record created on 16-Apr-1998. Database last updated on 11-Feb-2003 13:00:49 EST.

Domain servers in listed order:	
NS1.DCA.NET	204.183.80.2
NS2.DCA.NET	207.245.82.2

The two example domain names belong to two different type of registrants: a public interest organization whose contact information is already made publicly available through their website and an individual whose personal contact information has been made available through WHOIS, respectively.

2.2 WHOIS exposes various types of domain name registrants, including individuals, non-profit groups, political organizations, religious organizations, and businesses.[3]

Domain name registrants in the .com/.org/.net top-level domains consist of businesses; individuals; media organizations; non-profit groups; public interest organizations; political organization; religious organizations; support groups; and so on. These domain name registrants share their services, ideas, views, activities, and more by way of websites, email, newsgroups, and other Internet media. While some domain name registrants use the Internet to conduct fraud, other domain name registrants have legitimate reasons to conceal their identities and/or to register domain names anonymously. For example, different political, artistic and religious groups around the world rely on the Internet to provide information and express views while avoiding persecution - and concealing their identity is critical in this respect.

It is worth noting that requiring accurate WHOIS data without having appropriate privacy safeguards in place is problematic for a number of domain name registrants. Some registrants have legitimate reasons for providing inaccurate WHOIS information – for example, to protect their privacy and protect their personally identifiable information from being globally, publicly accessible – and especially when there are no privacy safeguards in place. A number of studies demonstrate that when no privacy safeguards are in place, individuals often withhold personal information and give false information.[4]

The corollary of privacy "self-defense" practices is that establishing and implementing appropriate privacy safeguards first is one way to improve the accuracy of

[3] Comments of the Public Interest Registry, the not-for-profit corporation that manages the .ORG registry, on the Final Report on Whois Accuracy and Bulk Access of the Whois Task Force of the Generic Names Supporting Organization (hereinafter "PIR Comments on WHOIS") accessible via http://gnso.icann.org/dnso/dnsocomments/comments-whois/Arc03/pdf00000.pdf.

[4] See "Privacy, Costs, and Consumers Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete", Robert Gellman, March 26, 2002, http://www.epic.org/reports/dmfprivacy.html; "Trust and Privacy Online: Why Americans Want to Rewrite the Rules", Pew Internet & American Life Project, August 20, 2000, http://www.pewinternet.org/reports/toc.asp?Report=19; and Graphic, Visualization, & Usability Center 7th WWW User Survey, April 1997, http://www.gvu.gatech.edu/user_surveys/survey-1997-04/#exec.

WHOIS data. Minimally, enforcement of accuracy and insurance of privacy safeguards should be concurrent.

2.3 WHOIS data is available to anyone with Internet access.

WHOIS data is globally, publicly accessible. Anyone with Internet access, including stalkers, corrupt governments who dislike international exposure, spammers, intellectual property lawyers, law enforcement, consumers, individuals, etc., has access to WHOIS data.[5] The important point to realize here is that WHOIS data lends itself to both good faith and bad faith uses, and that investigating fraud is only one of many uses of WHOIS data.

2.4 Does it makes sense to impose a rule that requires all domain registrants to make their WHOIS data globally, publicly accessible?

Given that we have various types of domain name registrants – from individuals, who may have legitimate reasons for anonymous speech, to Internet scam artists; that anyone with Internet access – from individuals, law enforcement, to scam artists – can access WHOIS data for any reason and use the data in any way; and that WHOIS data consists of personally identifiable information, does it makes sense to impose a rule that requires all domain registrants to make their WHOIS data globally, publicly accessible? ***The issues of privacy, free speech, and fraud must be considered before answering this question.***

3 Organization for Economic Cooperation and Development (OECD) Privacy Guidelines: The Starting Point For A Serious Discussion on WHOIS Privacy[6]

The OECD Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereinafter "OECD Privacy Guidelines") offer important international consensus on and guidelines for privacy protection. The OECD Privacy Guidelines establish eight principles for data protection that are widely used as the benchmark for assessing privacy policy and legislation.[7] These principles are Collection Limitation; Data Quality; Purpose Specification; Use Limitation; Security Safeguards; Openness; Individual Participation; and Accountability.[8]

---

[5] PIR Comments on WHOIS.

[6] Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 324-52 (EPIC 2002) ("OECD Privacy Guidelines").

[7] Marc Rotenberg, "What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy", Presented on February 7, 2000 at the Stanford Law School Symposium on Cyberspace and Privacy, http://stlr.stanford.edu/STLR/Symposia/Cyberspace/00_rotenberg_1/article.htm.

[8] Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 324-52 (EPIC 2002) ("OECD Privacy Guidelines").

Representatives from North America, Europe, and Asia drafted the original OECD Privacy Guidelines. Countries around the world, with varying cultures and systems of governance, have adopted roughly similar approaches to privacy protection with respect to the OECD Privacy Guidelines.[9] Thus, the OECD Privacy Guidelines reflect a broad consensus about how to safeguard the control and use of personal information in a world, and especially on the Internet, where data can flow freely across national borders.[10]

3.1 A serious discussion on privacy and WHOIS should begin with the framework set out by the OECD Privacy Guidelines.

The OECD Privacy Guidelines provide a well thought-out solution to challenging questions about international consensus on privacy and data protection that directly implicate WHOIS policies and practices. More importantly, the OECD Privacy Guidelines serve as a basis for a sensible WHOIS policy.

The following table serves to raise some issues and questions that surface immediately when analyzing current WHOIS policies and practices (as set forth by ICANN's Registrar Accreditation Agreement[11]) against the OECD Privacy Guidelines:

OECD Privacy Principle	WHOIS Resultant Issues and Questions
Collection Limitation: There should be limits to the collection of personal data; any such data collected should be obtained by lawful means and with the consent of the data subject, where appropriate.	Current WHOIS policy requires registrants to provide excessive information. For example, why is it necessary to collect a registrant's telephone and fax numbers? Worse yet, why should this data be published to the world? Current WHOIS policy also requires registrants to provide accurate WHOIS information, or otherwise forgo a domain name. This requirement does not conform to the standard definition of "consent" in the context of privacy and data protection.[12]

[9] Colin J. Bennett, "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data", Technology and Privacy: The New Landscape edited by Philip Agre and Marc Rotenberg, The MIT Press (Cambridge, 1997).

[10] Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 324-52 (EPIC 2002) ("OECD Privacy Guidelines").
Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 324-52 (EPIC 2002) ("OECD Privacy Guidelines").

[11] See Appendices A, B, and C.

[12] "Consent" is widely understood as any freely given specific and informed indication of a data subject's wishes by which the data subject signifies his agreement to personal data relating to him being processed. See Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 367-394 (EPIC 2002) ("European Union Data Protection Directive (1995)")

	Furthermore, are registrants even aware that their WHOIS information is globally, publicly accessible? Are registrants even aware of the policies set forth by ICANN's Registrar Accreditation Agreement?
Data Quality: Collected data should be relevant to a specific purpose, and be accurate, complete, and up-to-date.	Current WHOIS policy fails to conform to this principle, since the purposes for the collection and disclosure of WHOIS data is at best unclear. Current WHOIS policy requires accurate information, and the WHOIS Task Force has recommended enforcement of accuracy.[13] The key point to note here is that the OECD Privacy Guidelines consider accuracy in context of a framework that establishes appropriate privacy safeguards, while the WHOIS Task Force considers accuracy independently of privacy.
Purpose Specification: The purpose for collecting data should be settled at the outset.	The purposes for which WHOIS data is collected and disclosed is not settled at the outset.[14] Historically, only the technical contact information for domain names was necessary to maintain the stability of the Internet. Over time, other purposes came into practice.[15] Regardless, current WHOIS policy fails to conform to this principle entirely.
Use Limitation: The use of personal data ought be limited to specified purposes, and that data acquired for one purpose ought not be used for others.	Current WHOIS policy fails to conform to this principle.[16]
Security Safeguards: Data must be collected and stored in a way reasonably calculated to prevent its loss, theft, or modification	Current WHOIS policy fails to conform to this principle, since WHOIS data is globally, publicly accessible, and through an insecure port.
Openness: There should be a general position of	WHOIS policy strings across ICANN, registries, registrars, and finally the

[13] See the WHOIS Task Force's "Final Report of the GNSO Council's Whois Task Force Accuracy and Bulk Access", February 6, 2003, http://www.icann.org/gnso/whois-tf/report-06feb03.htm.
[14] See ICANN's Registrar Accreditation Agreement (RAA), May 17, 2001, http://www.icann.org/registrars/ra-agreement-17may01.htm.
[15] See Section 2.2 of this report.
[16] Id.

transparency with respect to the practices of handling data.	registrant. It is not clear whether registrants are aware of this chain and of the various policies that implicate them.
Individual Participation: Individual should have the right to access, confirm, and demand correction of their personal data.	ICANN's Registrar Accreditation Agreement requires registrars to provide notice to each new or renewed registrant stating how the registrant can access and, if necessary, rectify the data held about them.
Accountability: Those in charge of handling data should be responsible for complying with the principles of the privacy guidelines.	Those in charge of handling WHOIS data are currently not complying with the OECD Privacy Guidelines principles.[17]

A serious discussion on privacy and WHOIS should begin with the framework set out by the OECD Privacy Guidelines. A new Task Force should resolve the aforementioned issues immediately.

3.2 The International Working Group on Data Protections in Telecommunications' comments that WHOIS policies and practices do not reflect the goal of privacy and data protection indicate that current WHOIS policies and practices do not reflect international consensus.[18]

The International Working Group on Data Protections in Telecommunications (hereinafter "the Working Group") pointed out problems with WHOIS policies and practices with respect to privacy and data protection:

> "The current Registrar Accreditation Agreement (RAA) developed by ICANN does not reflect the goal of the protection of personal data of domain name holders in a sufficient way. The Working Group therefore recommends that the following topics be addressed in future versions of the RAA:.… The amount of data collected and made publicly available in the course of the registration of a domain name should be restricted to what is essential to fulfill the purpose specified. In this respect the Working Group has reservations against a mandatory publication of any data exceeding name (which might also be the name of a company and not of a natural person), address and e-mail-address in cases where the domain name holder is not himself responsible for the technical maintenance of the domain but has this done through a service provider (as is the case with many private persons who have registered domain names).…Any additional data (especially telephone and fax number) - although they might be collected by the registry as necessary with respect to its task - should in such cases either refer to the respective service provider or only be made available with the explicit consent of the data subject.… At the

[17] See ICANN's Registrar Accreditation Agreement (RAA), May 17, 2001, http://www.icann.org/registrars/ra-agreement-17may01.htm.
[18] PIR Comments on WHOIS.

> same time, any secondary use incompatible with the original purpose specified (e.g. marketing) should be based on the data subject´s informed consent."[19]

In other words, the Working Group commented that WHOIS policies and practices do not reflect the goal of privacy and data protection. The Working Group's comments reflect an evaluation of WHOIS policies and practices with respect to the principles set forth by the OECD Privacy Guidelines. Furthermore, the Working Group's comments indicate that current WHOIS policies and practices do not reflect international consensus. A new task force should resolve the issues raised by the Working Group immediately.

4 Free Speech, Privacy and Anonymity[20]

On December 10, 1948, the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights, which enumerates a list of rights to which all people are entitled.[21] This list includes free speech:

> ARTICLE 19. Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

It is well understood that the Internet – including chat rooms, email, newsgroups, websites, and domain names – is an unprecedented media through which many people exercise their free speech, including controversial religious and political speech.

4.1 The pinnacle of privacy is anonymity.

In the context of the OECD Privacy Guidelines, privacy may be understood as control of your own personal information, control over what others (other people, private organizations, and the government) know about you, and control over how others may use or exploit your personal information. Furthermore, policies and practices that respect privacy aim at minimizing the collection of personally identifiable information. Then intuitively, the starting point of privacy is anonymity, where no personally identifiable information is collected. Compelling the disclosure of personally identifiable information, as current WHOIS policies dictate, directly undermines privacy.

---

[19] International Working Group on Data Protection in Telecommunications, "Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet", May 4-5, 2000, http://www.datenschutz-berlin.de/doc/int/iwgdpt/dns_en.htm#TOP.

[20] PIR Comments on WHOIS.

[21] Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 367-394 (EPIC 2002) ("Universal Declaration of Human Rights (1948)")

4.2 The critical relationship between privacy, anonymity, free speech, and Internet free speech should not be disregarded.[22]

Privacy is critical to free speech. As a simplified explanation, if speakers are compelled to disclose their identity, speakers are reluctant to fully express their speech for fear of persecution. We established that the pinnacle of privacy is anonymity; hence, as a corollary, anonymity is critical for individuals to achieve their fullest ability to exercise free speech.

The United States courts in particular have recognized the importance of Internet free speech and the right of anonymity.[23] The Supreme Court's decision in Reno v. ACLU offers an opinion on why individuals and organizations would want to display material through the World Wide Web:

> Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer.[24]

For the purposes of political, artistic or controversial speech, the Internet is an unprecedented opportunity to reach a large audience at a relatively small cost.[25]

The one-to-many characteristics of the Internet through which an individual's speech can reach a global audience are further enhanced by the protection of anonymity.[26] In McIntyre v. Ohio Elections Commission, the Supreme Court upheld individuals' ability to distribute anonymous political leaflets and found:

> 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; and their ideas from suppression; at the hand of an intolerant society.[27]

Hence, the Supreme Court upheld the importance of anonymity for individuals to achieve their fullest ability to exercise free speech.

---

[22] PIR Comments on WHOIS.
[23] Daniel J. Solove and Marc Rotenberg, Information Privacy Law 427-37 (Aspen Publishers2003) ("Anonymity in Cyberspace").
[24] ACLU v. Reno, 521 U.S. 844, 896-97 (1997).
[25] See letter submitted by EPIC to U.S. House of Representatives Committee on the Judiciary Subcommittee on Courts, the Internet and Intellectual Property, July 12, 2001, http://www.epic.org/privacy/internet/whois_0701.html.
[26] Id.
[27] McIntyre v. Ohio Elections Commission, 514 U.S. 334, 357 (1995).

4.3 Requiring WHOIS data and then publicly disclosing the data have serious implications on free speech.

Under current WHOIS policies and practices, an individual who wants to create her own website must publicly disclose personal information and cannot remain anonymous.[28] ICANN's Registrar Accreditation Agreement, which requires registrants to supply accurate WHOIS data or otherwise forgo their domain name registration, places an unacceptable burden on the ability of individuals to maintain their anonymity and thus their fullest ability to exercise free speech on the Internet.[29]

4.4 Anonymizing proxy servers are not an adequate alternative.[30]

The establishment of an intermediary between the operator of a website and the general public may avoid short-term identification of the actual user of a particular domain name. However, for the most controversial artistic, political and religious speech, it will be difficult for an online speaker to find an intermediary that will offer to have her own identity made public in lieu of the actual speaker. In addition, the third-party licensing provision is unambiguous in stating that the intermediary will be directly liable for use of the domain name by the actual user.

5 Contribution Of Globally, Publicly Accessible WHOIS Information To Identity Theft And Other Fraud

The U.S. Federal Trade Commission (FTC) plays a critical role both in the investigation of consumer fraud and in the protection of consumers from fraud. According to the FTC's website, "The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them."[31]

In this vein, the FTC advises consumers not to disclose personal information, and if consumers choose to disclose personal information, they should know who is collecting the information, why the information is being collected, and how it is going to be used.[32] Not only does the global, public accessibility of WHOIS data contradict FTC's advice, but the consumer, as a domain name registrant, is stripped of these abilities, as the registrant has no way of knowing who collected his/her WHOIS data, why the information was collected, and how the collector intends to use the information.[33] Further yet, with the enforcement of the accuracy of WHOIS data, as is recommended by the WHOIS Task Force, consumers will not even have a choice on whether to disclose

[28] Daniel J. Solove and Marc Rotenberg, Information Privacy Law 431 (Aspen Publishers2003) ("Anonymity in Cyberspace").
[29] PIR Comments on WHOIS.
[30] Id.
[31] See, for example, http://www.ftc.gov/bcp/conline/pubs/online/dontharvest.htm.
[32] See Appendix D for a list that samples the FTC's privacy initiatives along with information on ways consumers can protect themselves from a number of frauds (or activities that could lead to fraud).
[33] PIR Comments on WHOIS.

their personal information. The alternative to relinquish a domain name is not giving consumers a genuine choice, and instead infringes on Internet free speech.

The global, public accessibility of WHOIS data imposes risks on domain name registrants, and may contribute to identify theft as well as other fraud. The FTC's guidelines in their effort to safeguard consumer privacy are applicable to the protection of domain name registrants; these safeguards should be appropriately enforced.

6 Evaluation of WHOIS Task Force Work

While the WHOIS Task Force has put two years of hard work behind WHOIS policies, unfortunately there are problems with their process and results. The WHOIS Task Force failed to adequately address privacy issues, failed to recommend appropriate privacy safeguards for domain name registrants with reasonable and legitimate expectations of privacy, and failed to assess the misuses of WHOIS data.[34]

The WHOIS Task Force postponed privacy by way of a privacy issues report, which by itself presents the unacceptable risk of privacy issues being dismissed or resolved unsatisfactorily[35] and especially when the WHOIS Task Force has made recommendations that directly implicate privacy without resolving such implications. Worse yet, for the GNSO Council to consider and initiate a new task force that would respond to the privacy issues report the WHOIS Task Force must submit the privacy issues report by March 11, 2003; however, the WHOIS Task Force has failed to submit an adequate privacy issues report by this timeline.[36]

6.1 The survey administered by the WHOIS Task Force is flawed.[37]

The WHOIS Task Force has argued that the WHOIS Task Force only focused on areas identified by the results obtained from a survey that was administered in the Summer of 2001 in order to:

1. solicit input from as many people as possible concerning the use of Whois service, and
2. assess whether changes should be considered to the current Whois policy adopted by ICANN.

[34] See the WHOIS Task Force's "Final Report of the GNSO Council's Whois Task Force Accuracy and Bulk Access", February 6, 2003, http://www.icann.org/gnso/whois-tf/report-06feb03.htm.
[35] The WHOIS Task Force is well aware of this risk (see http://gnso.icann.org/dnso/dnsocomments/comments-whois/Arc03/msg00004.html and http://gnso.icann.org/dnso/dnsocomments/comments-whois/Arc03/msg00006.html).
[36] Co-Chair Marilyn Cade of the WHOIS Task Force announced during the Task Force's teleconference on March 6, 2003 that there was not enough time for the WHOIS Task Force to submit a complete privacy issues report by March 11, 2003.
[37] See http://does-not-exist.net/whois/whois-survey-en-10jun01.htm for the survey.

The WHOIS Task Force noted that the survey questions were designed to focus on the purpose, use, and accuracy of the WHOIS service to establish the appropriate balance between competing interests.

The WHOIS Task Force has repeatedly acknowledged, "In no way should this survey be considered statistically valid; and that was not its intent...it is evident that some of the questions and choices for answers contained in the survey could have been designed better."

Specifically, there were no verification mechanisms of the status of the survey respondents (that is, the survey respondent could have falsely identified himself/herself as an "individual or household user"). Furthermore, there were no verification mechanisms to ensure that a survey respondent could not take the survey more than once. Finally, the survey was poorly designed, as the survey that was intended to assess WHOIS privacy issues repeatedly ignored requests made by some non-commercial constituency representatives to include questions specifically about privacy.

Nonetheless, the WHOIS Task Force has unfortunately based its areas of focus – namely, accuracy, uniformity, enhanced searchability, and bulk access/marketing – on the results of a poorly designed and improperly administered survey.

6.2 The WHOIS Task Force has overlooked the relationship between accuracy and privacy.

Some registrants have legitimate reasons for providing inaccurate WHOIS information – for example, to protect their privacy and protect their personally identifiable information from being globally, publicly accessible – and especially when there are no privacy safeguards in place. A number of studies demonstrate that when no privacy safeguards are in place, individuals often generally engage in privacy "self-defense." When polled on the issue, individuals regularly claim that they have withheld personal information and have given false information. See:

- Privacy, Costs, and Consumers Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete, (PDF Version) Robert Gellman, March 26, 2002, http://www.epic.org/reports/dmfprivacy.html;
- Trust and Privacy Online: Why Americans Want to Rewrite the Rules, Pew Internet & American Life Project, August 20, 2000, http://www.pewinternet.org/reports/toc.asp?Report=19; and
- Graphic, Visualization, & Usability Center 7th WWW User Survey, April 1997, http://www.gvu.gatech.edu/user_surveys/survey-1997-04/#exec.

The corollary of privacy “self-defense” practices is that establishing and implementing appropriate privacy safeguards first is one way to improve the accuracy of WHOIS data. Minimally, enforcement of accuracy and insurance of privacy safeguards should be concurrent.

In recommending the enforcement of accurate WHOIS data without establishing appropriate privacy safeguards, the WHOIS Task Force has overlooked a critical relationship between privacy and accuracy.

6.3 The WHOIS Task Force has failed to respond to critical critiques.

The WHOIS Task Force failed to recommend appropriate privacy safeguards for domain name registrants with reasonable and legitimate expectations of privacy and the WHOIS Task Force failed to assess the misuses of WHOIS data. A number of comments submitted to the WHOIS Task Force's recommendations report raise privacy and data misuse issues that the WHOIS Task Force has effectively ignored:

- there must be a provision for individuals to keep their personal phone numbers private (04 Dec 2002, see http://www.dnso.org/dnso/dnsocomments/comments-whois/Arc02/msg00005.html);
- unlimited public access to WHOIS data poses real risks to individuals (9 Dec 2002 , see http://www.dnso.org/dnso/dnsocomments/comments-whois/Arc02/msg00012.html);
- the Task Force has failed to properly and fully address community concerns regarding privacy (8 Jan 2003, http://www.dnso.org/dnso/dnsocomments/comments-whois/Arc02/msg00022.html);
- the availability of personally identifiable information on WHOIS raises major problems with respect to the increasingly serious problem of identity theft (08 Jan 2003, see http://www.dnso.org/dnso/dnsocomments/comments-whois/Arc02/msg00023.html);
- nothing in the Task Force's report answers the primary question regarding why personally identifiable information must be published to the public at all (9 Jan 2003, http://www.dnso.org/dnso/dnsocomments/comments-whois/Arc02/msg00025.html);
- choosing to use the domain name system for either personal or professional use should not be a cause for the abuse your name, address, phone number, fax number and e-mail (9 Jan 2003, http://www.dnso.org/dnso/dnsocomments/comments-whois/Arc02/msg00027.html);
- and more.

A number of privacy and data misuse issues have been expressed by way of comments to the Task Force's interim and final reports as early as July 2002. The International Working Group on Data Protections in Telecommunications' comments that WHOIS policies and practices do not reflect the goal of privacy and data protection were made available as early as May 2000.[38]

[38] See Section 3.2.

It is not clear why these points, which are central to the development of a sensible WHOIS policy, were not addressed.

7 Concluding Remarks And Recommendations

A new task force must be formed to further evaluate and resolve the privacy issues associated with WHOIS policies and practices. Further, a member from the noncommercial constituency who has expertise in privacy should chair this task force.

We further offer the following recommendations that should be considered by the new task force.

> **Recommendation 1:** Personal information, beyond that necessary for contacting system administrators about network or security problems, should not be included in the globally, publicly accessible database. International privacy standards, such as the OECD Privacy Guidelines, should apply to the collection and use of WHOIS data.
>
> **Recommendation 2:** Anonymous registration of domain names should be provided and should not be burdensome to Internet speakers who are engaging in political or religious speech.
>
> **Recommendation 3:** A study that considers whether the availability of WHOIS data contributes to consumer fraud, such as identity theft, should immediately be undertaken.
>
> **Recommendation 4:** Accuracy of WHOIS data should not be enforced until privacy issues are adequately resolved and appropriate privacy safeguards are implemented.

We look forward to the GNSO Council's balanced approach in creating a new task force that will undertake a full and fair evaluation of the privacy issues associated with WHOIS.

Appendix A

ICANN's current version of its Registrar Accreditation Agreement (RAA) requires registrars to provide public access to registrant data as specified below (excerpted from http://www.icann.org/registrars/ra-agreement-17may01.htm):

> 3.3.1 At its expense, Registrar shall provide an interactive web page and a port 43 Whois service providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar for each TLD in which it is accredited. The data accessible shall consist of elements that are designated from time to time according to an ICANN adopted specification or policy. Until ICANN otherwise specifies by means of an ICANN adopted specification or policy, this data shall consist of the following elements as contained in Registrar's database:
>
> 3.3.1.1 The name of the Registered Name;
>
> 3.3.1.2 The names of the primary nameserver and secondary nameserver(s) for the Registered Name;
>
> 3.3.1.3 The identity of Registrar (which may be provided through Registrar's website);
>
> 3.3.1.4 The original creation date of the registration;
>
> 3.3.1.5 The expiration date of the registration;
>
> 3.3.1.6 The name and postal address of the Registered Name Holder;
>
> 3.3.1.7 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and
>
> 3.3.1.8 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

Appendix B

Also, the current version of the RAA requires registrars to provide third-party bulk data access as specified below (excerpted from http://www.icann.org/registrars/ra-agreement-17may01.htm):

> 3.3.6 In addition, Registrar shall provide third-party bulk access to the data subject to public access under Subsection 3.3.1 under the following terms and conditions:
>
> > 3.3.6.1 Registrar shall make a complete electronic copy of the data available at least one time per week for download by third parties who have entered into a bulk access agreement with Registrar.
> >
> > 3.3.6.2 Registrar may charge an annual fee, not to exceed US$10,000, for such bulk access to the data.
> >
> > 3.3.6.3 Registrar's access agreement shall require the third party to agree not to use the data to allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass, unsolicited, commercial advertising or solicitations to entities other than such third party's own existing customers.
> >
> > 3.3.6.4 Registrar's access agreement shall require the third party to agree not to use the data to enable high-volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations.
> >
> > 3.3.6.5 Registrar's access agreement may require the third party to agree not to sell or redistribute the data except insofar as it has been incorporated by the third party into a value-added product or service that does not permit the extraction of a substantial portion of the bulk data from the value-added product or service for use by other parties.
> >
> > 3.3.6.6 Registrar may enable Registered Name Holders who are individuals to elect not to have Personal Data concerning their registrations available for bulk access for marketing purposes based on Registrar's "Opt-Out" policy, and if Registrar has such a policy, Registrar shall require the third party to abide by the terms of that Opt-Out policy; provided, however, that Registrar may not use such data subject to opt-out for marketing purposes in its own value-added product or service.

Appendix C

Finally, the current version of the RAA requires registrants to provide accurate WHOIS data, or otherwise forego their domain name registration (excerpted from http://www.icann.org/registrars/ra-agreement-17may01.htm):

> 3.7.7.1 The Registered Name Holder shall provide to Registrar accurate and reliable contact details and promptly correct and update them during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation; and the data elements listed in Subsections 3.3.1.2, 3.3.1.7 and 3.3.1.8.
>
> 3.7.7.2 A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration.

Appendix D

The following list samples the FTC's privacy initiatives along with information on ways consumers can protect themselves from a number of frauds (or activities that could lead to fraud):

FTC Identified Risk or Initiative	FTC Suggestion to Consumers
Don't Want Your Email Address Harvested? http://www.ftc.gov/bcp/conline/pubs/online/dontharvest.htm	**1. Consider "masking" your email address.** "johndoe@myisp.com" could be masked as "johndoe@spamaway.myisp.com" **2. Keep your private email address private:** • Use a separate screen name for online chatting. • Consider creating "disposable email addresses" for public postings in newsgroups or on websites, or for online purchases. • Consider using one email account for personal correspondence and another for public use. **3. Use a unique email address, containing both letters and numbers.**
How to Be Web Ready http://www.ftc.gov/bcp/conline/pubs/online/webready.html	**Keep private information private.** Smart surfers don't disclose personal information unless they know who's collecting it, why, and how it's going to be used. And they never disclose their password. …
Privacy: Tips for Protecting Your Personal Information http://www.ftc.gov/bcp/conline/pubs/alerts/privtipsalrt.htm	Every day you share personal information about yourself with others. It's so routine that you may not even realize you're doing it. You may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, buy a gift online, call home on your cell phone, schedule a doctor's appointment or apply for a credit card. Each transaction requires you to share personal information: your bank and credit card account numbers; your income; your Social Security number

	(SSN); or your name, address and phone numbers. It's important to find out what happens to the personal information you and your children provide to companies, marketers and government agencies. These organizations may use your information simply to process your order; to tell you about products, services, or promotions; or to share with others. And then there are unscrupulous individuals, like identity thieves, who want your information to commit fraud. Identity theft - the fastest-growing white-collar crime in America - occurs when someone steals your personal identifying information, like your SSN, birth date or mother's maiden name, to open new charge accounts, order merchandise or borrow money. Consumers targeted by identity thieves usually don't know they've been victimized. But when the fraudsters fail to pay the bills or repay the loans, collection agencies begin pursuing the consumers to cover debts they didn't even know they had. The Federal Trade Commission (FTC) encourages you to make sure your transactions - online and off - are secure and your personal information is protected. The FTC offers these tips to help you manage your personal information wisely, and to help minimize its misuse. • Before you reveal any personally identifying information, find out how it will be used and whether it will be shared with others. Ask about company's privacy policy: Will you have a choice about the use of your information; can you choose to have it kept confidential? …
IDENTITY THEFT[39]: Reduce Your Risk http://www.ftc.gov/bcp/conline/pubs/credit/idtheftamex.htm	… **Identity Theft Prevention Tips:** • • Safeguard your personal information.

[39] The FTC recently released its annual report, titled "National and State Trends in Identity Theft", analyzing consumer complaints about identity theft and listing the top ten fraud complaint categories reported by consumers. Identity theft was at the top of list -- continuing the trend for a third year -- constituting 43% of the complaints in the FTC's complaint database (referred to as Consumer Sentinel). The number of reported identity theft complaints increased from 31,117 in 2000 to 86,198 in 2001 to 161,819 in 2002. For FTC's report on "National and State Trends in Identity Theft", see http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf.

	• Do not share personal information with unknown persons or companies. • Carry with you only the information you need. • Order and review a copy of your credit report at least once a year. • Shred documents containing sensitive information before discarding. …

References

ACLU v. Reno, 521 U.S. 844, 896-97 (1997).

Lakshmi Chaudhry, "Virtual Refuge for Gay Muslims," Wired News, May 8, 2000, http://www.wired.com/news/print/0,1294,35896,00.html.

Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press 1992).

Colin J. Bennett, "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data", Technology and Privacy: The New Landscape edited by Philip Agre and Marc Rotenberg, The MIT Press (Cambridge, 1997).

Comments of the Public Interest Registry, the not-for-profit corporation that manages the .ORG registry, on the Final Report on Whois Accuracy and Bulk Access of the Whois Task Force of the Generic Names Supporting Organization ("PIR Comments on WHOIS"), http://gnso.icann.org/dnso/dnsocomments/comments-whois/Arc03/pdf00000.pdf.

Graphic, Visualization, & Usability Center 7th WWW User Survey, April 1997, http://www.gvu.gatech.edu/user_surveys/survey-1997-04/#exec.

Sarah Gauch, "Effects of Arab censorship blunted by Internet," Christian Science Monitor, January 29, 2001, http://archive.nandotimes.com/technology/story/0,1643,500304664-500488126-503379336-0,00.html.

ICANN's Registrar Accreditation Agreement (RAA), May 17, 2001, http://www.icann.org/registrars/ra-agreement-17may01.htm.

International Working Group on Data Protection in Telecommunications, "Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet", May 4-5, 2000, http://www.datenschutz-berlin.de/doc/int/iwgdpt/dns_en.htm#TOP.

McIntyre v. Ohio Elections Commission, 514 U.S. 334, 357 (1995).

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on September 23, 1980.

Privacy, Costs, and Consumers Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete, (PDF Version) Robert Gellman, March 26, 2002, http://www.epic.org/reports/dmfprivacy.html.

Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 367-394 (EPIC 2002) ("Universal Declaration of Human Rights (1948)")

Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 367-394 (EPIC 2002) ("European Union Data Protection Directive (1995)")

Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 367-394 (EPIC 2002) (“European Union Directive on Privacy and Electronic Communications (2002)”)

Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 324-52 (EPIC 2002) (“OECD Privacy Guidelines (1980)”).

Marc Rotenberg, "Review of Ruling the Root," EPIC Alert 9.14[7] (July 25, 2002)

Marc Rotenberg, "What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy", Presented on February 7, 2000 at the Stanford Law School Symposium on Cyberspace and Privacy, http://stlr.stanford.edu/STLR/Symposia/Cyberspace/00_rotenberg_1/article.htm.

Anya Schiffrin, "Analysis: China, the Net and free speech," The Industry Standard, February 16, 2001, http://www.cnn.com/2001/TECH/internet/02/16/huang.qi.idg/index.html.

Craig S. Smith, "Sect Clings to the Web in the Face of Beijing's Ban," New York Times, July 5, 2001, http://www.nytimes.com/2001/07/05/world/05FALU.html.

Daniel J. Solove and Marc Rotenberg, Information Privacy Law 427-37, 431 (Aspen Publishers2003) (“Anonymity in Cyberspace”).

Trust and Privacy Online: Why Americans Want to Rewrite the Rules, Pew Internet & American Life Project, August 20, 2000, http://www.pewinternet.org/reports/toc.asp?Report=19.

The U.S. Federal Trade Commission, Consumer Protection Information, http://www.ftc.gov/ftc/consumer.htm.

The U.S. Federal Trade Commission, “National and State Trends in Identity Theft”, January 22, 2003, http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf.

WHOIS Task Force Mail Archives, http://www.dnso.org/clubpublic/nc-whois/Arc00/maillist.html

WHOIS Task Force, “Final Report of the GNSO Council's Whois Task Force Accuracy and Bulk Access”, February 6, 2003, http://www.icann.org/gnso/whois-tf/report-06feb03.htm.