ELECTRONIC PRIVACY INFORMATION CENTER

Statement for the Record of

Marc Rotenberg, Executive Director
And
Ruchika Agrawal, IPIOP Science Policy Fellow
Electronic Privacy Information Center (EPIC)

Workshop on
Public/Private Partnerships to Combat Cross-Border Fraud on Cooperation Between the FTC and Domain Registration Authorities

Before the

Federal Trade Commission

February 19-20, 2003
Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC

A meaningful discussion of the accuracy of WHOIS data 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?
- 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.

Understanding WHOIS

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**
Domain ID:	D313895-LROR	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
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	Whois	

Street1: Registrant Street2: Name Server: Name Server: Name Server:	Server:whois.opensrs.net Referral URL:http://www.opensrs.org NS.2RAD.NET NS.PEREGRINEHW.COM NS2.2RAD.NET
	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.

Who are the domain name registrants? That is, whose WHOIS data is exposed?[1]

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.

Who has access to WHOIS data?

WHOIS data is globally, publicly accessible. Anyone with Internet access, including intellectual property lawyers, law enforcement, spammers, stalkers, individuals, etc., has access to WHOIS data.[2] 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.

Does one size fits all make sense?

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.

Privacy And Free Speech[3]

Global, public accessibility of accurate WHOIS data has serious implications on privacy and free speech.

The United States courts have recognized the importance of Internet free speech and the right of anonymity.[4] The Supreme Court's decision in Reno v. ACLU offers an

---

[1] 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.

[2] Id.

[3] Id.

[4] See Daniel J. Solove and Marc Rotenberg, Information Privacy Law 427-37 (Aspen Publishers2003) ("Anonymity in Cyberspace").

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.[5]

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.

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. In McIntyre v. Ohio Elections Commission, the Supreme Court upheld the 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.[6]

Enforcement of accurate WHOIS data places a burden on the ability of individuals to maintain their anonymity and thus their fullest ability to exercise free speech online.[7] Compelling the disclosure of personal information in such a manner implicates First Amendment rights and Internet free speech.[8]

Anonymizing proxy servers are not an adequate alternative.[9]

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,

---

[5] ACLU v. Reno, 521 U.S. 844, 896-97 (1997).
[6] McIntyre v. Ohio Elections Commission, 514 U.S. 334, 357 (1995).
[7] PIR Comments on WHOIS.
[8] The need for anonymous Internet activity, including the anonymous hosting of websites and domain name registration, is far from hypothetical. Different political, artistic and religious groups around the world rely on the Internet to avoid persecution - and anonymity will make this easier. See Lakshmi Chaudhry, "Virtual Refuge for Gay Muslims," Wired News, May 8, 2000, <http://www.wired.com/news/print/0,1294,35896,00.html>; 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>; 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>.
[9] PIR Comments on WHOIS.

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.

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

The 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."[10]

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.

[10] See, for example, http://www.ftc.gov/bcp/conline/pubs/online/dontharvest.htm.

	3. Use a unique email address, containing both letters and numbers.
How to Be Web Ready http://www.ftc.gov/bcp/conline/pubs/online/webredy.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[11]: Reduce Your Risk http://www.ftc.gov/bcp/conline/pubs/credit/idtheftamex.htm	… **Identity Theft Prevention Tips:** • Safeguard your personal information. • 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. …

In sum, 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. 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.[12] Further yet, with the enforcement of the accuracy of WHOIS data, consumers will not even have a choice on whether to disclose 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 importance of which has been recognized by U.S. Courts.

We appreciate the FTC's efforts in safeguarding consumer privacy and providing a plethora of information on how consumers can protect themselves from various forms of fraud. We expect that the FTC will similarly respond to the risks imposed by the global, public accessibility of WHOIS data for domain name registrants.

---

[11] 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.

[12] PIR Comments on WHOIS.

Concluding Remarks And Recommendations

We should evaluate and resolve the implications of the enforcement of accurate WHOIS data on privacy, free speech, and consumer fraud. We offer the following recommendations in this direction:

Recommendation 1: 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 2: 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.[13]

Recommendation 3: The FTC, or another appropriate organization, should produce an annual report on when/how WHOIS data is used by law enforcement and how useful it is in fraud investigations. This report should also include a study on whether the availability of WHOIS data contributes to consumer fraud, such as identity theft. Finally, the report should assess the Constitutional implications of compelling disclosure of personally identifiable information as a precondition for expressing political or religious views in the online world. Such an analysis should take free speech, privacy, and consumer fraud into account.

Recommendation 4: Accuracy of WHOIS data should not be enforced until an adequate resolution of and recommendation on privacy issues is achieved and implemented.

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