



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Bureau of Consumer Protection

J. Howard Beales, III
Director

August 6, 2001

Mr. Louis Touton
Vice President, General Counsel
Internet Corporation for Assigned Names and Numbers (ICANN)
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6601

Re: The ICANN DNSO Names Council *Whois* Survey

Dear Mr. Touton:

The staff of the Bureau of Consumer Protection of the Federal Trade Commission (FTC)* welcomes the opportunity to comment upon the issues raised in the survey of *Whois* database users being conducted by the ICANN Domain Names Supporting Organization (DNSO). The FTC is the federal government's primary consumer protection agency. Under the Federal Trade Commission Act, the agency's mandate is to take action against "unfair or deceptive acts or practices" and to promote vigorous competition in the marketplace.¹ In general, the Commission's efforts are directed toward stopping actions that threaten consumers' opportunities to exercise informed choice. The FTC is authorized to halt deception through civil actions filed by its own attorneys in federal district court, as well as through administrative cease and desist actions.

Since 1994, the FTC has used this authority to bring nearly 200 Internet-related cases, obtaining orders for more than \$180 million in consumer redress and injunctions prohibiting future illegal conduct. Many of the Commission's Internet cases have involved traditional scams that migrated online (e.g., pyramid schemes, miracle health cures, and credit repair scams) and an increasing number involve the use of new technology in devious ways to injure consumers. Whether traditional or high-tech, scams on the Internet can appear suddenly, spread rapidly, and disappear just as quickly. The challenge for law enforcement is to identify and stop rapidly the wrongdoers that harm consumers and undermine overall confidence in the burgeoning global online marketplace.

Although the Internet can be used to facilitate fraudulent practices, it has also become an increasingly valuable tool in the effort to fight fraud. Particularly useful is the *Whois* database of registration information about the operators of websites. When its registration data are accurate, *Whois* can help

* This comment represents the views of the staff of the Bureau of Consumer Protection of the Federal Trade Commission. They are not necessarily the views of the Federal Trade Commission or any individual Commissioner.

¹ 15 U.S.C. § 45(a).

law enforcers quickly identify actors responsible for online fraud. Apart from its utility as a tool for information gathering and communication, the Internet - actually the Domain Name System itself - offers a mechanism for bringing websites permeated by fraud to a rapid halt. Indeed, in a recent FTC enforcement action, the Court ordered that several domain name registrations be suspended by the registrar pending trial, effectively stopping the injurious practices.² The importance of accurate domain name registration information goes beyond the need to identify fraud operators. Because some online businesses do not provide sufficient identifying information on their websites, *Whois* information can provide consumers with a useful supplement to the website disclosures.

Survey Question 7 asks whether survey respondents have ever been harmed or inconvenienced because the *Whois* data received was inaccurate, incomplete, or out of date. For law enforcers working to prevent Internet fraud, the problem of false domain name registration information has become an impediment that slows the effective identification of law violators. Increasingly, Commission investigations are being hampered by registration information that is not only false, but sometimes clearly fictitious. For example, *Whois* information for "taboosisters.com," a website targeted in *FTC v. Pereira*,³ indicated that the domain name was registered to a company located at "4 Skin" Street in Amsterdam, with "Amanda Hugandkiss" listed as the administrative contact. In another Commission action, *FTC v. J.K. Publications, Inc.*,⁴ a query of the *Whois* database for a website operated by the defendants provided a street address of "here there, ca 10001" for the administrative and technical contacts. These examples do not appear to be isolated incidents. A sampling of *Whois* queries conducted by FTC staff turned up a number of domain names with facially false address information registered to "hacker," "FBI," "Bill Clinton," "Mickey Mouse," and "God."

The staff of the FTC's Bureau of Consumer Protection would, therefore, support measures to ensure that *Whois* data is current, complete, and accurate. Several measures already contained in ICANN's Accreditation Agreement with registrars apparently are aimed at addressing similar concerns. For example, the Agreement specifies that a domain registration applicant's willful failure to provide accurate information may result in the termination of the registration. The Accreditation Agreement also requires that, if registrars are notified of an inaccuracy in the registration information, they should "take reasonable steps to investigate that claimed inaccuracy." We urge ICANN to work with registrars to implement and enforce these provisions.⁵

Moreover, we urge ICANN to require registrars to provide information to law enforcement officials about domain name registrants upon request in appropriate circumstances. In December 1999, the Organization for Economic Cooperation and Development (OECD), an international organization consisting of 29 countries, issued Guidelines on Consumer Protection in Electronic Commerce. These Guidelines recommend that "businesses engaged in electronic commerce with consumers

² *FTC v. Pereira*, CV-99-1367-A (E.D.Va. filed Sept. 14, 1999) (Preliminary Injunction entered Sept. 21, 1999). See www.ftc.gov/os/1999/9909/index.htm#22.

³ *Id.*

⁴ *FTC v. J.K. Publ'ns*, 99 F. Supp. 2d 1176 (C.D. Cal. 2000).

⁵ The staff of the FTC's Bureau of Consumer Protection submitted a comment to ICANN in October 1999 that elaborates on this recommendation. This comment can be found at <http://www.ftc.gov/os/1999/9910/icann.htm>.

should provide accurate, clear and easily accessible information about themselves sufficient to allow, at a minimum . . . location of the business and its principals by law enforcement and regulatory officials.”⁶ Where this information is not provided on the registered websites, the *Whois* database can provide an important source of information to law enforcers to enable them to fight Internet fraud more effectively, thereby building consumer confidence in electronic commerce.

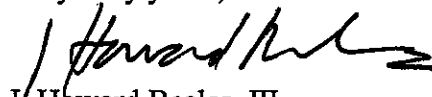
Survey Question 8.1 asks survey respondents who answer that the data elements currently available in the *Whois* database are inaccurate to specify additional data elements that should be included to promote public confidence in Internet activities. We suggest that current data element “G” (i.e., name and postal address of the registrant) should include either the telephone number or e-mail address. The OECD Guidelines referred to above state that consumers should have enough information about websites sufficient to identify the website operator. According to the Guidelines, this information should include, among other things, “the e-mail address or other electronic means of contact or telephone number.”⁷ This provision represents a consensus among the 29 member countries of the OECD as to the minimum information that consumers should be able to obtain about businesses operating websites, which we suggest should be considered by the ICANN DNSO.

Survey Question 10 asks whether survey respondents believe the publicly accessible *Whois* database should allow for searches on other data elements other than the domain name. The survey also asks respondents who respond in the affirmative to list those data elements that should be searchable. We would find the ability to search on other data elements besides the domain name very helpful in conducting law enforcement investigations given that we often need to determine whether a fraud artist has set up multiple websites. However, we would defer to the ICANN DNSO regarding how best to balance the increased utility provided by such searches against whatever costs may result.

In closing, on behalf of the staff of the FTC’s Bureau of Consumer Protection, I would again like to thank the ICANN DNSO for the opportunity to respond to the issues raised in its survey. The staff believes that accuracy of domain name registration information in the publicly available *Whois* database is vital to the efficient functioning of law enforcement efforts to combat online fraud and, thereby, help foster the continued growth of consumer confidence in this new medium. Accordingly, we recommend that steps be taken by ICANN and its constituent organizations to increase the accuracy of information in the publicly available *Whois* database. These steps should include implementing and enforcing the existing provisions of the ICANN Accreditation Agreement that require registrars to ensure that domain name registration information is accurate and to take steps if inaccuracies are brought to their attention. In addition, we recommend that the data elements in the *Whois* database be reflective of the OECD guidelines cited herein.

Inquiries regarding this comment may be directed to Bureau of Consumer Protection staff attorney Eric A. Wenger, 202.326.2310, ewenger@ftc.gov.

Very truly yours,



J. Howard Beales, III
Director

⁶ OECD Guidelines on Consumer Protection in Electronic Commerce, Section 3(a). See www.oecd.org.

⁷ *Id.*