PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

of the

HOUSE COMMITTEE ON FINANCIAL SERVICES

on

PUBLIC ACCESS TO WHOIS DATABASES

Washington, D.C.

July 18, 2006

I. Introduction

Good morning. Mr. Chairman and members of the Subcommittee, I am Eileen Harrington, a Deputy Director in the Bureau of Consumer Protection at the United States Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to appear before you today to discuss the importance of continued public and law enforcement access to Whois databases. Simply put, the FTC is concerned that attempts to limit the purpose of Whois

the proposed changes to Whois databases, voted to limit the purpose of Whois databases to technical purposes only.[3]

Because of its concern about preserving access to Whois databases, the FTC attended the ICANN meeting in Marrakech, Morocco last month to highlight the importance of public access to Whois databases. On behalf of the FTC, Commissioner Jon Leibowitz participated in a panel comprised of representatives of law enforcement agencies from other countries. He was joined by the Chairman of OPTA, the Independent Post and Telecommunications Authority in the Netherlands that enforces anti-spam laws, and a Deputy Director of Japan's Telecommunications Consumer Policy Division in the Ministry of Internal Affairs and Communications. Collectively, they emphasized the importance of law enforcement access to Whois databases and encouraged the GNSO to reconsider its decision to adopt the narrow purpose definition for Whois databases. The Commission understands that, in part because of these discussions, the GNSO is re-evaluating its decision.

The FTC is pleased to continue this dialogue today by providing this statement on the importance of public Whois databases in enforcing consumer protection laws and in empowering consumers. First, the testimony provides some general background about the FTC. Then, the testimony describes how the FTC uses Whois databases for its law enforcement purposes, discusses the importance of consumer and business access to Whois data about *commercial*

---

[3] The GNSO vote is not final. After considering other recommendations submitted by the Whois Task Force, the GNSO will make formal recommendations to the ICANN Board, which has the ultimate responsibility for making the final decision on any proposed changes to the Whois databases.

advertising and marketing on the Internet[13] and to consumers about what they should look for before making purchases and providing information online.[14]

III. How the FTC Uses Whois Databases

FTC investigators and attorneys have used Whois databases for the past decade in multiple Internet investigations. Whois databases often are one of the first tools FTC investigators use to identify wrongdoers. Indeed, it is difficult to overstate the importance of quickly accessible Whois data to FTC investigations.

For example, in the FTC's first spyware case, *FTC v. Seismic Entertainment*, the Commission alleged that the defendants exploited a known vulnerability in the Internet Explorer browser to download spyware to users' computers without their knowledge.[15] The FTC alleged that the defendants' software hijacked consumers' home pages, delivered an incessant stream of pop-up ads, secretly installed additional software programs, and caused computers to slow down severely or crash. The spyware in this case was installed using so-called "drive-by" tactics – exploiting vulnerabilities to install software onto users' computers without any notice. Using Whois data, the FTC found the defendants, stopped their illegal conduct, and obtained a

---

[13] *E.g.*, "Advertising and Marketing on the Internet - Rules of the Road," http://www.ftc.gov/bcp/conline/pubs/buspubs/ruleroad.htm.

[14] *See, e.g.*, "Consumer Guide to E-Payments," "Holiday Shopping? How to be Onguard When You're Online," http://www.ftc.gov/bcp/conline/pubs/alerts/shopalrt.htm, "How Not To Get Hooked By a Phishing Scam," http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm, and OnguardOnline.com (consumer education website providing practical tips concerning online fraud and other online threats).

[15] *FTC v. Seismic Entertainment, Inc.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

judgment for millions of dollars in consumer redress.[16] It is uncertain whether the FTC would have been able to locate the defendants without the Whois data.

In another matter, the FTC cracked down on companies that illegally exposed unwitting consumers to graphic sexual content without warning.[17]

In some instances, though, even inaccurate Whois information can be useful in tracking down Internet fraud operators. One of the FTC's recent spyware cases involved defendants that used free lyric files, browser upgrades, and ring tones to trick consumers into downloading spyware on their computers.[19] Rather than receiving what they opted to download, consumers instead received spyware with code that tracked their activities on the Internet. In this particular investigation, several of the defendants' websites were registered to a non-existent company located at a non-existent address. Despite the registrant's use of false information, FTC staff was able to link the websites to each other because all of the registrations listed the same phony name as the administrative contact in the Whois databases. Of course, with a "narrow purpose" Whois, not even such inaccurate registration information would be available.

Having "real-time" access to Whois data is particularly important for a civil law enforcement agency like the FTC. Where a registrar is located in a foreign jurisdiction, the FTC often has no other way to obtain the information it needs. The FTC cannot, in most cases, readily require a foreign entity to provide us with information. Thus, particularly in cross-border cases, Whois databases are often the primary source of information available to the FTC about fraudulent domain name registrants.[20]

---

[19] *FTC v. Enternet Media*, No. CV05-7777 CAS (C.D. Cal., filed Nov. 1, 2005).

[20] The number of cross-border complaints received by the FTC continues to rise. In 2005, 20% of the complaints in the FTC's Consumer Sentinel database had a cross-border component, compared to 16% in 2004, and less than 1% in 1995. *See* www.consumer.gov/sentinel.

In short, if ICANN were to restrict the use of Whois data to technical purposes only, it would greatly impair the FTC's ability to identify Internet malefactors quickly – and ultimately stop perpetrators of fraud, spam, and spy

---

The Red Cross recently explained how it used Whois data to shut down fraudulent websites that mimicked its website after Hurricane Katrina in connection with donation scams.[23] The simple yet crucial point is this: many legitimate uses of Whois data by the business community and other non-governmental organizations have an important, and often ignored, consumer protection dimension. Their continued access to Whois information often helps protect consumers from online scams and deception.

VI. Whois Databases and Privacy

Concerns about the privacy of domain name registrants have driven much of the Whois debate. The FTC, as the primary enforcement agency for U.S. consumer privacy and data security laws, is very concerned about protecting consumers' privacy. Thus, the Commission has always recognized that registrants engaged in non-commercial activity may require some privacy protection from *public* access to their contact information, without compromising appropriate real-time access by law enforcement agencies.[24] The FTC supports the further study of how this goal could be achieved. In the meantime, however, at the very least, the FTC believes that ICANN should preserve the status quo and reject limiting the Whois databases to technical uses.

Restricting public access to Whois data for *commercial* websites would deprive the public of the ability to identify and contact the operators of online businesses and would contravene well-settled international principles. If people want to do business with the public, they should

---

[23] *See* Red Cross Comment to GNSO Whois Task Force Preliminary Report, March 14, 2006, http://forum.icann.org/lists/whois-comments/msg00043.html.

[24] *See supra* note 2.

not be able to shield their basic contact information. The 1999 OECD Guidelines on Electronic Commerce state that consumers should have information about commercial websites "sufficient to allow, at a minimum, identification of the business. . . [and] prompt, easy and effective consumer communication with the business."[25] Thus, commercial website operators have no legitimate claim for privacy, and the public should continue to have access to their Whois data.[26]

Moreover, the existing availability of Whois databases can actually help enforcement agencies find out who is violating privacy laws and, consequently, help prevent er, esoey

summarizes the recommendations the Commission made to the ICANN community and then concludes with a recommendation that Congress consider enacting the US SAFE WEB Act, which the Senate passed on March 16, 2006.[27]

A. Recommendations to ICANN Community

The FTC made three recommendations to the ICANN community. First, the FTC recommended that the GNSO reconsider and reverse its position that the Whois databases should be used for technical purposes only. If this narrow purpose were to be adopted, the FTC, other law enforcement agencies, consumers, and businesses would

no reason to prevent access to contact information for a commercial website. The FTC urged ICANN to consider additional measures to improve the accuracy and completeness of domain name registration information. The FTC is also interested in exploring the viability of "tiered access" as a solution capable of satisfying privacy, consumer, and law enforcement interests.[28] Restricting the purpose of the Whois databases does not satisfy any of these interests and is a step in the wrong direction. Maintaining accessibility and enhancing the Whois databases would make great strides toward improving the safety and fulfilling the promise of the Internet.

B. US SAFE WEB Act

The FTC has previously recommended that Congress consider enacting the US SAFE WEB Act, passed by the Senate on March 16, 2006. The Commission continues to recommend enactment of this legislation, which would give it additional tools to fight fraud. Even with the current access to Whois databases, the Commission needs these additional tools. If the Commission's access to Whois data becomes unavailable, the Commission's need for the tools provided by the US SAFE WEB Act becomes even more crucial.

The US SAFE WEB Act would make it easier for the FTC to gather information about Internet fraud from sources other than Whois databases. For example, the US SAFE WEB Act would help the FTC obtain information and investigative assistance from foreign law enforcement agencies. It would also allow the FTC to obtain more information from the private sector and from financial institutions about Internet fraud. The FTC's ability to obtain

---

[28] Tiered access refers to a system in which different categories of stakeholders would get different levels of access to Whois databases.