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 databases will hinder its ability to protect consumers and their privacy.

As you know, Whois databases are information directories containing contact information about website operators. The FTC has long recognized that Whois databases are critical to the agency's consumer protection mission, to other law enforcement agencies around

[1] This written statement reflects the views of the Federal Trade Commission. My oral statements and responses to any questions you may have represent my own views, and do not necessarily reflect the views of the Commission or any individual Commissioner.

the world, and to consumers. In fact, four years ago, the Commission testified before Congress on the importance of improving the accuracy of information in Whois databases.[2]

[2] Prepared Statement of the Federal Trade Commission on "*The Integrity and Accuracy of the 'Whois' Database*," Before the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary, U.S. House of Representatives, May 22, 2002.

The Internet Corporation for Assigned Names and Numbers, commonly referred to as ICANN, is currently engaged in a policy development process that could modify the information that is maintained on public Whois databases. In April 2006, ICANN's Generic Names Supporting Organization ("GNSO"), the organizational body within ICANN that is evaluating 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

[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.

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* websites and other legitimate uses of Whois data, and addresses the privacy concerns that some stakeholders have raised about public access to Whois databases. The statement concludes with some of the FTC's recommendations on how to move forward.

II. FTC Enforcement of Consumer Protection Laws

The FTC is the only federal agency empowered to enforce both competition and consumer protection laws. The principal consumer protection statute that the FTC enforces is the FTC Act, which prohibits "unfair or deceptive acts or practices."[4] The FTC Act authorizes the FTC to stop businesses engaged in such practices. The FTC also can seek monetary redress and other equitable remedies for consumers injured by these illegal practices.

[4] 15 U.S.C. § 45.

The FTC has used its authority against "unfair or deceptive acts or practices" to take action against a wide variety of Internet-related threats, including Internet auction fraud,[5] Internet-based pyramid schemes,[6] websites making deceptive health claims,[7] and websites promoting "get rich quick" schemes.[8] More recently, the Commission has focused its actions against deceptive claims delivered through spam,[9] "phishing" schemes,[10] and spyware–all violations of consumer privacy that Whois data help us eliminate.[11] In many of these cases, the FTC has worked cooperatively with its consumer protection counterparts across the globe.

In addition, the FTC has made a high priority of protecting consumers' privacy and improving the security of their sensitive personal information, both online and offline. The FTC has brought several law enforcement actions targeting unfair and deceptive practices that involve the failure to protect consumers' personal information.[12] Indeed, the FTC recently created a new

---

[5] *E.g.*, *FTC v. Silverman*, No. 02-8920 (GEL) (S.D.N.Y., filed Aug. 30, 2004).

[6] *E.g.*, *FTC v. Skybiz.com, Inc.*, No. 01-CV-396-AA(M) (N.D. Okla. filed Jan. 28, 2003).

[7] *E.g.*, *FTC v. CSCT, Inc.*, No. 03C 00880 (N.D. Ill., filed Feb. 6, 2003).

[8] *E.g.*, *FTC v. National Vending Consultants, Inc.*, CV-5-05-0160-RCJ-PAL (D. Nev., filed Feb. 7, 2006).

[9] *E.g.*, *FTC v. Cleverlink Trading Limited*, No. 05C 2889 (N.D. Ill., filed May 16, 2005).

[10] *E.g.*, *FTC v. _____, a minor*, CV No. 03-5275 (C.D. Cal. filed 2003).

[11] *E.g.*, *FTC v. Enternet Media,* No. CV 05-7777 CAS (C.D. Cal., filed Nov. 1, 2005); *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. filed Sept. 21, 2005); *In the Matter of Advertising.com*, FTC Docket No. C-4147 (Sept. 12, 2005).

[12] *E.g.*, *In the Matter of DSW, Inc.,* FTC Docket No. C-4157 (Mar. 7, 2006); *In*

Division of Privacy and Identity Protection to address specifically the need to protect consumer privacy and the security of consumers' personal information.

---

the Matter of CardSystems Solutions, Inc., FTC Docket No. 052-3148 (proposed settlement
posted for public comment on Feb. 23, 2006); *United States v. ChoicePoint*, *Inc.*, No. 106-CV-0198 (N.D. Ga. filed Feb. 15, 2006); *In the Matter of BJ's Wholesale Club, Inc.,* FTC Docket No. C-4148 (Sept. 20, 2005).

The FTC also promotes consumer welfare in the electronic marketplace through education, outreach, and advocacy. For example, FTC staff provides guidance to businesses advertising and marketing on the Internet[13] and to consumers about what they should look for before making purchases and providing information online.[14]

---

[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).

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 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] The Commission

---

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

[16] *See* News Release, Court Halts Spyware Operations, May 4, 2006, http://www.ftc.gov/opa/2006/05/seismic.htm.

[17] *See* News Release, FTC Cracks Down on Illegal "X-Rated Spam," July 20, 2005,

charged seven entities with violating federal laws that require warning labels on e-mail containing sexually-explicit content. In these cases, accurate Whois information helped the FTC to identify the operators of websites that were promoted by the illegal spam messages.

---

http://www.ftc.gov/opa/2005/07/alrsweep.htm.

Information in Whois databases is most useful when it is accurate. Indeed, the Commission has advocated that stakeholders work to improve the accuracy of such information, because inaccurate data has posed significant obstacles in FTC investigations.[18]

[18] Prepared Statement of the Federal Trade Commission on "*The Integrity and Accuracy of the 'Whois' Database*," before the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary, U.S. House of Representatives, May 22, 2002 (noting that FTC had found websites registered to "God," "Mickey Mouse," and other obviously false names). FTC investigators have had to spend many additional hours tracking down fraud on the Internet because of inaccurate Whois data – hours that could have been spent pursuing other targets. *See also* U.S. Government Accountability Office, Report to the Subcommittee on Courts, The Internet, and Intellectual Property, House of Representatives, "Internet Management: Prevalence of False Contact Information for Registered Domain Names"

(Nov. 2005) (noting that, based on a random sample of domain names from the .com, .net, and .org domains, 8.65 percent of websites were registered with patently false or incomplete data in the required Whois contact information fields).

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

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

cross-border cases, Whois databases are often the primary source of information available to the FTC about fraudulent domain name registrants.[20]

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 spyware from infecting consumers' computers.

IV. How Consumers Use Whois Databases

Consumers also benefit from access to Whois data for commercial websites. Where a website does not contain contact information, consumers can go to the Whois databases and find out who is operating the website. This helps consumers resolve problems with online merchants directly, without the intervention of law enforcement authorities. Indeed, it is crucial that consumers continue to have the ability to settle disputes prior to–or instead of–law enforcement involvement.

[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.

Consumers do in fact regularly rely on Whois databases to identify the entities behind websites. FTC staff recently searched the FTC's database of consumer complaints, and found a significant number of references to the term "Whois." These results indicate that when consumers encounter problems online, the Whois databases are a valuable initial tool they use to identify with whom they are dealing. Consumer access to Whois also helps the FTC because it allows consumers to gather valuable contact information that they can pass on to the FTC – information that might no longer be available by the time the agency initiates an investigation because the website operators have moved on to different scams.

The Organization for Economic Cooperation and Development ("OECD") has recognized that consumer access to Whois data about commercial websites serves an important public policy interest. In 2003, the OECD Committee on Consumer Policy issued a paper unequivocally stating that "[f]or commercial registrants, all contact data should be accurate and publicly available via WHOIS."[21] In support of this conclusion, the paper says:

> Easy identification of online businesses is a key element for building consumer trust in the electronic marketplace. Because a Web site has no obvious physical presence, consumers are deprived of many of the usual identifying characteristics that help instil trust in a traditional retailer . . . While the most obvious location for an online business to provide contact

[21] OECD, *Consumer Policy Considerations on the Importance of Accurate and Available Whois Data*, DSTI/CP(2003)1/REV1 (April 30, 2003), available at http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-cp(2003)1-final.

details is on the Web site itself, domain name registration information can serve as a useful compliment [sic].[22]

This OECD paper represents an international consensus about the importance of accurate and accessible Whois data for consumers.

V. Other Legitimate Uses of Whois Data

There are other legitimate private users of Whois databases–businesses, financial institutions, non-governmental organizations, and intellectual property rights owners–all of which heavily rely on access to accurate Whois data. Although the FTC does not represent these entities' interests in the Whois debate, their use of Whois databases can help consumers. For example, a financial institution concerned about the misuse of its name by "spoofing" its website is not only protecting its own business interests, but it is also protecting its customers from being "phished."

[22] *Id.*

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

---

[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.

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 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 the misuse of consumers' personal information. For example, Whois databases were invaluable in FTC investigations in phishing cases where the defendants sought to steal sensitive personal and financial information from consumers. In addition, the spyware cases discussed earlier also involve serious threats to consumer privacy, as spyware can monitor

---

[25] OECD, *Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999), available at http://www.oecd.org/dataoecd/18/13/34023235.pdf.

[26] Consistent with this approach, the European Union's Distance Selling Directive *requires* that European websites ***selling*** to consumers include the name and address of the website operator. European Distance Selling Directive (Directive 97/7/EC), Article 4.

consumers' Internet habits and can even retrieve sensitive consumer information, including financial information, by logging keystrokes. Whois data has helped the FTC to stop these privacy violations and, hopefully, will continue to do so.

VII. Recommendations

In light of the FTC's experience in enforcing consumer protection laws, the FTC made several recommendations to the ICANN community at its meeting last month. This testimony 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 not be able to use the Whois databases for their legitimate needs. This would hurt consumers around the world and could allow Internet malefactors to violate consumer privacy with impunity. The Commission understands that the GNSO is currently taking steps to incorporate the input of the FTC and other law enforcement agencies into its final recommendation to the ICANN board.

[27] Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers across Borders (US SAFE WEB Act), S. 1608, 109th Cong. (2006) (as passed by Senate, Mar. 16, 2006).

Second, the FTC encouraged members of ICANN's Governmental Advisory Committee ("GAC") to continue their outreach with law enforcement colleagues in their respective countries to reinforce the serious law enforcement and consumer protection implications of losing access to Whois databases. The Commission is pleased to note that GAC members from several countries are undertaking such an effort.

Third, the FTC recommended that ICANN carefully consider improvements in Whois databases. For example, as the OECD statements referenced above make clear, there is simply 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.

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

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 information under the US SAFE WEB Act is no substitute for real-time, desktop access to Whois data. Where such data is limited, inaccurate, unavailable, or inapplicable, however, having access to a broader range of investigative sources about Internet and other cross-border fraud would surely help.

VIII. Conclusion

In sum, the FTC believes that improvements need to be made to the current Whois database system and is committed to working with others toward a solution. In the meantime, ICANN should ensure that Whois databases are kept open, transparent, and accessible so that agencies like the FTC can continue to protect consumers, and consumers can continue to protect

themselves. Further, Congress should enact the US SAFE WEB Act to provide the FTC with additional tools to fight Internet and other fraud. Together, these tools will help ensure that consumers are free from deceptive practices that undermine the promise of the Internet.