Prepared Statement of the Federal Trade Commission
before the
Internet Corporation for Assigned Names and Numbers ("ICANN")
Meeting Concerning Whois Databases
Marrakech, Morocco
June 2006

I. Introduction

Good morning. I am pleased to have this opportunity to speak here today about Whois databases. I am Jon Leibowitz, one of five Commissioners of the United States Federal Trade Commission ("FTC" or "Commission") in Washington, D.C.[1] The FTC is an independent federal agency of the United States government, the lead agency charged with protecting Americans' privacy, and the only agency in the United States empowered to enforce both competition and consumer protection laws.

The FTC believes that the Whois databases, despite their limitations, are nevertheless critical to the agency's consumer protection mission, to other law enforcement agencies around the world, and to consumers. The use of these databases to protect consumers is at risk as a result of the Generic Names Supporting Organization's ("GNSO") recent vote to define the purpose of Whois data as technical only. The FTC is concerned that any attempt to limit Whois to this narrow purpose will put its ability to protect consumers and their privacy in peril.

The principal consumer protection statute that the FTC enforces is the FTC Act, which prohibits "unfair or deceptive acts or practices."[2] The FTC Act authorizes the FTC to stop

---

[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.

[2] 15 U.S.C. § 45.

businesses engaged in such practices. The FTC also can seek monetary redress and other equitable remedies for consumers injured by these illegal practices. The FTC is a ***civil*** law enforcement agency without criminal authority.

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,[3] Internet-based pyramid schemes,[4] websites making deceptive health claims,[5] and websites promoting "get rich quick" schemes.[6] More recently, the Commission has focused its actions against deceptive claims delivered through spam,[7] "phishing" schemes,[8] and spyware.[9] In many of these cases, the FTC has worked cooperatively with its consumer protection counterparts across the globe. The FTC's goal in bringing these cases has been to help ensure that consumers are free from deceptive practices that undermine the promise of the Internet.

---

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

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

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

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

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

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

[9] *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).

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.[10] Indeed, the FTC recently created a new Division of Privacy and Identity Protection to address specifically the need to protect consumer privacy and the security of consumers' personal information.

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.[11] FTC staff educates consumers about what they should look for before making purchases and providing information online.[12] The Commission also advocates before legislative bodies; on several recent occasions, for example, the Commission has testified before Congress on protecting consumer privacy and data security.[13]

---

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

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

[12] *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).

[13] *See* http://www.ftc.gov/ftc/congress.htm/os/testimony/109hearings.htm.

This statement addresses the importance of public Whois databases in enforcing consumer protection laws and in empowering consumers. It describes how the FTC uses Whois databases for its law enforcement purposes, discusses the importance of consumer access to Whois data about commercial websites and other legitimate uses of Whois data, addresses the privacy concerns that some stakeholders have raised about public access to Whois databases, and concludes with some of the FTC's recommendations on how to move forward.

II. 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.[14] The FTC alleged that the defendants' software hijacked consumers' home pages, resulted in an incessant stream of pop-up ads, allowed the secret installation of additional software programs, and caused computers to slow down severely or crash. The software 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

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

conduct, and obtained a judgment for millions of dollars in consumer redress.[15] 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.[16] The Commission 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.

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.[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

---

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

[16] *See* News Release, FTC Cracks Down on Illegal "X-Rated Spam," July 20, 2005, http://www.ftc.gov/opa/2005/07/alrsweep.htm.

[17] 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).

used free lyric files, browser upgrades, and ring tones to trick consumers into downloading spyware on their computers.[18] 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.[19]

In short, if ICANN restricts the use of Whois data to technical purposes only, it will greatly impair the FTC's ability to identify Internet malefactors quickly – and ultimately stop perpetrators of fraud, spam, and spyware from infecting consumers' computers.

---

[18] *FTC v. Enternet Media, et al., Civil Action* No. CV05-7777CAS (AJWx) (C.D. Cal. Oct 27, 2005).

[19] 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.

III. 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 can help consumers resolve problems with online merchants directly, without the intervention of law enforcement authorities.

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."[20] In support of this conclusion, the paper says:

---

[20] 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.

> 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 details is on the Web site itself, domain name registration information can serve as a useful compliment [sic].[21]

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

IV. Other Legitimate Uses of Whois Data

There are other legitimate private users of Whois databases whose views and concerns should be reflected in the Whois policy development process at ICANN. These are 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 trademark owner concerned about the misuse of its name by "spoofing" its website is not only protecting its own business interests but is protecting its customers from being "phished."

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.[22] The simple yet crucial point is this: many legitimate uses of Whois data by the business

---

[21] *Id.*

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

community and other non-governmental organizations have an important, and often ignored, consumer protection dimension.

V. 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 non-commercial registrants may require some privacy protection from *public* access to their contact information, without compromising appropriate real-time access by law enforcement agencies.[23] The FTC supports the further study of how this goal could be achieved. In the meantime, however, at the very least, ICANN should preserve the status quo and reject limiting the Whois databases to technical uses.

Restricting public access to Whois data for commercial websites and depriving the public of the ability to find information about such websites would contravene well-settled international principles. 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."[24] Thus, commercial website operators have no legitimate claim for privacy, and the public should continue to have access to their Whois data.

---

[23] *See supra* note 17.

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

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 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.

VI. Recommendations

Based on the foregoing discussion of the FTC's consumer protection and law enforcement experience, the FTC respectfully makes the following recommendations. First, the GNSO should reconsider and reverse its position that the Whois databases should be used for technical purposes only. If this narrow purpose is adopted, the FTC, other law enforcement agencies, businesses, and consumers will 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 FTC recommends that the GNSO reverse its position *at this stage* and *before* the Whois task force considers other outstanding Whois issues in light of this narrow definition.

Second, the FTC has found it immensely helpful in developing its position to reach out to consumer protection and law enforcement partners in the United States and overseas. The FTC

is particularly pleased to be joined today by consumer protection enforcement colleagues from other countries who will share their views. The FTC is confident that such outreach between ICANN's Governmental Advisory Committee ("GAC") representatives and their consumer protection and law enforcement colleagues will reinforce the serious law enforcement and consumer protection implications of losing access to Whois databases. Certainly, the current direction of the Whois debate will seriously impair efforts of criminal and civil law enforcement agencies to stop online fraud and other illegal conduct.

Third, the FTC recommends carefully considering 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 urges 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.[25] 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 fulfilling the promise and safety of the Internet.

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,

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

Whois databases should be kept open, transparent, and accessible so that agencies like the FTC can continue to protect consumers, and consumers can continue to protect themselves.