

**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/online/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/online/pubs/alerts/shopalrt.htm>, "How Not To Get Hooked By a Phishing Scam," <http://www.ftc.gov/bcp/online/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-

c/TT0 1 Tf0.C,.12 0 0 12 388leT0 1 Tf12 0 0 12 08 Tw 12recom

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](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 W

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 inform

is particularly pleased to be joined today by consumer protection enforcement colleagues from

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.