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
United States House of Representatives

Washington, D.C.

May 22, 2002

Mr. Chairman, I am Howard Beales, Director of the Bureau of Consumer Protection at the Federal Trade Commission. I am pleased to be here today to discuss the importance of accurate domain registration information in the Whois database to our consumer protection mission.(1) As you know, the Whois database is the popular name for a combination of information directories containing registration information about website operators.

The FTC's consumer protection efforts include fighting Internet fraud. Because fraudulent website operators can defraud consumers quickly and disappear quickly, we need to move just as quickly to find them and stop them. The Whois database - when it is accurate - can help law enforcers quickly identify wrongdoers and their location, halt their conduct, and preserve money to return to defrauded consumers. Inaccurate Whois data, however, help Internet scam artists remain anonymous and stymie law enforcement efforts.(2)

The testimony will begin with a general overview of the FTC and its enforcement authority, the challenges we have faced in fighting Internet fraud, and how we work to overcome those challenges. Second, we will discuss the importance of the Whois database to these efforts and the problems we encounter when Whois information is inaccurate. Third, we will address current registrar practices with respect to Whois information. Finally, the testimony will close with a few words about the balancing of privacy interests of domain registrants and the interest of other stakeholders in the transparency of Whois information.

I. The FTC's Fight Against Internet Fraud

A. The FTC's Law Enforcement Authority

The FTC is an independent agency charged with protecting consumers and promoting a competitive marketplace. The cornerstone of the Commission's mandate is Section 5 of the Federal Trade Commission Act, which prohibits "unfair methods of competition" and "unfair or deceptive acts or practices."(3) The FTC focuses on stopping actions that threaten consumers' opportunities to exercise informed choice. The FTC halts deception through civil actions filed by its own attorneys in federal district court, as well as through administrative cease and desist actions.(4)

B. The Challenges Posed by Internet Fraud

The Internet and e-commerce have seen dramatic growth. The number of American adults with

Internet access has grown, by one estimate, from approximately 88 million in mid-2000 to more than 174 million in March 2002.(5) The Census Bureau of the Department of Commerce estimated that in the fourth quarter of 2001, not adjusted for seasonal, holiday, and trading-day differences, online U.S. retail sales were more than $10 billion, an increase of 13.1 percent from the fourth quarter of 2000. Total e-commerce sales for 2001 were estimated at $32.6 billion, an increase of 19.3 percent from 2000.(6)

Unfortunately, but not surprisingly, the e-commerce boom of the last several years has created fertile ground for fraud. In 2001, close to 50,000 complaints - roughly 41 percent of all complaints logged into the FTC's fraud database, Consumer Sentinel, by various organizations that year - were Internet-related.(7)

There is real danger that the benefits of the Internet may not be fully realized if consumers identify the Internet with fraud operators. We need to act quickly to stop fraud, both to protect consumers and to protect consumer confidence in e-commerce. We have therefore made fighting Internet fraud a top priority. Since 1994, the FTC has brought more than 225 Internet-related law enforcement actions against 688 defendants and respondents, stopping consumer injury estimated at more than $2.1 billion.

The Commission faces a host of novel challenges in its efforts to combat fraud and deception online. Traditional scams - such as pyramid schemes and false product claims - thrive on the Internet. A colorful, well-designed Web site imparts a sleek new veneer to an otherwise stale fraud; and the reach of the Internet also allows an old-time con artist to think - and act - globally. Moreover, the architecture of the Internet itself has given rise to new high-tech scams that were not possible before the development of the Internet. Both traditional scams and the innovative ones exploit the global reach and instantaneous speed of the Internet. In addition, the Internet enables con artists to cloak themselves in anonymity, which makes it necessary for law enforcement authorities to act much more quickly to stop newly-emerging deceptive schemes before the perpetrators disappear. And because the Internet transcends national boundaries, law enforcement authorities must be more creative and cooperative to successfully combat online fraud.

C. The FTC's Efforts to Fight Internet Fraud

Given the speed with which Internet fraudsters can con consumers, the Commission has worked to identify problems and go after perpetrators rapidly. In light of the challenges posed by the borderless nature of the Internet, the Commission has worked to gather information from international sources and cooperate with its foreign counterparts through multilateral and bilateral efforts. Some of the tools we have used to accomplish these goals include the following:

- **Databases**: To gather information quickly, the Commission has developed Consumer Sentinel, a web-based consumer complaint database that is accessible to more than 420 law enforcement organizations in the U.S., Canada and Australia.(8) In 2001, numerous organizations in the U.S. and Canada contributed more than 200,000 consumer complaints to Consumer Sentinel.(9) These complaints can help us identify trends and target fraudsters quickly and efficiently.

- **International Cooperation**: The Commission cooperates with its international counterparts to meet the challenges posed by cross-border fraud. The FTC is a member of the International Marketing Supervision Network (IMSN), a group of 30 consumer protection enforcement agencies that meets twice a year to discuss cross-border cooperation.(10) Fifteen IMSN countries have launched econsumer.gov, a public website where consumers can file cross-border e-commerce complaints online that are accessible to law enforcement agencies in the member countries. The site is available in English,

French, Spanish and German.(11) Complaints from econsumer.gov can help us identify trends and fraudsters on an international level. The FTC has also signed consumer protection cooperation agreements with Canada, the U.K. and Australia, which has enhanced our cooperation with these countries.(12)

- **Surf Days:** The Commission also coordinates law enforcement Surf Days to help identify international fraudsters. During a typical surf day, law enforcers at the federal, state, local and international levels "surf" the Internet for a specific type of claim or solicitation that is likely to violate the law. When a suspect site is identified, the page is downloaded and saved as potential evidence. Frequently, the operator of the site is sent a warning that explains the law and provides a link to educational information. Often, investigators obtain the e-mail or postal address from Whois information in order to send such warnings. A law enforcement team later revisits the previously warned sites to determine whether they have remedied their questionable claims or solicitations. Sites that continue to make unlawful claims are targeted for possible law enforcement action. Surf days achieve visible results: to date, more than 250 law enforcement agencies and consumer organizations around the world have joined the FTC in approximately 33 surf days; collectively, they have identified more than 6,000 Internet sites making dubious claims. In each of these efforts, a significant percentage of the Web site operators who received a warning came into compliance with the law, either by taking down their sites or by modifying their claims or solicitations.

- **Sweeps**: The FTC also coordinates law enforcement sweeps, both domestically and internationally, and here too Whois information can play an important role. In our experience, "sweeps" of a particular area can generate substantial publicity, which can in turn provide meaningful consumer education and further deter fraudulent conduct in that area. In "Operation Top Ten Dot Cons," for example, law enforcement agencies from nine countries announced 251 law enforcement actions against online companies. More recently, the FTC announced earlier this month that it had joined forces with 12 other U.S. and Canadian agencies to form an International Netforce targeting deceptive spam and Internet fraud. The agencies brought 63 law enforcement actions against Web-based scams, ranging from auction fraud to bogus cancer cure sites, and sent more than 500 warning letters to senders of deceptive spam.(13)

- **Internet Training**: Recognizing that law enforcement officials have to be one step ahead of the technology used by scam artists, the FTC has also hosted Internet training seminars. Since FY 2001, the Commission has educated more than 1,750 law enforcement personnel from more than 20 countries, 38 states, 23 U.S. federal agencies, and 19 Canadian agencies.

- **Internet-Based Tools**: The Commission also provides its staff with the tools they need to investigate high-tech fraud quickly, anonymously, and efficiently. The FTC's Internet Lab is an important example. With high speed computers that are separate from the agency's network and equipped with current hardware and software, the Lab allows staff to investigate fraud and deception in a secure environment and to preserve evidence for litigation. Staff often conducts Whois searches in the Internet lab.

II. The Importance of Whois Data

You have asked us to discuss the importance of accurate Whois data to our work. Such a discussion necessarily takes place against the backdrop of discussions about ICANN reform. Interested stakeholders are actively discussing various reform proposals.

It is hard to overstate the importance of accurate Whois data to our Internet investigations. In all of

our investigations against Internet companies, one of the first tools FTC investigators use to identify wrongdoers is the Whois database. We cannot easily sue fraudsters if we cannot find them. We cannot even determine which agency can best pursue them if we are unable to figure out the country in which they are located.

The pace of Internet fraud makes it necessary to obtain rapidly the basic identifying information about the operator of a website. The existing Whois database does not serve this function as well as it could. Indeed, one survey on e-commerce issues by the Australian Taxation Office found that 10 to 15 percent of the data in the Whois database is inaccurate.(14)

A. FTC Experience with Inaccurate Whois Data

FTC investigations are being hampered by registration information that is not only false, but sometimes blatantly so. For example, Whois information for "taboosisters.com," a website targeted in *FTC v. Pereira*,(15) 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 *FTC v. J.K. Publications, Inc.*,(16) a Whois query 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. An informal 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." Several recent searches have turned up false phone numbers such as 555 555-5555 and 888 888-8888. One recent search for Whois information listed the organization, administrative, technical and zone contact as "xxxxxxxxxxxxxx." Another listed U.S. address information for a business that in fact operated from another continent.

Besides hampering our law enforcement investigations, inaccurate Whois data decreases the effectiveness of our Surf Days. As described above, the FTC and its law enforcement partners often "surf" the Internet for particular types of claims and send warning messages to sites that make potentially deceptive or misleading claims, following up later to determine if enforcement action is appropriate. Surfers rely on Whois data to find addresses for this purpose. If the Whois data are not accurate, the utility of the Surf Day as a law enforcement tool is diluted.

Problems with inaccurate Whois data were illustrated in a surf conducted by the FTC and its law enforcement partners in connection with the recent "International Netforce" initiative described above. One part of this initiative was a surf to test compliance with "remove me" or "unsubscribe" options.(17)

The object of the surf was to test whether "remove me" or "unsubscribe" options in spam were being honored. From e-mail forwarded to the FTC's database of unsolicited commercial e-mails by the participating agencies, we culled more than 200 e-mails that purported to allow recipients to remove their name from a spam list. The agencies set up dummy e-mail accounts to test the pledges. We discovered that most of the addresses to which they sent the requests were invalid. Most of the "remove me" requests did not get through. Based on information gathered, the FTC sent 77 letters warning spammers that deceptive "removal" claims in unsolicited e-mail are illegal. We sent the letters to addresses listed in the Whois database. Interestingly, 16 of the 77 letters, or approximately 21 percent, were sent back to us because the addresses we obtained from the Whois database were inaccurate. We have notified the registrars of this inaccuracy and have encouraged them to take appropriate action.(18)

The importance of law enforcement officials having access to accurate contact information for commercial website operators has also been recognized internationally. In 1999, the Organization

for Economic Cooperation and Development (OECD), an international organization consisting of 30 countries, issued consensus Guidelines on Consumer Protection in Electronic Commerce. These Guidelines recommend that "businesses engaged in electronic commerce with consumers 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."(19) Where this information is not provided on the registered websites, the Whois database can provide an important supplementary resource for law enforcers.

B. Registrar Responsiveness

The problem of inaccurate Whois information is compounded when registrars fail to act promptly to suspend domain names registered by registrants who have willfully provided inaccurate contact information. Under Registrar Accreditation Agreements between registrars and ICANN, registrars must collect contact information from registrants and post such information on a Whois service.(20) Suspension of a domain name for willful failure to provide accurate contact information is within the discretion of the registrar.(21) However, registrars have little incentive to suspend a domain name. Their failure to suspend a domain name can allow anonymous fraudsters to remain online and have their sites viewed by thousands of consumers in a short period of time.

Here is an anecdote illustrating how difficult it can be to suspend a domain name. At the most recent meeting of the OECD's Committee on Consumer Policy, which FTC Commissioner Mozelle Thompson now chairs, OECD staff presented a paper on its experience trying to contact a cybersquatter.(22) The OECD had let its registration for its French language site www.ocde.org lapse. A cybersquatter bought the domain name and used it to post a pornographic site with an offer to sell the domain name.(23) The Whois database indicated that the site had been registered by "Domain For Sale," located in Armenia, but the administrative and technical contact was an employee of the American Institute of Architects in Washington, D.C. The OECD called this individual and found that Domain For Sale had falsely listed him as a contact. The OECD demonstrated to the registrar that Domain For Sale had willfully provided false contact information. Rather than suspend Domain For Sale's registration, the registrar sent an e-mail to Domain For Sale, giving it fifteen days to correct its registration.

Domain For Sale modified its registration information, but the new information was on its face incomplete, as it did not list a person as a contact for the company, in violation of the Registrar Accreditation Agreement.(24) The registrar offered to de-register Domain For Sale only if OECD would indemnify the registrar for any breach of contract claim, the registrar's legal expenses in responding to OECD's complaint, and two years potential loss of registration business from Domain For Sale, which had 113 registrations with that particular registrar. The OECD refused and submitted affidavits from Armenian government officials stating that there was no legal entity registered at the address Domain For Sale had listed as its contact information. Only after some additional correspondence between the OECD and the registrar over a period of about one month was the registrar prepared to return the name to the OECD.

According to the OECD, the registrar failed to suspend the registration even after the OECD had twice shown that the registrant willfully submitted false contact information. Thus, OECD did not have access to www.ocde.org for almost two months.(25) By analogy, if a fraudulent website remains posted for a two-month period, it could cause consumers substantial injury.

IV. Current Registrar Practices with Respect to Whois Information

Current registrar practices with respect to accuracy of Whois information vary, depending on the type of registrar at issue. All registrars for generic Top Level Domains (gTLDs), including .com, .net, .org, .biz, .info and .name, are required to comply with ICANN's Registrar Accreditation

Agreement.(26) This Agreement contains provisions requiring registrars to collect accurate contact information from registrants and post such information on a Whois site. ICANN does not currently have any contractual provisions in place for most country code Top Level Domains (ccTLDs), such as .uk for the United Kingdom or .de for Germany. Registrar practices for these ccTLDs vary widely.(27) The following discusses each of these areas in turn.

A. Generic TLDs

ICANN's Registrar Accreditation Agreements with the gTLD registrars include some noteworthy provisions that illustrate ICANN recognition of the benefits of accurate Whois data. For example, the Agreement specifies that "a Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure promptly to update information provided to Registrar, or its failure to respond for more than fifteen calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration."(28) 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."(29)

The FTC Bureau of Consumer Protection letter to the ICANN DNSO Names Council dated August 6, 2001, mentioned earlier, had asked ICANN to work with registrars to implement and enforce the provisions of its Registrar Accreditation Agreement that ensure the completeness and accuracy of Whois data. There is some room for improvement in the Registrar Accreditation Agreements that could address our concerns.(30)

First, it would be extremely useful if registrars would weed out blank or incomplete registration forms, as well as some of the obviously false information that undermines the integrity of the Whois database. Second, it would very be useful to us if registrars could be required to suspend a domain registration upon wilful failure to provide accurate contact information, or failure to correct inaccurate contact information, until accurate information is obtained. The current ICANN Registrar Accreditation Agreements leave cancellation of a domain registration in these circumstances to the registrar's discretion.(31) This policy is problematic for two important reasons. As noted above, registrars have little incentive to suspend a domain name. Without a suspension requirement, scam artists are free to perpetrate fraud anonymously. In addition, registrars that adopt relaxed policies on accurate contact information may attract businesses seeking anonymity, creating havens for bad actors to shield their true identity from law enforcement and others. The OECD experience described above shows the consequences of lack of registrar cooperation: when registrars refuse to suspend domain registrations, websites operating for nefarious purposes can continue to operate on the Internet unchecked.

Although the Registrar Accreditation Agreements contain many important provisions for ensuring accuracy of domain registration information, these provisions have not solved the problem of inaccurate data described above. We believe it is worth examining whether registrars should have additional obligations to suspend registrations for failure to provide accurate information under Section 3.7.7.2 of the Registrar Accreditation Agreement and to implement reasonable up-front verification procedures for accuracy of contact information provided.(32)

B. Country-Code TLDs

Websites operating from the two-letter country-code top-level domains (ccTLDs) are likely to become increasingly important to our Internet fraud efforts. Websites operating from ccTLDs are viewable by U.S. consumers, and an increasing number of our actions involve foreign-based websites targeting U.S. consumers.

Registration of domain names within ccTLDs is administered by country-code registry managers. The rules and policies for registering domain names in the ccTLDs vary significantly, and the ccTLD registry managers do not have uniform rules on collection and publication of contact information for domain registrants.(33) Thus, the policies on disclosure of Whois information for domains registered with ccTLDs vary widely, and unavailability of such information can hinder our investigations. For example, the public Whois database for the .uk TLD (United Kingdom) only provides name of the registrar and no contact information for the domain registrant.(34) The .ie (Ireland) public Whois service only provides the name of the person who registered the website, but no contact information.(35) The .cn Whois service for China provides virtually no public information.(36)

ICANN's existing ccTLD Sponsorship Agreements with Australia and Japan state that ccTLD registry managers should obtain, maintain and provide public access to accurate and up-to-date contact information for domain name registrants consistent with ICANN policies.(37) Neither of these agreements prescribes detailed rules for what information should be collected and what information should be published. The Australian ccTLD registry manager seems to provide contact information, including name, address, telephone number, fax number and e-mail address, for the registrant, whereas the Japanese ccTLD registry manager seems to only provide the name of the registrant.(38) ICANN's model ccTLD Sponsorship Agreement and ICANN's Governmental Advisory Committee Principles for Delegation and Administration of ccTLDs Presented contain the same provision as the .jp (Japan) and .au (Australia) ccTLD sponsorship agreements on public access to contact information of registrants.(39)

It would be extremely useful for our law enforcement purposes for the ccTLD registry managers to implement measures to improve accuracy and accessibility of Whois data for ccTLD registrants. For the reasons that we have outlined, we will continue to work with businesses, consumer groups, governments, international organizations and other stakeholders to advocate internationally the importance of collecting accurate contact details for ccTLD registrants to assist law enforcers in their efforts to protect consumers from Internet fraud.(40)

V. Privacy Issues

Finally, there are tradeoffs between transparency of domain registrant information and personal privacy. The FTC has a unique perspective on these issues, given that we are a law enforcement agency that has committed substantial resources to protecting consumers' privacy.(41) There are legitimate privacy interests at stake for websites, especially those developed for personal or political purposes. At the same time, there are often legitimate reasons for making such information available to law enforcers and/or the public.

For commercial websites, we believe the balance weighs in favor of public disclosure of basic registrant contact information. Once a company decides to sell products on the Internet, it should be accountable to the public so that the public can determine who the company is and where it operates from. The OECD Guidelines on Electronic Commerce cited above affirm these principles. The Guidelines 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.(42) This provision represents a consensus among the 30 member countries of the OECD as to the minimum information that consumers should be able to obtain about businesses operating websites. Because some online businesses do not provide sufficient identifying information on their websites, Whois information can provide consumers with a useful supplement.

With respect to websites registered by individuals, such as websites registered under the .name Top Level Domain,(43) or websites registered for non-commercial purposes, there are different considerations to balance. On one hand, these individuals and website operators have legitimate privacy concerns. On the other hand, a fraudster should not be permitted to hide from law

enforcement authorities simply by registering under the .name TLD or by claiming registration for non-commercial purposes. It is also important in this context to consider both the question of what disclosure to the public is warranted and the question of what disclosure to law enforcement is warranted. We are continuing to work through international organizations, businesses and consumer groups to develop workable solutions that balance the privacy interests with the interests in transparency of Whois data.(44)

VI. Conclusion

In short, our Internet fraud enforcement efforts require quick identification of problems, quick identification of perpetrators, and the ability to gather information about international entities and organizations. Accurate Whois data is essential to these efforts, and inaccurate data can significantly frustrate them. We look forward to continuing to work with this Subcommittee and all international stakeholders toward improving accuracy of Whois information.

Mr. Chairman, the FTC greatly appreciates this opportunity to testify. I would be happy to answer any questions that you and other Members may have.

Endnotes:

1. This written statement presents the views of the Federal Trade Commission. My oral statement and responses to questions are my own and are not necessarily those of the Commission or any individual Commissioner.

2. The FTC's Bureau of Consumer Protection staff also filed a public comment with the ICANN DNSO Names Council on the importance of accurate Whois data for law enforcement purposes. See Letter of Howard Beales to Louis Touton dated August 6, 2001, re ICANN DNSO Names Council Whois Survey.

3. 15 U.S.C. § 41 et seq. The Commission has responsibilities under 40 additional statutes, including the Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 et seq., which prohibits unfair and deceptive acts and practices in connection with the collection and use of personally identifiable information from and about children on the Internet. See www.ftc.gov/ogc/coppa1.pdf. The Commission also enforces over 30 rules governing specific industries and practices, including the Mail and Telephone Order Merchandise Rule, 16 C.F.R. Part 435, which covers purchases made over the Internet and spells out the ground rules for making promises about shipments, notifying consumers about unexpected delays, and refunding consumers' money. See www.access.gpo.gov/nara/cfr/waisidx_99/16cfr435_99.html.

4. 15 U.S.C. §§ 45(a) and 53(b).

5. See Leslie Miller, *"Web Growth Slows, But Online Time Rises,"* USA Today, March 28, 2002, available at www.usatoday.com/life/cyber/tech/2002/03/28/net-statistics.htm.

6. See U.S. Census Bureau, "Retail E-Commerce Sales in Fourth Quarter 2001 Were $10.0 Billion, Up 13.1 Percent from Fourth Quarter 2000," www.census.gov/mrts/www/current.html.

7. This number represents an exponential growth in the number and percentage of Internet fraud-related complaints received in 1997, when the Commission received fewer than 1,000 Internet fraud complaints. See Prepared Statement of the Federal Trade Commission on 'Internet Fraud,' Before the House Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection, 107th Cong., 1st Sess. (May 23, 2001), available at http://www.ftc.gov/os/2001/05/internetfraudttmy.htm For additional statistics from the Consumer Sentinel database, see www.consumer.gov/sentinel.

8. *See* www.consumer.gov/sentinel.

9. *See* www.consumer.gov/sentinel/trends.htm.

10. For more information about the IMSN, see www.imsnricc.org.

11. *See* www.econsumer.gov.

12. *See* Agreement Between the Government of the United States of America and the Government of Canada Regarding the Application of their Competition and Deceptive Marketing Practices Laws, Trade Reg. Rep. (CCH) ¶ 13,503 (1995); Agreement Between the Federal Trade Commission of the United States of America and the Australian Competition & Consumer Commission

On the Mutual Enforcement Assistance in Consumer Protection Matters (July 20, 1999), www.ftc.gov/opa/2000/07/usaccc.htm; Memorandum Of Understanding On Mutual Enforcement Assistance In Consumer Protection Matters Between The Federal Trade Commission Of The United States of America And Her Majesty's Secretary of State for Trade And Industry And The Director General Of Fair Trading In The United Kingdom (October 31, 2000), www.ftc.gov/opa/2000/10/ukimsn.htm.

13. Information on "Operation Top Ten Dot Cons" (October 21, 2000) is available at www.ftc.gov/opa/2000/10/topten.htm; information on the International Netforce project (April 2, 2002) is available at www.ftc.gov/opa/2002/04/spam.htm.

14. Cited in Thomas Fuller, "OECD's Cautionary Tale of Porn and Cyberspace," International Herald Tribune at 1 (April 3, 2002), available at www.iht.com/articles/53353.html.

15. 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.

16. Civ. No. 99-000-44ABC (AJWx) (C.D. Cal.).

17. Many of these initiatives were generated by the FTC's database of unsolicited commercial e-mail (UCE or spam). Consumers currently send unwanted spam to the agency at a rate of approximately 35,000 e-mails a day using the agency's database address, uce@ftc.gov. The FTC has collected more than 10 million unwanted spam messages since 1998.

18. *See* http://www.ftc.gov/opa/2002/04/spam.htm.

19. Guidelines on Consumer Protection in the Context of Electronic Commerce, Part Two, Section III(A), OECD (December 9, 1999) available at www.ftc.gov/opa/1999/9912/oecdguide.htm.

20. ICANN Registrar Accreditation Agreement, May 17 2001, § 3.3.1, www.icann.org/registrars/ra-agreement-17may01.htm.

21. Id. at § 3.7.7.2.

22. Cybersquatting means registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else. It refers to the practice of buying up domain names reflecting the names of existing businesses, intending to sell the names for a profit back to the businesses when they go to put up their websites. See http://www.nolo.com/lawcenter/ency/article.cfm/objectID/60EC3491-B4B5-4A98-BB6E6632A2FA0CB2. For an FTC case involving cybersquatting, see *FTC v. Zuccarini*, C.A. No. 01-CV-4854 (E.D. Pa., filed Sept. 25, 2001), available at http://www.ftc.gov/opa/2001/10/cupcake.htm.

23. *See* Cybersquatting - The OECD's Own Experience and the Problems It Illustrates with Registrar Practices and the 'Whois' System, OECD Directorate for Science, Technology and Industry, Committee on Information, Computer and Communications Policy, DSTI/ICCP(2002)8 (2002), available at www.oecd.org/pdf/M00027000/M00027316.pdf.

24. *See supra* note 20 at § 3.7.7.1.

25. *See supra* note 14.

26. *See supra* note 20.

27. Two letter domains, such as .uk, .de and .jp (for example), are called country code top level domains (ccTLDs) and correspond to a country, territory, or other geographic location. The rules and policies for registering domain names in the ccTLDs vary significantly and some are reserved for use by citizens of the corresponding country. See ICANN Frequently Asked Questions, available at www.icann.org/general/faq1.htm.

28. *See supra* note 20 at § 3.7.7.2.

29. *See supra* note 20 at § 3.7.8.

30. Of course, as noted above, exactly what might be done will depend on whether and to what extent the structure of ICANN is changed as a result of the reform process.

31. See supra note 20 at § 3.7.7.2 (stating that a registrant's wilful failure to provide accurate contact details shall "be a basis for cancellation of the Registered Name registration.")

32. The Commission recognizes that the proposed measures are not a cure-all. They would not, for example, limit in any way the

ability of a registrant who has had a domain name terminated to register new domain names.

33. See www.icann.org/cctlds for more information about ccTLDs.

34. *See* www.nic.uk.

35. *See* www.domainregistry.ie.

36. *See* www.cnnic.net.cn. U.S. law enforcement efforts against websites with country-code TLDs is made more difficult by the fact that it is extremely difficult, and in some cases, virtually impossible to enforce a subpoena against a foreign registrar requesting additional information about a registrant.

37. *See* .jp ccTLD Sponsorship Agreement (April 1, 2002), at § 4.5.1, www.icann.org/cctlds/jp; *see* .au ccTLD Sponsorship Agreement (October 25, 2001), at § 4.5.1, www.icann.org/cctlds/au/sponsorship-agmt-25oct01.htm

38. *See* http://www.aunic.net; *see* http://jprs.jp/eng.

39. *See* Model ccTLD Sponsorship Agreement--Triangular Situation, Posted September 2, 2000, at 4.5.1, available at www.icann.org/cctlds/model-tscsa-02sep01.htm., Principles for Delegation and Administration of ccTLDs Presented by Governmental Advisory Committee (23 February 2000), www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm.

40. Although these comments here focus largely on data accuracy and integrity, there are also a number of related issues, such as the scope of information collected and the searchability of that information. For a further discussion of these issues, *see* FTC Bureau of Consumer Protection letter to Louis Touton, *supra* note 2. We plan to examine these issues as well with the relevant international stakeholders.

41. Our initiatives in this area include beefing up enforcement against deceptive spam, helping victims of identity theft, enforcing privacy promises, increasing enforcement and outreach on children's online privacy, and encouraging consumers to report privacy complaints. *See* www.ftc.gov/privacy/index.html.

42. Guidelines for Consumer Protection in the Context of Electronic Commerce, OECD, December 9, 1999, Part Two, § 3(a), available at www.ftc.gov/opa/1999/9912/oecdguide.htm.

43. The .name TLD is reserved for registrations by individuals.

44. We acknowledge that requiring all registrars to police whether a site is being registered for commercial or non-commercial purposes may impose undue costs on registrars. We will take into account this concern in our further consideration of these issues.