ORAL STATEMENT OF COMMISSIONER JON LEIBOWITZ
on
"Internet Governance: The Future of ICANN"
(September 20, 2006, 10:00 a.m.)

Thank you, Mr. Chairman, Senator Dorgan and Members of the Subcommittee. I am pleased to be here on behalf of the Federal Trade Commission. I ask that the Commission's written statement be made part of the record. My oral testimony reflects my own views and not necessarily the views of the Commission.

This morning, I want to focus my remarks on the importance of continued unrestricted access to Whois information. Simply put, our ability to protect consumers is being placed ***at risk*** by a movement within ICANN to limit Whois to "technical purposes" only – and thus prevent law enforcement and the public from using this critical resource to identify scammers who operate websites.

Those who want to restrict access to Whois databases are no doubt sincere in their efforts to protect privacy. But the irony is that any attempt to cabin Whois information so narrowly could actually jeopardize the ability of the FTC and other law enforcement authorities to protect people's privacy – for example, by stopping spam, spyware, and identity theft – an outcome nobody wants.

Because this is such an important issue, in June the Commission sent a delegation to the ICANN meeting in Morocco, where we joined with several of our foreign consumer protection counterparts to emphasize to ICANN the importance of access to Whois. We understand that in the wake of that meeting, the ICANN advisory body is reevaluating its earlier decision.

Mr. Chairman, we certainly hope so. Because the "future of ICANN" is really on the line here – it has to show the leadership necessary to properly govern the Internet.

Having said that, I have met with the ICANN Board, they understand the seriousness of the Whois issue, and my strong sense is that they're committed to doing the right thing.

From our perspective, access to Whois databases raises four important considerations:

1. law enforcement's ability to obtain information about malefactors who use Internet web sites;
2. consumers' ability to know who they are dealing with when they engage in e-commerce;
3. businesses' ability to serve important functions; and
4. individual privacy interests.

First, law enforcement. The FTC frequently challenges a wide variety of Internet-related threats, for example, spam, spyware, phishing, deceptive health claims, and get-rich-quick schemes. Whether acting to stop fraud or otherwise protecting consumers, our investigators need to identify offenders who hide behind the electronic shield of the Internet.

For the past decade, we have used Whois databases in virtually ***all*** of our Internet investigations. In fact, Whois is often one of the ***first tools*** we use to identify wrongdoers.

Sometimes, we can unmask the bad guys and learn their whereabouts from Whois databases. And even when scammers provide false information, Whois data may still provide invaluable leads. Con artists often provide the same phony information for multiple websites, so Whois sometimes enables us to link seemingly unrelated scams.

Second, ***consumers*** themselves need to know who they're doing business with. This is especially true in the online environment. Continued public access to Whois data provides consumers with essential contact information if an online seller fails to deliver goods or services as promised. Consumer self-help is vital to ensuring consumer confidence in our market economy – and, often, to resolve disputes before they reach law enforcement.

Third, ***business*** access to Whois data also serves an important public policy purpose. Last week, I was on the West Coast meeting with some of our leading Internet companies. These companies frequently rely upon Whois databases to take real-time action against phishers and identity thieves who are using their brands to target their customers. Impeding businesses' ability to quickly take down scams will only further the risk of serious consumer harm.

Of course, the FTC is concerned about legitimate ***privacy interests***. We have always recognized that individual non-commercial registrants may require protection from ***public*** access to their contact information without compromising appropriate access by law enforcement. (Think, for example, of the dissident who needs anonymity.) But from our perspective, anyone selling a product or engaged in commercial activity should have to publicly reveal who they are.

Before I conclude, let me raise one related issue. There is another critically important tool that we need to fight online fraud in the global marketplace – the US SAFE WEB Act – which would allow us to more effectively work with foreign law enforcement agencies to protect American consumers. We all know that time is running short this Congress and that the House has yet to act on your [non-controversial] bill. But Mr. Chairman, we do want to thank you for your continued leadership. All of us at the Commission stand ready to help you with any final legislative push.

With that, I think I've "pushed" my time limit. Thank you, and I'm happy to answer any questions.