Statement of Commissioner Orson Swindle
Federal Trade Commission

Before the

Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
United States House of Representatives

June 11, 2003

Thank you, Mr. Chairman and members of the Subcommittee, for this opportunity to appear before you with Chairman Muris and my fellow Commissioners.

Today, I would like to briefly address a growing and very threatening problem for all of us - unwanted e-mail, or spam.

Consumers must have trust and confidence in technology and its uses, particularly when it comes to the privacy and security of their personal and sensitive information. Because spam undermines consumer trust and confidence, it represents a significant and rapidly growing threat to web-based services.

The Commission's testimony provides the Subcommittee with an overview of our efforts to combat spam and also legislative recommendations to address spam. The legislative recommendations are modeled on the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. §§ 6101-6108; however, many of the Commission's recommendations are already contained in the Burr spam bill. For example, the Burr bill addresses specific practices that would likely be classified as deceptive or abusive in a Commission rulemaking. In addition, like the Telemarketing Act, the Burr bill provides for state law enforcement action in federal court, allows for the collection of civil penalties, and grants the Commission narrow rulemaking authority to implement key provisions of the bill.

Spam raises a number of concerns. The volume of spam is increasing at astonishing rates. Current estimates indicate it constitutes at least 40% of all e-mail. In addition, recent Commission studies indicate that spam has become the weapon of choice for those engaged in fraud and deception. Nearly 66% of the spam messages that Commission staff examined appeared to contain obvious indicia of falsity in their "From" lines, "Subject" lines, or message text. In addition, because spam can transmit viruses, "Trojan horses," and other damaging code, it threatens to cause major damage to the Internet and our critical infrastructure. All of these concerns represent enormous costs to consumers, businesses, and the economy.

There is no easy solution to the spam problem. Certainly, no single approach will solve the problem. Nevertheless, spam raises problems that demand attention by policy makers and industry leaders. First, there is a complex combination of technology, market forces, and public policy that will be evolving for years to come. In addition, the spam problem is heavily influenced by the emotions of millions of computer users who are literally fed up with spam.

Spam is about to kill the "killer app" of the Internet - specifically, consumer use of e-mail and e-commerce. If consumers lose trust and confidence in web-based services and stop using them as tools for communication and online commerce, it will cause tremendous harm to the economic potential of information technology.

Solving these problems requires innovation, resources, and time. However, dealing with the emotional reaction to spam by millions of users requires our immediate attention before it gets out of hand.

Internet service providers, software manufacturers, and those engaged in designing operating systems must empower consumers with better control over their incoming e-mail. Easing the spam burden on consumers would help to "shore up" trust and confidence. Surely this is possible right now.

Why hasn't industry done this? Frankly, I am not convinced that industry really wants to empower consumers by giving them easy-to-use tools to control their incoming e-mail.

Spam is a crisis today. I think solving tough and threatening problems by coming together to fight the battle is the American way. We need great minds to quickly find solutions to spam. Empowering consumers would be a good first step. Industry must do this now.

The Commission will continue its multi-faceted efforts to address spam. For example, the Commission will continue its aggressive law enforcement program against deceptive spam. However, it is both resource intensive and technically challenging to find the "guilty parties."

Consumer education and awareness are also essential. The Commission disseminates educational materials to help inform consumers about the steps they can take to decrease the amount of spam they receive. In addition, the Commission's consumer security website, <www.ftc.gov/infosecurity>, contains practical tips for staying secure online. The Commission's private sector partnerships help disseminate these educational materials so that the largest number of individuals and groups obtain this information.

The Commission also conducts research on various aspects of spam. Three recent Commission studies help us to better understand the magnitude of deceptive spam, the online activities that place consumers at risk for receiving spam, and the validity of "remove me" or "unsubscribe" links found in e-mail messages.

The Commission's Spam Forum in May was intended to better inform the dialogue and to explore possible solutions to spam. The Forum provided an incredible amount of valuable information. The participation at the Forum was also remarkable: over 80 panelists participated in the discussions and over 400 people attended the conference. I would like to share some of the Forum's revelations about the realities of spam.

First and foremost, the private sector must lead the way to finding solutions to spam. We likely will not find the perfect solution. The target will be constantly moving as technology evolves.

Second, more laws are not necessarily the right answer. Laws bestowing a competitive advantage to larger firms over smaller firms are questionable. Unenforceable laws will have little real effect. Overreaching laws will have unintended adverse consequences. Passing legislation to mandate best practices for "good actors" will not help us track down the "bad actors" engaged in fraud and deception.

Third, industry, government, consumers, other end-users, and civil society organizations must be a part of a continuing dialogue to find solutions.

Finally, because of the threats that spam containing malicious code can cause, it is essential to develop consumer awareness about engaging in safe computing practices. It is imperative to develop a "culture of security" where all participants work to enhance consumer security and minimize the vulnerabilities to the Internet and our critical infrastructure.

The effort to solve the spam problem and secure our information systems and networks is a journey, not a destination. And we have miles to go before we sleep.

Thank you, Mr. Chairman.