Protecting Consumers in a High-Tech World
Internet Foundation Lunch
Brussels, April 6, 2005
Remarks by Chairman Majoras

I. Introduction

Thank you. I am delighted to be with you in Brussels today and to introduce you to some of the important work of the U.S. Federal Trade Commission. The FTC is the only federal agency in the United States empowered to promote competition and consumer welfare by enforcing both antitrust and consumer protection laws. The scope of FTC authority is broad, but I would like to focus my remarks this afternoon specifically on some of the FTC's activities to protect consumers in the global electronic marketplace.

To protect consumers, we use a multi-pronged strategy that incorporates aggressive law enforcement, consumer and business education, and research and advocacy. The principal consumer protection statute enforced by the FTC is the FTC Act, which prohibits "unfair or deceptive practices." The statute empowers the FTC to file civil actions in U.S. federal district court seeking injunctive relief against businesses engaged in fraudulent, deceptive, or misleading practices. The FTC also can seek monetary redress for consumers injured by such practices.

Of particular relevance to today's discussion, the prohibition on "unfair or deceptive practices" is not limited to any specific medium. In the past, we have used this language to take action against door-to-door salespeople selling their bogus wares to unsuspecting consumers. Today, we use the same statutory language to take action against high-tech frauds with interesting names like spamming, cramming, and modem hijacking, that cross geographical boundaries.

Protecting consumers from such high-tech frauds is important, not only to redress consumer injury and deter wrongful conduct, but to build consumer confidence in new technologies. These technologies have created enormous benefits for consumers in the form of increased convenience, choice, and efficiency. They also have led to globalization of the marketplace, which further increases consumer choice, improves competition, and lowers prices.

But in some cases, the tremendous benefits of new technology also have created risks for consumers. In the FTC's experience, fraudulent operators are always among the first to appreciate the potential of technologies and then to use that potential to exploit and deceive consumers. Using these technologies, fraud operators can strike quickly on a global scale, victimize thousands of consumers in a short time, and disappear nearly without a trace – along with their ill-gotten gains.

Indeed, as we would expect, an increasing number of complaints we receive involve international transactions. Thus, I have made it plain that strengthening our international relationships and cooperating to achieve more effective consumer protection in the electronic marketplace are essential. I came to the FTC as an antitrust lawyer, and, having worked on a global basis with competition enforcers, I know that no such relationship is more critical than that with the European Union.

With this background, I would like to describe how we are approaching the challenges posed in three related areas – spam, spyware, and information security – and highlight international initiatives in each of these areas.

II. Spam

Spam is one of the most intractable consumer protection problems that the FTC – like you and computer users – has ever faced. The extremely low cost of sending email makes it an appealing marketing channel even for legitimate companies. Unfortunately, low cost combines with anonymity, making spam an ideal vehicle for con artists as well. Indeed, a 2003 FTC staff survey revealed that two-thirds of spam in our sample contained facial indications of falsity.

We are devoting significant resources to aggressive law enforcement against spammers. Since 1997, the Commission has been ferreting out fraudulent offers sent via spam, and more recently, spam messages that violate the new federal anti-spam legislation, the CAN-SPAM Act. To date, we have filed 68 spam-related cases against 198 individuals and companies. The number of consumers who received spam from these malefactors is mind-boggling. We continue to receive 300,000 new spam messages per day in our spam database (known as the "refrigerator"), and, together with our law enforcement partners, we will use this information to go after more spammers. The biggest problem we face, however, is tracing the spammers.

We cannot solve the spam problem with new laws and law enforcement alone. First, we must educate consumers and businesses, not just in the United States, but around the world, about how to protect themselves and others from unwanted spam. The campaign against "phishing" is a prime example of a problem that is best addressed by consumer education. "Phishing" occurs when criminals send an email or pop-up message that claims to be from a business, such as a bank or online payment service, and that says the business needs consumers to "update" or "validate" account information. The message directs consumers to a Web site that looks just like a legitimate site, but it is not. Instead, the purpose of the bogus site is to trick consumers into divulging their personal information. Identifying individual "phishers" is

extremely difficult; but if consumers know not to provide financial information through email in response to a pop-up solicitation or email inquiry, they themselves can effectively stop this criminal activity.

Second, this is also a technological problem, and it requires a technological solution. The FTC, of course, cannot develop the technological solutions to mitigate the problem. But we are working to encourage and facilitate private market innovations. Last November, the Commission convened an Email Authentication Summit, cosponsored by the National Institute of Standards at the U.S. Department of Commerce. The Summit enabled the Commission to gather a wide spectrum of interested parties, capable of finding a solution to the problem of email anonymity, with the goal of invigorating the search for – and agreement on – an authentication standard.

Third, spam is inherently a global issue. The path from a fraudulent spammer to a consumer's in-box typically crosses at least one international boundary, and usually several. Most of our enforcement actions involving spam have had an international component, and we have cooperated with foreign enforcement agencies on many of them. In the last six months alone, we have worked with authorities in the United Kingdom, Netherlands, and Cyprus on spam investigations.

In addition to cooperating with foreign partners on individual cases, the FTC has participated in various multilateral and bilateral initiatives on spam. FTC staff is actively involved in the OECD Spam Task Force, and we follow very closely the activities of the European Cooperation Network of Spam Authorities (CNSA), led by DG Information Society. We have signed Memoranda of Understanding on spam enforcement cooperation with agencies

in the U.K., Australia, and Spain. The FTC is also active in the recent London Action Plan initiative, an informal network of spam enforcers and industry representatives from 20 countries that allows participants to discuss cases, investigation techniques, and educational initiatives. Already, agencies and organizations from 13 European countries participate in the London Action Plan, and participation remains open to spam enforcement agencies and relevant private sector representatives from around the world. Commitments to cooperate, however, will not be enough; we must productively implement cooperative steps to stop spammers.

III. Spyware

Just when we were getting a good start on addressing spam, spyware popped up. The term spyware may be amorphous, but there is no doubt that its negative impact is real. It is hard to find any computer user who has not struggled for hours to remove spyware from his computer.

We recently issued a staff report on a public workshop on spyware we held last year. The workshop explored what spyware is, how it is distributed, and how much harm it causes. We used the information from the workshop to start developing cases, and equally important, to start the discussion of what technology is or may be available to protect consumers. Here, we believe a critical role for government is to encourage technological solutions to help reduce spyware problems.

We have also brought enforcement actions against illegal spyware. We filed our first spyware case in October 2004. In that case, we alleged that the defendants violated the FTC Act by loading spyware onto consumers' computers that changed their web browsers and barraged them with pop-up advertisements, in addition to installing other software programs without the consumers' knowledge or consent. Then, after creating computer crashes and other

malfunctions, the defendants launched pop-up ads that offered to sell an anti-spyware solution for $30. Fortunately, the court granted us a preliminary injunction, which stopped the business from distributing spyware. And, last month, we filed our second case, this one against purveyors of alleged worthless spyware protection software.

Like spam, the problem of spyware highlights the truly global dimension of consumer protection. Purveyors of spam and spyware can operate from anywhere in the world and easily, cheaply, and anonymously target anyone in the world. One tool we need now to combat spam and spyware is improved authority to combat cross-border fraud generally. We have recommended legislation that, if enacted, will facilitate information sharing with foreign agencies and allow the FTC to provide more investigative assistance to foreign counterparts who bring fraud cases. While the legislation is phrased in terms of combating cross-border fraud, we believe it could be invaluable in giving us tools to fight spam and spyware that cross international boundaries.

I know that the European Union has recently enacted similar legislation in the form of a regulation on consumer protection enforcement cooperation. In addition to improving cooperation among consumer protection authorities in Member States, the regulation contemplates increased cooperation with non-European Union countries on consumer protection enforcement issues. We have been in discussions with DG Sanco on how best to maximize cooperation under our respective initiatives.

IV. Information Security

The explosive growth of the Internet and the development of sophisticated computer systems and databases has made it easier than ever for companies to gather and use information about their customers, employees, and business associates. Recent news reports about the release of consumers' sensitive information from one of the United States' largest commercial information services and a major U.S. bank demonstrate that, if this data is not adequately secured, it can fall into the wrong hands and cause serious harm to consumers. The consequences of security breaches are often severe, ranging from identity theft and unauthorized charges to consumers' accounts, to an increase in spam and "phishing" schemes.

Our primary goal is to encourage all companies to put in place solid information security practices *before* a breach can occur. But where significant breaches do occur, we will continue to determine whether they were caused by the failure to take reasonable steps to safeguard consumers' information. If so, we will take appropriate action. Given the importance of information security to consumers, the FTC has made it one its top law enforcement priorities, and we will be dedicating even more resources to this critical issue.

To date, we have filed five cases challenging false security claims under the FTC Act. In each case, we alleged that the defendants promised that they would take reasonable steps to protect consumers' sensitive information, but failed to do so. For example, last month, the FTC alleged that Petco Animal Supplies promised to keep its customers' information secure, but failed to take reasonable measures to prevent commonly known attacks to its Web site by hackers. The flaws in Petco's Web site allowed a hacker to access consumer records, including credit card numbers. As with the Commission's prior information security cases, the settlement requires that Petco implement a comprehensive information security program for its Web site.

The FTC also has a central role in educating consumers and businesses about the risks of identity theft and assisting victims and law enforcement officials. The FTC maintains a Web site and a toll-free hotline staffed with trained counselors to advise victims on how to reclaim their identities. We receive roughly 15 to 20 thousand contacts per week on the hotline, or through our Web site or mail from victims and from consumers who want to avoid becoming victims. The FTC also facilitates cooperation, information sharing, and training among federal, state, and local law enforcement authorities fighting this crime.

Because information security is increasingly a global issue, the FTC remains active in international policy issues relating to information security and privacy. One of my fellow Commissioners, Commissioner Orson Swindle, led the U.S. delegation to the OECD Committee that drafted the 2002 OECD Security Guidelines that aimed to create a global culture of security, in which consumers, industry, and governments each play an important role. In addition, we work closely with the European Commission on privacy and security issues, including the Safe Harbor framework. Although American and European approaches to these issues may differ, we do share the common goal of protecting consumers' personal information from security breaches. **V. Conclusion**

I want to conclude by emphasizing that each of the issues I have discussed today has an international component, as does consumer protection in electronic commerce generally. I hope today's luncheon can start a productive ongoing dialogue on how we can work together to protect consumers on both sides of the Atlantic. Thank you again for the opportunity to speak to you today.