U.S. House of Representatives
Committee on the Judiciary

Testimony of Representative Bob Goodlatte
Subcommittee on Crime, Terrorism and Homeland Security
Hearing on H.R. 1525, the Internet Spyware (I-SPY) Prevention Act
May 1, 2007

Chairman Scott, Ranking Member Forbes, and members of the Subcommittee, thank you for inviting me to testify at this important hearing.

I was pleased to join with my colleague from California, Representative Zoe Lofgren, to reintroduce H.R. 1525, the "Internet Spyware (I-SPY) Prevention Act." This bi-partisan legislation will impose tough criminal penalties on those that use software for nefarious purposes, without imposing a broad regulatory regime on legitimate online businesses. I believe that this targeted approach is the best way to combat spyware.

The continued growth of the Internet has brought tremendous enhancements to our quality of life – from advances in the delivery of health care, to the ability of consumers to seamlessly and instantaneously conduct transactions online. Increasingly, consumers want a fast connection to the Internet and want the delivery of online services to be seamless, and online service providers have invested significant resources to develop software to make their services as safe, reliable and fast as possible.

However, the Internet will never reach its full potential until consumers feel safe to conduct transactions online. One enormous hurdle to consumer confidence in the Internet is the purveyance of spyware. Unfortunately, similar types of software to what legitimate businesses use to deliver new and innovative services can also be used by bad actors to break into computers, steal personal information and commit identity theft and other crimes.

Spyware is software that provides a tool for criminals to secretly crack into computers to conduct nefarious activities, such as altering a user's security settings, collecting personal information to steal a user's identity, or to commit other crimes. A recent study done by the National CyberSecurity Alliance revealed that over 90% of consumers had some form of spyware on their computers and most consumers were not aware of it. With the interstate nature of the Internet, Congress clearly has a role to play in punishing those that use software to commit online crimes and thus prevent the continuing erosion of consumer confidence in the Internet.

However, as Congress considers legislation in this area I believe that four overarching principles should guide the development of any spyware legislation. First, we must punish the bad actors, while protecting legitimate online companies. Second, we must not over-regulate, but rather encourage innovative new services and the growth of the Internet. Third, we must not stifle the free market. Fourth, we must target the behavior, not the technology.

The I-SPY Prevention Act would impose criminal penalties on the most egregious behaviors associated with spyware. Specifically, this legislation would impose up to a five-year prison sentence on anyone who uses software to intentionally break into a computer and uses that software in furtherance of another federal crime. In addition, it would impose up to a two year prison sentence on anyone who uses spyware to intentionally break into a computer and either alter the computer's security settings or obtain personal information with the intent to defraud or injure a person or with the intent to damage a computer. By imposing stiff penalties on these bad actors, this legislation will help deter the use of spyware, and will thus help protect consumers from these aggressive attacks.

Enforcement is also crucial in combating spyware. The I-SPY Prevention Act authorizes $10 million for fiscal years 2008 through 2011, to be devoted to prosecutions involving spyware, phishing and pharming scams, and expresses the sense of Congress that the Department of Justice should vigorously enforce the laws against these crimes. Phishing scams occur when criminals send fake e-mail messages to consumers on behalf of famous companies and request account information that is later used to conduct criminal activities. Pharming scams occur when hackers re-direct Internet traffic to fake sites in order to steal personal information such as credit card numbers, passwords and account information. This form of online fraud is particularly egregious because it is not as easily discernable by consumers. With pharming scams, innocent Internet users simply type the domain name into their Web browsers, and the signal is re-routed to the devious Web site.

The I-SPY Prevention Act is a targeted approach that protects consumers by imposing stiff penalties on the truly bad actors, while protecting the ability of legitimate companies to develop new and exciting products and services online for consumers.

The I-SPY Prevention Act also avoids excessive regulation and its repercussions, including the increased likelihood that an overly regulatory approach focusing on technology would have unintended consequences that could discourage both consumer use of the Internet as well as the creation of new and exciting

technologies and services on the Internet. By encouraging innovation, the I-SPY Prevention Act will help ensure that consumers have access to cutting-edge products and services at lower prices.

In addition, the approach of the I-SPY Prevention Act does not interfere with the free market principle that a business should be free to react to consumer demand by providing consumers with easy access to the Internet's wealth of information and convenience. Increasingly, consumers want a seamless interaction with the Internet, and we must be careful to not interfere with businesses' abilities to respond to this consumer demand with innovative services. The I-SPY Prevention Act will help ensure that consumers, not the federal government, define what their interaction with the Internet looks like.

Finally, by going after the criminal behavior associated with the use of spyware, the I-SPY Prevention Act recognizes that not all software is spyware and that the crime does not lie in the technology itself, but rather in actually using the technology for nefarious purposes. People commit crimes, not software.

Thank you again for the opportunity to testify before the Subcommittee. I look forward to answering any questions you may have.