U.S. House of Representatives
Committee on the Judiciary

Testimony of
Representative Zoe Lofgren of California
Before the Subcommittee on Crime, Terrorism, Crime, and Homeland Security
Hearing on
H.R. 1525, the "Internet Spyware (I-SPY) Prevention Act of 2007"
Tuesday, May 1st, 2007

Chairman Scott, Ranking Member Forbes, and distinguished members of the subcommittee, thank you for inviting me to speak before you today on the growing threat to Internet users and Internet commerce posed by spyware and phishing scams, and on the way that the Internet Spyware (I-SPY) Prevention Act of 2007 will counter that threat.

Spyware is a serious and growing problem for American consumers and businesses. Thieves are using spyware to harvest personal information such as Social Security numbers and credit card numbers for use in a variety of criminal enterprises. Although the definition of spyware is a moving target, the FTC loosely defines the term as software that "aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge." The Anti-Spyware Coalition offers a slightly different definition of spyware as "technologies deployed without the appropriate user consent and/or implemented in ways that impair user control," including:

- Material changes that affect user experience, privacy, or system security;
- Use of system resources, including what programs are installed on computers; and/or
- Collection, use, and distribution of personal or other sensitive information.

Two of the most serious forms of spyware are "keystroke loggers" that capture every key typed on a particular computer, allowing cyber-criminals to gain access to credit card accounts and other personal information, and programs that hijack users' system settings.

Nine out of every ten Internet users have modified their online behavior out of fear of falling victim to spyware. Indeed, consumers spent $2.6 billion last year trying to block or remove spyware from their computers. But consumers are seldom successful at completely eliminating spyware from their systems. Recent studies estimate that 80 percent of computers are infected with some form of spyware and 89 percent of consumers are unaware of that fact. 93 million American adults experienced a spyware-related problem in 2004. As broadband reaches American communities that have less experience with the online world, the number of victims of spyware will almost certainly increase.

Spyware is as much a problem for technology companies and other businesses as it is for individuals. Microsoft analysts have reported that spyware is at least partially responsible for about one-half of all the application crashes that are reported to them. Spyware is also threat to the Internet as a whole. Just this February, a massive denial-of-service attack targeted DNS root servers, including one maintained by the Department of Defense. Although the source of the ultimately unsuccessful attack was unclear, hijacked computers are often turned into "zombies" that participate in denial-of-service attacks without the knowledge of their users.

As the Judiciary committee has noted in the past, there is no "silver bullet" for ending spyware. Instead, we must rely on a multi-pronged approach that involves greater consumer awareness, the use of available technological countermeasures, and an effective criminal enforcement strategy. The legislation you are considering today is a crucial component of this last prong. That is why I was pleased to work once again with Representative Goodlatte to introduce the I-SPY Prevention Act.

The Act imposes significant criminal penalties for the most serious and prevalent criminal activities that employ spyware. For example, the Act would impose a prison sentence of up to 5 years for use of spyware in furtherance of another Federal crime. The Act also imposes up to a 2-year sentence for hacking into a computer and altering its security settings or obtaining personal information with the intent to defraud or injure the person or damage a computer.

The Act also assists the Department of Justice in enforcing these new provisions. The legislation authorizes $10 million in funding for fiscal years 2008 through 2011 for prosecutions to deter the use of spyware as well as "phishing" scams. Phishing scams involve criminals using websites or e-mail addresses that mimic those of well-known and legitimate businesses to deceive Internet users into revealing personal information that can be used to defraud them.

The central feature of the Act is that it targets bad actors and bad behavior without unduly restricting innovation in the online universe. As the Judiciary committee and other entities have noted, one of the greatest difficulties in solving the spyware problem is that many legitimate and beneficial tools for making a user's Internet experience more enjoyable and productive are technologically indistinguishable from spyware that is used to harm users and computers. For example, an Internet "cookie" can be used to store detailed information about a user's preferences when visiting a much-frequented website. But the same technology can be used by identity thieves to track and store personal and financial information. The appropriate legislative target is not the cookie itself, but the criminals who use it for illegal purposes. The I-SPY Prevention Act is a measured and careful approach to combating spyware that captures this distinction.

Other legislative approaches revolve around notice-and-consent procedures that require computer users to be notified and either "opt in" or "opt out" of installing code at the time of installation. Ensuring user consent is critical, as is implicit in the term "authorized access" contained in the I-SPY Act and in existing Section 1030. In my view, however, a notice-and-consent approach is ill-advised for three reasons.

First, bad actors – the criminals we should be most concerned about – are unlikely to comply with that requirement. As we learned with the CAN-SPAM Act, legislatively mandating a certain approach is a far cry from ensuring that others comply with it. Thus, legitimate uses of technology will be burdened by notice-and-consent requirements while bad actors will most likely ignore them.

Second, the more notices and warnings that Internet users see, the less likely they are to pay attention to any single one. In 2005, the Pew Internet & American Life Project proved this point. A diagnostic site included a clause in one of its user agreements that promised $1,000 to the first person to write in and request the money. The agreement was downloaded more than 3,000 times before someone finally read the fine print and claimed the reward. Additionally, a Pew survey found that 73 percent of Internet users said that they do not always read user agreements, privacy statements, or other disclaimers before downloading or installing programs.

Finally, and most importantly, we must take care not to legislate the online user experience. Internet users have come to expect and demand a seamless, intuitive, and interactive experience with their online environment. Those expectations have led to the development of social networking and bookmarking sites, "wikis," and an explosion in user-generated content. Users are interacting with the Internet in a way that allows them to shape and control their online experience to a degree that, until recently, would have been unimaginable. This has been a tremendous boon to both consumers and the American economy. It would be unwise and unfortunate if we were to interfere with the continued evolution of the Internet through overbroad regulation.

The I-SPY Prevention Act avoids these pitfalls by focusing attention and resources where they are needed most, on criminal enterprises that harm Internet users and Internet commerce. That is why the Act also expresses the sense of Congress that the Department of Justice should use the Act to prosecute vigorously those who use spyware to commit crimes and those that conduct phishing scams.

Finally, I wish to clarify the Act's provision addressing state civil actions. Some people have construed § 1030A(c) as a bar on any civil action premised on conduct that violates the Act. That construction is incorrect. The Act merely states that violation of the Act *itself* cannot supply the basis for a state civil action. This provision is necessary because some States permit tort claims based on the violation of Federal criminal statutes. Were we to allow the Act to serve as the basis for tort claims in multiple jurisdictions, we would wind up with multiple and inconsistent state-court interpretations of the Act. Because much of the power and promise of the Internet comes from its ability to transcend geographic and political boundaries, we must avoid miring Internet commerce in potentially inconsistent state applications of Federal law. Section 1030A(c) ensures that this does not happen. At the same time, that provision does *not* preempt state-court cases based on independent state-law causes of action. Nor does it preempt actions of any kind in Federal court.

In closing, I simply note that a very broad coalition of high technology industries, commercial organizations, and public interest groups have come together to support this legislation. The breadth of the support for this bill extends to the House itself. When Representative Goodlatte and I brought this legislation to the floor in the past two Congresses it passed by an overwhelming majority. Indeed, the floor vote in the 109th Congress was 395-1. That support was there for a reason. Spyware is a serious and growing problem and the I-SPY Prevention Act is the right way to fight it.

I applaud the subcommittee for once again focusing on this very important piece of legislation. Thank you for the opportunity to testify today.