Oral Statement of

Arthur A. Butler
Attorney
Ater Wynne LLP

On Behalf of

Americans for Fair Electronic Commerce Transactions (AFFECT)

Before the United States Senate
Committee on Commerce, Science, and Transportation
Impact and Policy Implications of Spyware on Consumers and Businesses
June 11, 2008

Good afternoon. My name is Art Butler. I am an attorney with Ater Wynne LLP in Seattle, Washington. Today I represent AFFECT (Americans for Fair Electronic Commerce Transactions), which is a diverse group of non-profit and commercial entities, including consumer organizations, who are strongly committed to promoting the growth of fair and competitive commerce in software and other digital products. We commend you, Chairman Pryor, and all the sponsors of the Counter Spy Act (S. 1625), for introducing this important bill and holding today's hearing because, like you, our members are very worried about the privacy and security risks associated with spyware.

Our long statement makes it clear that AFFECT strongly supports S. 1625 because spyware is an insidious problem that needs to be addressed. The sad fact is that every computer in the United States is under attack from numerous sources trying to surreptitiously install or prevent removal of spyware that will allow the spy to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

Often spyware will contain a "backdoor", which is a method of bypassing normal authentication, securing remote access to a computer, while attempting to remain undetected. Someone who has gained access to your computer can install many types of devices to compromise security. It is generally agreed that spyware represents a significant threat to the security of any computer user's system and data.

AFFECT has one very serious concern with S. 1625. It is with the exception language of Subsection 6(a)(10)**,** which would permit a provider to monitor or interact with an individual's computer, or Internet or other network connection or service for the "detection or prevention of the unauthorized use of software fraudulent or other illegal activities."

This language is overly broad and could be construed to protect wrongful acts that can result in great harm to computer users in direct opposition to the purpose of the bill. It would allow a software vendor to surreptitiously download code onto a user's computer and freely violate the user's privacy by monitoring everything on his or her computer, as long as it did so under the guise of looking for unauthorized use, fraudulent, or illegal activities. It would allow the provider to set itself up as an ad hoc police force to conduct warrantless searches and to act as judge and jury to conduct unilateral seizures. Private entities *do not* and *should not* have the right to conduct law enforcement activities.

More troubling is the fact that the language of Subsection 6(a)(10) would effectively allow a software provider to unilaterally decide to remotely shut down the user's computer or Internet or other network connection or service. But whether the use of a particular software is "unauthorized," "fraudulent," or "illegal" is often subject to legitimate dispute and merits some judicial consideration before a provider is allowed to unilaterally employ a drastic remedy like remote disablement**.**

Our long statement summarizes a number of reported cases where software developers unilaterally determined that licensees didn't make appropriate payments and simply shut down the computer programs. But many disputes never make it to the courthouse steps because the balance of harm to be done via exercise of remote disablement is so overwhelmingly against the computer user that the mere threat of its use puts the user in an unfair position, and it must cave to the demands of the software vendor.

Moreover, in reaching into an individual's computer remotely to disable software residing on that computer, a software provider may not only violate privacy rights, but also damage the computer owner's other files. And the simple fact is that the code used to remotely enter a computer and disable the software or the network connection makes the computer vulnerable to security breaches by hackers, saboteurs, industrial and foreign governmental spies, and terrorists.

AFFECT strongly recommends that the exception provision of S. 1625 should <u>only</u> limit liability for interaction with a network, service, or computer that is undertaken to detect or prevent fraudulent or other illegal activities <u>as prohibited by the act itself</u>. Therefore, AFFECT proposes that Subsection 6(a)(10) of the bill be amended to read as follows:

> "(10) detection or prevention of fraudulent or other illegal activities <u>as prohibited by this Act</u>."

On behalf of AFFECT, thank you very much for the opportunity to appear before you today and for your consideration of our concerns. I would be happy to answer any questions you might have.