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. I am very pleased to appear before you today on behalf of AFFECT (Americans for Fair Electronic Commerce Transactions) at this important hearing on the impact and policy implications of spyware on consumers and businesses. AFFECT is a national coalition of consumer representatives, retail and manufacturing businesses, insurance institutions, financial institutions, technology professionals, librarians, and public interest organizations 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 because, like you, our members are very worried about the privacy and security risks associated with spyware. AFFECT strongly supports S. 1625. However, we are very concerned with the exception provision and believe it is overly broad. In our view, it could in fact be construed to protect wrongful acts that can result in great harm to computer users. We believe this section is in direct opposition to the laudable purpose of the bill and hope very much that you will consider the amendment which we propose today.

AFFECT's Concerns with Spyware

AFFECT has been active in representing the interests of software consumers in the debates about the appropriate language to be included in anti-spyware legislation in several states and has advocated strenuously that these legislatures not adopt exception language so broad that it swamps the prohibitions that are designed to protect computer users. Since AFFECT began actively educating legislators in the states of the potential for damage, creation of security vulnerabilities, and for invasion of privacy and unauthorized search and seizure in relation to consumers' computers due to the exception language in question – the language has failed to pass in even one state legislature.

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.

While the term "spyware" suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware can collect various types of personal information, interfere with the user's control of the computer, change computer settings, result in slow connection speeds, loss of Internet or other programs, disable software firewalls and anti-virus software, and/or reduce browser security settings, thus opening the system to further infections. It can enable identity theft and fraud.

Often spyware will contain a "backdoor," which is a method of bypassing normal authentication, securing remote access to a computer and obtaining access to plaintext, while attempting to remain undetected. Someone who has gained access to your computer can install many types of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. Some backdoors, such as the Sony/BMG rootkit[1]

[1] A "rootkit" is a program designed to take fundamental control of a computer system, without authorization by the system's owners and legitimate managers. Typically, rootkits act to obscure their presence on the system through

distributed silently on millions of music CDs through late 2005, are intended as digital rights management (DRM) measures and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers. The copy prevention software Sony BMG included on its CDs was automatically installed on Windows desktop computers when customers tried to play the CDs. The software interferes with the normal way in which the Microsoft Windows operating system plays CDs, opening security holes that allow viruses to break in, and causing other problems.[2]

It is generally agreed that spyware represents a significant threat to the security of any computer owner's data. Even for large enterprises spyware represents a serious threat to the integrity of intellectual property, confidential data, and personally identifiable information of employees and customers. Accordingly, AFFECT supports legislative efforts, like S. 1625, that are designed to curb the use of harmful spyware.[3]

AFFECT's Concerns with the Exception Provision of S. 1625

AFFECT has concerns with the exception section of S. 1625, section (6), which 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.

We are particularly concerned about 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." The reference to "unauthorized" is too vague and raises a number of questions. "Authorized" by whom? What is the process for authenticating the identity of the person using the software? And what are the standards for determining whether that person has the authority to perform a certain operation, and who decides?

This language 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

---

subversion or evasion of standard operating system security mechanisms. Often, they are also Trojans as well, fooling users into believing they are safe to run on their systems.

[2] As a result, a number of parties filed lawsuits against Sony BMG; the company eventually recalled all the affected CDs.

[3] S. 1625 (Pryor), introduced in June 2007, would protect against the unauthorized installation of software that is used to take control of a computer in order to cause damage, collect personal information without consent, or otherwise enable identity theft.

judicial consideration before a provider is allowed to unilaterally employ a drastic remedy like remote disablement**.**

Permitting unilateral remote disablement is simply bad public policy. Unilateral remote disablement can cause great harm to any computer owner who depends on access to and use of that computer, connection or service. For example, the shutdown of an owner's system can cause great harm to:

- a teacher using a computer to prepare for classroom lectures;
- an insurer depending on a computer system to pay claims;
- a manufacturer trying to deliver its products to meet contractual commitments; or
- the public's access to online library materials.

That harm can be significantly larger than the harm to the software vendor (not getting a license fee).

Even large enterprises are concerned about the threat of remote disablement. There have been a number of reported cases where software developers unilaterally determined that licensees didn't make appropriate payments and simply shut down the computer programs.[4] The most widely reported was a case where a small software developer, Logisticon, Inc., installed malware within

[4] Other cases include the following: In 1998 in *Franks & Sons, Inc. v. Information Solutions, Inc.*, the software developer installed a "drop-dead" code in the program. When the customer failed to pay as promised, the developer activated the drop-dead code, which prevented the customer from accessing the software as well as any stored information. The customer didn't know about the drop-dead code, and the court found that it would be unconscionable to allow the software developer to hold the licensee ransom as it did.

In 1991, in *American Computer Trust Leasing v. Jack Farrell Implement Co.*, 763 F. Supp. 1473 (D. Minn. 1991), the software developer, in a dispute over payment for the software, remotely deactivated the software. The contract provided that he developer, who owned the software, could remotely access the licensee's computer in order to service the software and that, if the licensee defaulted, the agreement was cancelled. When the licensee didn't pay, the developer told the licensee that it was going to deactivate the program, which it promptly did. The licensee sued for damages, but the court ruled in favor of the developer on the grounds that the deactivation was "merely an exercise of [the developer's] rights under the software license agreement. . ."

There have been many other cases involving software developers either putting drop-dead code in their products or remotely disabling code when they thought the other party was in breach. For example, a Dallas medical device software developer was sued in 1989 for using a phone line to deactivate software that compiled patients' lab results. The case was settled. In 1990, during a dispute about the performance of a piece of code, the developer simply logged in and removed the code, until the licensee released the developer from any liability. The licensee claimed that the general release was signed under duress, since he was being held economic hostage. *Art Stone Theatrical Corp. v. Technical Programming & Support Systems, Inc.*, 549 N.Y.S.2d 789 (App. Div. 1990).

In 1991, in *Clayton X-Ray Co. v. Professional Systems Corp.*, 812 S.W.2d 565 (Mo. Ct. App. 1991), a company involved in a payment dispute logged into the licensee's computer and disabled the software. When the licensee tried to log on to see its files, all it saw was a copy of the unpaid bill. A jury awarded the licensee damages.

In *Werner, Zaroff, Slotnick, Stern & Askenazy v. Lewis*, 588 N.Y.S.2d 960 (Civ. Ct. 1992), a law firm contracted with a company to develop billing and insurance software. When the software reached a certain number bills, and when the developer decided it had not been paid sufficiently, it shut down the software disabling access to the law firm's files. The law firm sued successfully.

warehouse-management software delivered to cosmetic company, Revlon Inc. When the parties got into a dispute over whether the software had bugs and didn't perform as promised, Revlon withheld payment. Logisticon then tapped into Revlon's computers and disabled the program, which paralyzed Revlon's shipping operations for three days. Losses to Revlon were about $20 million. Revlon sued, charging extortion. Logisticon claimed this was simply "electronic repossession." The case was settled out of court.

Clearly 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. The ability to unilaterally disable a user's computer or critical software running on it provides the software, network, or service provider undue leverage in a dispute even if the remedy is not exercised. Faced with a crippling and possibly even fatal disruption of its business, a user could be intimidated into relinquishing its rights and setting up precedents for its further disadvantage. This is because the risk to the provider that it will be held to have acted improperly is indefinite and its potential liability severely limited. Even if a provider wrongly exercises the remote disablement, it is unlikely the injured user will be able to recover money damages for the harm resulting from this action, including losses to the user's business attributable to the wrongful act, because providers routinely disclaim consequential damages in their licensee agreements; in fact, they routinely limit recoverable damages to the amount of the license fee.

Moreover, in reaching into an individual's computer remotely to disable software residing on that computer, the software provider may not only violate privacy rights, but also damage the computer owner's other files. And the monitoring and remote disablement of software on an owner's computer by an outsider may compromise private information of employees, confidential and proprietary information of the owner, and, in some cases, national security information. As a result, it is possible that they could put an owner into breach of obligations it has under other laws (e.g., Health Insurance Portability and Accountability Act).

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. The consequences of a successful intentional or even accidental misuse of a computer system range from loss of confidentiality to loss of system integrity, which may lead to more serious concerns, like data theft or loss, or, in the case of a business, significant financial losses or worse. When there is an opportunity to negotiate, many enterprises, including governmental entities, will insist that their software license agreements contain a warranty prohibiting any "self-help code" or other software routing designed to disable a computer program automatically or that is under the positive control of a person other than the licensee of the software. Unfortunately, with mass market licenses individual consumers and businesses are not able to negotiate for a "no self-help code" warranty.

Proposed Amendment

S. 1625 is a commendable piece of legislation that addresses a real problem faced by computer users throughout this country. AFFECT supports it, but strongly recommends that the exception

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

> "(10) detection or prevention of ~~the unauthorized use of software~~ fraudulent or other illegal activities as prohibited by this Act."

Conclusion

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.