

Section 106, Computer Trespassers (Section 105 in HR 2975)

PROBLEMS WITH ADMINISTRATION PROPOSAL

- One of the overlooked but most troubling provisions of the Administration's bill.
- Would eviscerate the protections of the Electronic Communications Privacy Act by allowing an ISP to allow the government to intercept wire or electronic communications of any "unauthorized" user.
- Could turn ISP "terms of service" into a license to intercept email without court order.
- Says that anyone accessing a computer "without authorization" has no privacy rights and can be tapped by the government without a court order, if the operator of the computer system says its okay. "Without authorization" is not defined.
- Relatively minor violations - like downloading a copyrighted mp3 file - would allow an ISP to authorize the government to tap all of that person's communications. With no judicial permission, oversight, or supervision.
- No time limit – the extrajudicial wiretapping could go on for ever.
- Not limited to computer communications – allows interception of telephone conversations of computer hacker (this has to be a drafting flaw, but it exemplifies the overbreadth of the provision).
- ISPs will be put in the unenviable position of choosing between the privacy rights of their customers or the requests of law enforcement agents who claim that a person is committing a crime or violating terms of service.

EXPLANATION OF AMENDMENT

Limited to situations where the protected computer is experiencing an ongoing pattern of activity characteristic of hackers.

Focused on interception of communications to, from or through the protected computer.

Conforms to DOJ section by section justification, which is that this should allow service providers "to exercise their rights to protect themselves from unauthorized attackers."

Conforms to existing language in Title III allowing service providers to monitor their own systems to protect their "rights or property."

Limited to emergency situations involving an ongoing attack upon a protected computer. The language requiring the interception to cease as soon as the communications sought are obtained to 48 is drawn directly from the current emergency authority, 18 USC

2518(7), which covers situations involving organized crime, threats to the national security, and situations involving immediate danger of death or serious physical injury.

Includes language agreed to by DOJ in the Senate making it clear that a person shall not be considered a computer trespasser if the person is known by the owner or operator of the protected computer to have a preexisting contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

We are not trying to protect the communications of unauthorized persons - we are trying to limit the warrantless interception of their communications to the situations where time is of the essence and a system operator is trying to protect its system from attack. We are trying to put a time limit on such interception, after which a judge can decide what is authorized and what isn't. We would use a 48 hour time frame, which is the emergency period already in the law for national security cases and cases involving risk of loss of life.

We agree with DOJ that interception without court order should be permitted in the following circumstance: a computer owner or operator (a university, an ISP, a web host) sees its system being attacked. Under 2511(2)(a)(i), the operator can monitor its own system to protect its rights or property and disclose the results to the government. But some system operators are initially at a loss in terms of expertise, equipment or resources to monitor their systems and determine the nature of the attack. They want the assistance of the government, until they can respond to the attack. Most of these cases are very short-lived - hours, usually. Our amendment is designed to allow the operator to request the government's assistance.

This is what we don't want: unlimited monitoring anytime an ISP thinks that someone is making unauthorized use of their system. "Unauthorized access" is not a defined term. Our fear is that ISP terms of service (no streaming video, no downloading copyrighted material) will be the basis for declaring a person an unauthorized user, justifying unlimited government monitoring.

Already, if an ISP suspects that a user is making illegal use of their system, they can report that to the FBI and the FBI can get an order for interception.

Amendment to H.R. 2975

Page 10, line 25, strike "and" and all that follows through page 11, line 24 and insert –

(2) in subsection 2511(2)(a) of title 18, United States Code, by inserting after subparagraph (ii) the following:

"(iii) It shall not be unlawful under this chapter for a person acting under color of law to assist the owner or operator of a protected computer to intercept electronic communications to, from or through such computer where –

- (A) such owner or operator of a protected computer is attempting to respond to an ongoing pattern of communications activity that threatens the integrity or operation of any protected computer and requests assistance to protect its rights or property,
- (B) the interception is limited to communications threatening the integrity or operation of a protected computer,
- (C) the interception is limited to communications to or from a person who has no authorization to access the protected computer where the interception will occur,
- (D) the interception does not acquire the communications of any person known by the owner or operator of the protected computer where the interception occurs to have a pre-existing contractual relationship with the owner or operator of such computer for access to all or part of the protected computer, and
- (E) the interception ceases as soon as the communications sought are obtained or after 48 hours, whichever is earlier, unless an interception order is obtained under this chapter."; and