U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 14, 2008

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

This letter presents the views of the Department of Justice on H.R. 1525, the "Internet Spyware (I-SPY) Prevention Act of 2007." The Department supports the bill's goal of addressing the use of spyware to commit identity theft and other privacy invasions, but believes that the most effective and efficient way to accomplish that goal is to amend existing statutes, not to create a new offense. Indeed, the Senate has already taken this approach when it passed S. 2168 on November 15, 2007, which, if enacted, would render H.R. 1525 totally unnecessary. The Department has strongly supported S. 2168 and believes that it would provide substantial assistance in combating the widespread damage that identity theft inflicts upon its victims and the U.S. economy.

The Department's overarching concern is that the existing laws criminalizing conduct related to computers, particularly 18 U.S.C. § 1030, are complex and increasingly interdependent. Creating another Federal offense related to the unauthorized access of computers risks disturbing the balance of the computer crime regime. In particular, not only will proposed section 1030A overlap with much of the current law, but it also may have the unintended consequence of *decreasing* the effectiveness of the Department's current tools for prosecuting computer crimes. The following sections detail our specific concerns with the proposed bill.

1. The Basic Definition of the New Offense Would Not Reach Many Types of Attacks Involving Spyware

Both proposed subsection 1030A(a) and subsection 1030A(b) define the offense as unauthorized access of a computer "by causing" software to be installed. One reading of this phrase suggests that the access and the installation must be essentially one action. However, the Department's experience is that there frequently are two or more separate steps to an intrusion involving spyware. For example, a hacker could use some other method to bypass a computer's security and only then install spyware on the system. Indeed, even automated worms generally do not accomplish the unauthorized access of a computer by the very act of installing spyware.

This problem of interpretation highlights the difficulty of establishing a new Federal spyware crime flexible enough to remain relevant to advances in technology. Existing 18 U.S.C. § 1030 would reach almost all of these types of intrusions without regard to exactly how many steps the intruder employed before causing installation of the spyware. The better course would be to correct limitations in the existing law, as the Senate did when it passed S. 2168 on November 1, 2007. In that bill, the Senate, among other things, proposed amending 18 U.S.C. § 1030(a)(5) to appropriately penalize the use of malicious spyware and keyloggers by eliminating the current requirement that the defendant's actions must result in a loss exceeding $5,000 and by adding a provision to 18 U.S.C. § 1030(c)(4) to make causing damage to ten or more computers a felony.

2. Proposed Section 1030A is Unnecessary.

We believe that H.R. 1525 would provide little benefit to law enforcement in fighting spyware, especially if S. 2168 was signed into law. First, proposed 18 U.S.C. § 1030A(a) would create the new crime of accessing a computer without authorization by causing a computer program to be installed, in furtherance of another Federal criminal offense. However, existing laws already prohibit virtually all of this conduct. For example, 18 U.S.C. § 1030(a)(4) makes it a felony punishable by five years of imprisonment to access a computer *in any way* without authorization in furtherance of the crime of fraud. Installation of spyware in furtherance of a fraud scheme also is covered by the traditional wire fraud statute, 18 U.S.C. § 1343, which carries a maximum penalty of 20 years imprisonment. Prosecutors have employed existing statutes successfully to prosecute offenses in which criminals install spyware in order to obtain information for financial gain.

In addition, if a spyware program intercepts communications instead of merely extracting stored information from a victim computer, the spyware's use would violate existing wiretap laws, 18 U.S.C. §§ 2511 and 2512 (punishable by five years in prison). Conversely, obtaining stored information from a computer without authorization already is prohibited by 18 U.S.C. § 1030(a)(2)(C) (making it a felony to obtain information without authorization "in furtherance of any criminal or tortious act," punishable by five years of imprisonment); 18 U.S.C. § 1030(c)(2)(B).[1]

Proposed paragraphs 1030A(b)(1) and (2) of the bill reflect the serious damage that spyware causes to victims' computers. These provisions would criminalize, among other things, obtaining information by installing spyware with the intent to cause damage to a computer and impairing the security protection of the computer by installing spyware with intent to cause damage to a computer. However, both are superfluous because installation of any spyware program would qualify as causing damage under existing 18 U.S.C. § 1030(e)(8) (by impairing

[1] The only limitation on the use of existing section 1030(a)(2)(C) is that it requires that the conduct involve an interstate communication. Although this fact would not be a hindrance in most spyware prosecutions, S. 2168 closes this loophole.

the integrity of the data, program, or system). Thus, these acts can be punished under existing paragraph 1030(a)(5). Although existing paragraph 1030(a)(5) does contain some limitations in prosecuting spyware offenses, the better course would be to eliminate these limitations within the existing framework, as in S. 2168.

3. Proposed 1030A Could Actually *Reduce* Penalties for Installing Spyware

Proposed subsection 1030A would impose maximum sentences of two or five years of incarceration, depending upon whether the violation fell under paragraph (a) or (b). The bill does not include the recidivist provision contained in offenses under 18 U.S.C. § 1030 that doubles the maximum penalty for repeat offenders. The Department does not believe that there is any reason to treat a second offense related to installing spyware more leniently than a second offense for any other type of computer intrusion.

Proposed paragraph 1030A(b)(1) is unclear. It would prohibit installing spyware that stole personal information with the "intent to defraud," but this prohibition overlaps with proposed paragraph 1030A(a), which would prohibit installing spyware used in furtherance of any criminal offense, including fraud. Because paragraph 1030A(b)(1) contains a maximum sentence of only two years, courts may feel bound to apply the subsection with a lesser penalty to spyware fraud schemes. Moreover, paragraph 1030A(b)(1) also would conflict with existing 18 U.S.C. § 1030(a)(4), which criminalizes unauthorized access of a computer with intent to defraud and subjects offenders to five years of imprisonment. H.R. 1525 could lead courts to apply its provision instead of existing section 1030(a)(4), actually reducing the penalty for criminals who install spyware.

Additionally, paragraph 1030A(d)(2) would define "personal information" to include, among other things, "drivers license number" [sic], credit card or bank account number or any password or access code associated with a credit card or bank account. This definition is too narrow, omitting brokerage accounts, mortgages, insurance, and other financial accounts that can be accessed online.

Similarly, paragraph 1030A(b)(1) would punish the unauthorized installation of spyware that "obtains ... personal information with the intent to ... injure a person" with a maximum sentence of two years. Most economic injuries to victims are already punishable by five years of imprisonment under 18 U.S.C. § 1030(a)(4)'s "intent to defraud" language. Other injuries are covered by 18 U.S.C. § 1030(a)(2), a 5-year felony where the intrusion occurs in furtherance of a tortious act. If H.R. 1525 were enacted, courts could impose penalties under its provisions that are less than those provided for under current law.

4. Technical Suggestions for H.R. 1525

If, despite our concerns, Congress proceeds with H.R. 1525, the Department has several specific concerns about the language used in the bill. In that event, we would be happy to consult with Congress to offer drafting suggestions to make H.R. 1525 less likely to hinder existing enforcement efforts.

Thank you for the opportunity to present our views. The Department appreciates the House of Representatives' leadership in ensuring that our country's laws evolve to meet these new challenges. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Brian A. Benczkowski
Principal Deputy Assistant Attorney General

cc: The Honorable Arlen Specter
Ranking Minority Member