

ATTORNEY GENERAL'S LEGISLATIVE PROGRAM
PROGRAM BILL # 58-05

Senate #

Assembly #

Attorney General Eliot Spitzer
The Capitol, Albany, NY 12224
(518) 486-3000

MEMORANDUM

AN ACT to amend the Penal Law, in relation to
computer crimes

PURPOSE:

This bill will facilitate the prosecution of computer crimes.

SUMMARY OF PROVISIONS:

Section 1 of the bill adds Penal Law §§ 156.40 and 156.41 to create two new crimes of Criminal Use of Encryption in the Second Degree (A misdemeanor) and First Degree (E felony). A person is guilty of Criminal Use of Encryption in the Second Degree when he or she intentionally uses encryption to facilitate or conceal the commission of a crime, conceal the identity of another person who commits a crime, or disrupt the normal operation of a computer or computer system. Criminal Use of Encryption in the First Degree applies when the crime which is concealed or facilitated is a felony, or the offender has previously been convicted of a Penal Law Article 156 computer crime.

Section 2 of the bill amends Penal Law § 156.00(6) to delete the requirement that unauthorized computer users be notified that access requires authorization.

Section 3 of the bill adds Penal Law § 156.00(8) to define the term "encryption."

Sections 4 and 5 of the bill amend Penal Law §§ 215.35 and 215.40 to clarify that the crime of tampering with physical evidence covers: (1) tampering with computer information, including computer programs, computer data and computer services; and (2) tampering with evidence that has been requested as part of a government investigation, even if the material or information may not actually be offered as evidence in an official proceeding. In addition, Section 5 of the bill makes the crime of tampering with physical evidence a class D felony rather than a class E felony.

Section 6 of the bill amends Penal Law § 156.00(5) to include within the definition of "computer material" personal information such as employment, salary, credit, or other financial or personal data.

Sections 7 and 8 of the bill amend Penal Law § 156.10 to increase to a class E felony gaining unauthorized access to a computer or computer service by means of an access device

which is known to be forged or stolen, or through use of a fictitious identity.

Sections 9 through 12 of the bill amend Penal Law §§ 156.20, 156.25, 156.26 and 156.27 to prohibit intentionally damaging or concealing computer data or a computer program. In addition, section 11 increases to a class D felony tampering with a computer or computer service with the intent to endanger public safety, including interrupting or impairing the provision of services by a public or private utility, governmental agency, public carrier or public communication service.

Sections 13 and 14 add Penal Law § 115.00(3) to include within the crime of Criminal Facilitation in the Fourth Degree disclosure of a computer password, identifying code, personal information number or other confidential information about a computer security system where such disclosure provides the means, and in fact aids, another person to commit any crime.

Section 15 of the bill amends Penal Law § 460.10(1) to certain offenses under Penal Law Article 156 (Offenses Involving Computers) within the definition of "criminal act" for purposes of an enterprise corruption prosecution.

EXISTING LAW

Penal Law §§ 156.05 and 156.10 require proof that computer use was "without authorization" to prosecute an individual for, respectively, Unauthorized Use of a Computer or Computer Trespass. "Without authorization" under Penal Law §156.0 is limited to instances where actual, or constructive, notice of restricted use is given to the unauthorized user.

JUSTIFICATION:

The dramatic increase in the use of computers, and ever-increasing interconnection through the Internet and other networks, have fundamentally altered the types of crimes that can be committed and the ease with which individuals can be victimized. This bill seeks to address such conduct by creating new crimes and increasing punishment for others in a number of ways.

First, this bill creates two new crimes of Criminal Use of Encryption in the First and Second Degree. The use of encryption to engage in criminal conduct poses special risks to society because it adds to the difficulties of law enforcement. The new crimes apply when encryption is used to facilitate or conceal the commission of a crime, conceal the identity of another person who commits a crime, or disrupt the normal operation of a computer or computer system.

Second, one byproduct of the evolution of information technology has been the erosion of our right to privacy. This bill seeks to protect the privacy of personal information by increasing criminal penalties when an unauthorized person knowingly gains access through a computer or computer system to data about employment, salary, credit, or other financial or personal

information. The bill further protects privacy interests by increasing criminal penalties for gaining unauthorized access to a computer or computer service by means of an access device which is known to be forged or stolen, or through use of a fictitious identity.

Third, this bill expands the scope of conduct covered, and increases criminal penalties for tampering with a computer or computer system with the intent to endanger public safety, including shutting down the operation of a public utility or public communication system. This provision responds to the heightened awareness, since the September 11th attacks, of the potential for dangerous large scale disruptions. In addition, the bill expands the scope of conduct prohibited under Penal Law Article 156 tampering crimes to include intentionally concealing or damaging computer data or the computer programs of another person. Current law prohibits only the alteration or destruction of such data or programs.

Fourth, this bill updates the evidence tampering law to make clear that the term "physical evidence" includes all forms of computer records and information, and specifies that encryption, which is a form of "concealment," constitutes "tampering with physical evidence." The bill also makes "tampering with physical evidence" a class D felony offense rather than a class E felony. The federal Sarbanes-Oxley law (Public Law 107-204) imposes imprisonment of up to 20 years for tampering with records to be used in official proceedings. This bill would create comparable penalties under New York law. Finally, Penal Law § 215.40 refers to tampering with evidence that "is about to be produced" in an "official proceeding or a prospective official proceeding." The courts have construed this language broadly, and it clearly covers evidence that has been or may be subpoenaed by regulatory and law enforcement agencies, but the language should be updated to make explicit that it prohibits the destruction of information that has been or may be requested by government as a part of an informal inquiry.

Finally, the bill updates the statutory provisions governing the crimes of Computer Trespass and Unauthorized Use of a Computer. In prosecuting such crimes, prosecutors currently must demonstrate that notice forbidding unauthorized computer access has actually, or constructively, been provided to unauthorized users. This requirement may allow hackers and others who surreptitiously gain access to, and use, computers, but do not steal or destroy computer material, to do so with impunity. In particular, the current definition of "without authorization" requires that a criminal be notified that access is not authorized by (a) actual or written notice, (b) written notice posted adjacent to the computer, or (c) a notice displayed on or announced by the computer.

When this notice requirement was enacted in 1986, most computer users gained access to computers by sitting in front of a CPU and monitor that were not connected to any other computer. That is no longer the case, and now almost every computer is connected to other computers, including other computers on an office network or through the Internet.

Because of this ubiquitous connectivity, there are now numerous ways for users to enter a computer, sometimes surreptitiously. There is no way, for most of these entry points, to provide

notice to users that authorization is required to enter. Penal Law §156.00(6)(c) does establish a presumption that such notice was provided if the computer is programmed to announce a warning against unauthorized use automatically. However, there has been an extraordinary increase in the number of computers owned by individuals for personal use in their homes since codification of this presumption, and most such computers are not programmed to provide such warnings.

This legislation does not affect the requirement that prosecutors prove that the defendant knowingly used or caused use of a computer without, or in excess of, authorization and, in the case of Unauthorized Use of a Computer, to further prove that the computer was programmed with a password or other system designed to prevent unauthorized entry.

LEGISLATIVE HISTORY

Similar provisions were introduced during the 2003-04 legislative session as S.4842 and S.7205.

FISCAL IMPLICATIONS

There are no fiscal implications..

EFFECTIVE DATE

The bill would take effect on the first day of November following enactment.