



Senate

General Assembly

File No. 479

January Session, 2001

Substitute Senate Bill No. 1280

Senate, April 26, 2001

The Committee on Judiciary reported through SEN. COLEMAN of the 2nd Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

AN ACT CONCERNING COMPUTER CONTAMINANTS.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1 Section 1. Section 53a-250 of the general statutes is repealed and the
2 following is substituted in lieu thereof:

3 For the purposes of this part and section 52-570b:

4 (1) "Access" means to instruct, communicate with, store data in or
5 retrieve data from a computer, computer system or computer network.

6 (2) "Computer" means a programmable, electronic device capable of
7 accepting and processing data.

8 (3) "Computer network" means (A) a set of related devices
9 connected to a computer by communications facilities, or (B) a complex
10 of two or more computers, including related devices, connected by
11 communications facilities.

12 (4) "Computer program" means a set of instructions, statements or
13 related data that, in actual or modified form, is capable of causing a
14 computer or computer system to perform specified functions.

15 (5) "Computer services" includes, but is not limited to, computer
16 access, data processing and data storage.

17 (6) "Computer software" means one or more computer programs,
18 existing in any form, or any associated operational procedures,
19 manuals or other documentation.

20 (7) "Computer system" means a computer, its software, related
21 equipment, communications facilities, if any, and includes computer
22 networks.

23 (8) "Data" means information of any kind in any form, including
24 computer software.

25 (9) "Person" means a natural person, corporation, limited liability
26 company, trust, partnership, incorporated or unincorporated
27 association and any other legal or governmental entity, including any
28 state or municipal entity or public official.

29 (10) "Private personal data" means data concerning a natural person
30 which a reasonable person would want to keep private and which is
31 protectable under law.

32 (11) "Property" means anything of value, including data.

33 (12) "Computer contaminant" means any set of computer
34 instructions that are designed to damage or destroy information within
35 a computer, computer system or computer network without the
36 consent or permission of the owner of the information. Computer
37 contaminants include, but are not limited to, viruses or worms that are
38 self-replicating or self-propagating and are designed to contaminate
39 other computer programs or data, consume computer resources or

40 damage or destroy the normal operation of a computer.

41 Sec. 2. Section 53a-251 of the general statutes is repealed and the
42 following is substituted in lieu thereof:

43 (a) A person commits computer crime when [he] such person
44 violates any of the provisions of this section.

45 (b) (1) A person is guilty of the computer crime of unauthorized
46 access to a computer system when, knowing that [he] such person is
47 not authorized to do so, [he] such person accesses or causes to be
48 accessed any computer system without authorization.

49 (2) It shall be an affirmative defense to a prosecution for
50 unauthorized access to a computer system that: (A) The person
51 reasonably believed that the owner of the computer system, or a
52 person empowered to license access thereto, had authorized [him]
53 such person to access; (B) the person reasonably believed that the
54 owner of the computer system, or a person empowered to license
55 access thereto, would have authorized [him] such person to access
56 without payment of any consideration; or (C) the person reasonably
57 could not have known that [his] such person's access was
58 unauthorized.

59 (c) A person is guilty of the computer crime of theft of computer
60 services when [he] such person accesses or causes to be accessed or
61 otherwise uses or causes to be used a computer system with the intent
62 to obtain unauthorized computer services.

63 (d) A person is guilty of the computer crime of interruption of
64 computer services when [he] such person, without authorization,
65 intentionally or recklessly disrupts or degrades or causes the
66 disruption or degradation of computer services or denies or causes the
67 denial of computer services to an authorized user of a computer
68 system.

69 (e) A person is guilty of the computer crime of misuse of computer
70 system information when: (1) As a result of [his] such person accessing
71 or causing to be accessed a computer system, [he] such person
72 intentionally makes or causes to be made an unauthorized display,
73 use, disclosure or copy, in any form, of data residing in, communicated
74 by or produced by a computer system; or (2) [he] such person
75 intentionally or recklessly and without authorization (A) alters,
76 deletes, tampers with, damages, destroys or takes data intended for
77 use by a computer system, whether residing within or external to a
78 computer system, or (B) intercepts or adds data to data residing within
79 a computer system; or (3) [he] such person knowingly receives or
80 retains data obtained in violation of subdivision (1) or (2) of this
81 subsection; or (4) [he] such person uses or discloses any data [he] such
82 person knows or believes was obtained in violation of subdivision (1)
83 or (2) of this subsection.

84 (f) A person is guilty of the computer crime of destruction of
85 computer equipment when [he] such person, without authorization,
86 intentionally or recklessly tampers with, takes, transfers, conceals,
87 alters, damages or destroys any equipment used in a computer system
88 or intentionally or recklessly causes any of the foregoing to occur.

89 (g) A person is guilty of the computer crime of introduction of a
90 computer contaminant when such person knowingly, wilfully and
91 without authorization, directly or indirectly, damages or destroys or
92 attempts to damage or destroy any computer, computer network,
93 computer software, computer system, computer program or data by
94 introducing a computer contaminant into any computer, computer
95 program, computer system or computer network.

ET *JOINT FAVORABLE SUBST. C/R* *JUD*
JUD *JOINT FAVORABLE*

The following fiscal impact statement and bill analysis are prepared for the benefit of members of the General Assembly, solely for the purpose of information, summarization, and explanation, and do not represent the intent of the General Assembly or either House thereof for any purpose:

OFA Fiscal Note

State Impact: Potential Minimal Cost, Potential Minimal Revenue Gain

Affected Agencies: Various Criminal Justice Agencies

Municipal Impact: None

Explanation

State Impact:

The bill appears to expand the range of activities that could be considered computer crime. The extent to which this would occur is anticipated to be minimal and any associated workload for criminal justice agencies can be handled within normal budgetary resources. According to court statistics, computer crimes rarely result in conviction under the original charge. During the year 2000, 16 computer crime offenses occurred, all of which did not result in a conviction. No revenue related to fines was collected for these offenses.

OLR Bill Analysis

sSB 1280

AN ACT CONCERNING COMPUTER CONTAMINANTS.**SUMMARY:**

This bill makes it a crime to introduce a contaminant such as a virus into a computer system or its components. Under the bill, the penalty for this crime depends on the amount of damage the contaminant does, with a maximum penalty of a fine of up to \$15,000, imprisonment from one to 20 years, or both. The action must be knowing, willful, and without authorization to be a crime.

EFFECTIVE DATE: October 1, 2001

INTRODUCING COMPUTER CONTAMINANTS

Under the bill, a person is guilty of the computer crime of introducing a computer contaminant if he directly or indirectly damages or destroys or attempts to damage or destroy any computer, program, system, network, software, or data by introducing a contaminant into a computer, program, system, or network.

Under the bill, a contaminant is any set of instruction designed to damage or destroy information within a computer, system, or network without the information owner's consent or permission. Contaminants include viruses and worms that replicate or propagate themselves and that are designed to (1) contaminate other programs or data, (2) consume computer resources, or (3) destroy the computer's normal operations.

The law already makes a crime to destroy computers or perform other specified destructive acts. By law, the penalty for computer crime depends on the amount of damage done. Table 1 lists the penalties for various degrees of computer crime, which the bill applies to the crime of introducing a contaminant. For each degree of the crime, the

violator can be fined, imprisoned, or both.

Table 1: Penalties for Computer Crimes

Degree	Amount of Damage	Maximum Fine	Imprisonment
1 st	More than \$10,000	\$15,000	1 to 20 years
2 nd	More than \$5,000	\$10,000	1 to 10 years
3 rd	More than \$1,000	\$5,000	1 to 5 years
4 th	More than \$500	\$2,000	Up to one year
5 th	Up to \$500	\$1,000	Up to six months

COMMITTEE ACTION

Energy and Technology Committee

Joint Favorable Substitute Change of Reference

Yea 13 Nay 0

Judiciary Committee

Joint Favorable Report

Yea 39 Nay 0