WEST VIRGINIA LEGISLATURE

2020 REGULAR SESSION

Introduced

Senate Bill 261

BY SENATORS IHLENFELD, BALDWIN, STOLLINGS, AND

MAYNARD

[Introduced January 10, 2020; referred

to the Committee on the Judiciary]

1   A BILL to amend and reenact §61-3C-3 and §61-3C-4 of the Code of West Virginia, 1931, as

2   amended, all relating to contaminating a computer with ransomware; creating criminal

3   penalties for introducing ransomware into any computer, computer system, or computer

4   network with the intent to extort money or other consideration; setting forth the elements

5   of the offense; and defining a term.

Be it enacted by the Legislature of West Virginia:

ARTICLE 3C. WEST VIRGINIA COMPUTER CRIME AND ABUSE ACT.

§61-3C-3. Definitions.

1   As used in this article, unless the context clearly indicates otherwise:

2   (a) "Access" means to instruct, communicate with, store data in, retrieve data from,

3   intercept data from, or otherwise make use of any computer, computer network, computer

4   program, computer software, computer data, or other computer resources.

5   (b) "Authorization" means the express or implied consent given by a person to another to

6   access or use said person's computer, computer network, computer program, computer software,

7   computer system, password, identifying code, or personal identification number.

8   (c) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-

9   speed data processing device performing logical, arithmetic, or storage functions and includes

10   any data storage facility or communication facility directly related to or operating in conjunction

11   with such device. The term "computer" includes any connected or directly related device,

12   equipment, or facility which enables the computer to store, retrieve, or communicate computer

13   programs, computer data, or the results of computer operations to or from a person, another

14   computer, or another device, file servers, mainframe systems, desktop personal computers,

15   laptop personal computers, tablet personal computers, cellular telephones, game consoles, and

16   any other electronic data storage device or equipment, but such term does not include an

17   automated typewriter or typesetter, a portable hand-held calculator, or other similar device.

18   (d) "Computer contaminant" means any set of computer instructions that are designed to

19   damage or destroy information within a computer, computer system or computer network without

20   the consent or permission of the owner of the information. They include, but are not limited to, a

21   group of computer instructions commonly called viruses or worms that are self-replicating or self-

22   propagating and are designed to contaminate other computer programs or computer data,

23   consume computer resources, or damage or destroy the normal operation of the computer.

24   (e) "Computer data" means any representation of knowledge, facts, concepts, instruction,

25   or other information computed, classified, processed, transmitted, received, retrieved, originated,

26   stored, manifested, measured, detected, recorded, reproduced, handled, or utilized by a

27   computer, computer network, computer program, or computer software and may be in any

28   medium, including, but not limited to, computer printouts, microfilm, microfiche, magnetic storage

29   media, optical storage media, punch paper tape, or punch cards, or it may be stored internally in

30   read-only memory or random access memory of a computer or any other peripheral device.

31   (f) "Computer network" means a set of connected devices and communication facilities,

32   including more than one computer, with the capability to transmit computer data among them

33   through such communication facilities.

34   (g) "Computer operations" means arithmetic, logical, storage, display, monitoring, or

35   retrieval functions or any combination thereof and includes, but is not limited to, communication

36   with, storage of data in or to, or retrieval of data from any device, and the human manual

37   manipulation of electronic magnetic impulses. A "computer operation" for a particular computer

38   shall also mean any function for which that computer was designed.

39   (h) "Computer program" means an ordered set of computer data representing instructions

40   or statements, in a form readable by a computer, which controls, directs, or otherwise influences

41   the functioning of a computer or computer network.

42   (I) "Computer software" means a set of computer programs, procedures, and associated

43   documentation concerned with computer data or with the operation of a computer, computer

44   program, or computer network.

45   (j) "Computer services" means computer access time, computer data processing, or

46   computer data storage and the computer data processed or stored in connection therewith.

47   (k) "Computer supplies" means punch cards, paper tape, magnetic tape, magnetic disks

48   or diskettes, optical disks or diskettes, disk or diskette packs, paper, microfilm, and any other

49   tangible input, output, or storage medium used in connection with a computer, computer network,

50   computer data, computer software, or computer program.

51   (l) "Computer resources" includes, but is not limited to, information retrieval; computer data

52   processing, transmission and storage; and any other functions performed, in whole or in part, by

53   the use of a computer, computer network, computer software, or computer program.

54   "Financial instrument" includes, but is not limited to, any check, draft, warrant, money

55   order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction

56   authorization mechanism, marketable security, or any computerized representation thereof.

57   (m) "Owner" means any person who owns or leases or is a licensee of a computer,

58   computer network, computer data, computer program, computer software, computer resources,

59   or computer supplies.

60   (n) "Person" means any natural person, general partnership, limited partnership, trust,

61   association, corporation, joint venture, or any state, county, or municipal government and any

62   subdivision, branch, department, or agency thereof.

63   (o) "Property" includes:

64   (1) Real property;

65   (2) Computers and computer networks;

66   (3) Financial instruments, computer data, computer programs, computer software, and all

67   other personal property regardless of whether they are:

68   (I) Tangible or intangible;

69   (ii) In a format readable by humans or by a computer;

70   (iii) In transit between computers or within a computer network or between any devices

71   which comprise a computer; or

72   (iv) Located on any paper or in any device on which it is stored by a computer or by a

73   human; and

74   (4) Computer services.

75   "Ransomware" means a computer contaminant, or lock placed or introduced without

76   authorization into a computer, computer system, or computer network that restricts access by an

77   authorized person to the computer, computer system, computer network, or any data therein

78   under circumstances in which the person responsible for the placement or introduction of the

79   ransomware demands payment of money or other consideration to remove the computer

80   contaminant, restore access to the computer, computer system, computer network, or data, or

81   otherwise remediate the impact of the computer contaminant or lock.

82   (p) "Value" means having any potential to provide any direct or indirect gain or advantage

83   to any person.

84   ~~(q) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money~~

85   ~~order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction~~

86   ~~authorization mechanism, marketable security or any computerized representation thereof~~

87   (r) "Value of property or computer services" shall be: (1) The market value of the property

88   or computer services at the time of a violation of this article; or (2) if the property or computer

89   services are unrecoverable, damaged or destroyed as a result of a violation of §61-3C-6 or §61-

90   3C-7 of this code, the cost of reproducing or replacing the property or computer services at the

91   time of the violation.

§61-3C-4. Computer fraud; access to Legislature computer; criminal penalties.

1   (a) Any person who, knowingly and willfully, directly or indirectly, accesses or causes to

2   be accessed any computer, computer services, or computer network for the purpose of (1)

3   executing any scheme or artifice to defraud or (2) obtaining money, property, or services by

4   means of fraudulent pretenses, representations or promises is guilty of a felony and, upon

5   conviction, ~~thereof~~ shall be fined not more than $10,000 or ~~imprisoned in the penitentiary~~ <u>confined</u>

6   <u>in a state correctional facility</u> for not more than 10 years, or both fined and ~~imprisoned~~ <u>confined.</u>

7   <u>(b) (1) A person who, with intent to extort money or other consideration from another,</u>

8   <u>introduces ransomware into any computer, computer system, or computer network is guilty of a</u>

9   <u>felony and, upon conviction, shall be fined not more than $10,000 or confined in a state</u>

10   <u>correctional facility for not more than 10 years, or both fined and confined.</u>

11   <u>(2) Prosecution pursuant to this subsection does not prohibit or limit prosecution under</u>

12   <u>any other law.</u>

13   <u>(3) A person is responsible for placing or introducing ransomware into a computer,</u>

14   <u>computer system, or computer network if the person directly places or introduces the ransomware</u>

15   <u>or directs or induces another person to do so, with the intent of demanding payment or other</u>

16   <u>consideration to remove the ransomware, restore access, or otherwise remediate the impact of</u>

17   <u>the ransomware.</u>

18   ~~(b)~~ <u>(c)</u> (1) Any person who, knowingly and willfully, directly or indirectly, accesses,

19   attempts to access, or causes to be accessed any data stored in a computer owned by the

20   Legislature without authorization is guilty of a felony and, upon conviction, ~~thereof~~ shall be fined

21   not more than $5,000 or ~~imprisoned in the penitentiary~~ <u>confined in a state correctional facility</u> for

22   not more than five years, or both fined and ~~imprisoned~~ <u>confined.</u>

23   (2) Notwithstanding the provisions of §61-3C-17 of this code to the contrary, in any criminal

24   prosecution under this subsection against an employee or member of the Legislature, it shall not

25   be a defense (A) that the defendant had reasonable grounds to believe that he or she had

26   authorization to access the data merely because of his or her employment or membership, or (B)

27   that the defendant could not have reasonably known he or she did not have authorization to

28   access the data: *Provided,* That the Joint Committee on Government and Finance shall

29   promulgate rules for the respective houses of the Legislature regarding appropriate access of

30   members and staff and others to the legislative computer system.

NOTE: The purpose of this bill is to create criminal penalties for introducing ransomware into any computer, computer system, or computer network with the intent to extort money or other consideration. The bill sets forth the elements of the offense. The bill defines a term.

Strike-throughs indicate language that would be stricken from a heading or the present law, and underscoring indicates new language that would be added.