H-4439.1

SUBSTITUTE HOUSE BILL 2678

State of Washington 65th Legislature 2018 Regular Session

By House Public Safety (originally sponsored by Representatives Tarleton, Hudgins, Jinkins, Ortiz-Self, and Irwin)

READ FIRST TIME 02/02/18.

AN ACT Relating to modifying cybercrime provisions; and amending RCW 9A.90.030 and 9A.90.080.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

Sec. 1. RCW 9A.90.030 and 2016 c 164 s 3 are each amended to read as follows:

The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Access" means to gain entry to, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of electronic data, data network, or data system, including via electronic means.

(2) "Cybercrime" includes crimes of this chapter.

(3) "Data" means a digital representation of information, knowledge, facts, concepts, data software, data programs, or instructions that are being prepared or have been prepared in a formalized manner and are intended for use in a data network, data program, data services, or data system.

(4) "Data network" means any system that provides digital communications between one or more data systems or other digital input/output devices including, but not limited to, display terminals, remote systems, mobile devices, and printers.

(5) "Data program" means an ordered set of electronic data representing coded instructions or statements that when executed by a computer causes the device to process electronic data.

(6) "Data services" includes data processing, storage functions, internet services, email services, electronic message services, web site access, internet-based electronic gaming services, and other similar system, network, or internet-based services.

(7) "Data system" means an electronic device or collection of electronic devices, including support devices one or more of which contain data programs, input data, and output data, and that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control. This term does not include calculators that are not programmable and incapable of being used in conjunction with external files.

(8) "Identifying information" means information that, alone or in combination, is linked or linkable to a trusted entity that would be reasonably expected to request or provide credentials to access a targeted data system or network. It includes, but is not limited to, recognizable names, addresses, telephone numbers, logos, HTML links, email addresses, registered domain names, reserved IP addresses, usernames, social media profiles, cryptographic keys, and biometric identifiers.

(9) "Malware" means any set of data instructions that are designed, installed, or used, without authorization and with malicious intent, to disrupt computer operations, monitor computer use, gather information about a person or organization, gather sensitive information, or gain access to private computer systems. "Malware" does not include software that installs security updates, removes malware, or causes unintentional harm due to some deficiency. It includes, but is not limited to, a group of data instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to infect other data programs or data, consume data resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the data, data system, or data network.

(10) "White hat security research" means accessing a data program, service, or system solely for purposes of good faith testing, investigation, identification, and/or correction of a security flaw or vulnerability, where such activity is carried out,

and where the information derived from the activity is used, primarily to promote security or safety.

(11) "Without authorization" means to knowingly circumvent technological access barriers to a data system in order to obtain information without the express or implied permission of the owner, where such technological access measures are specifically designed to exclude or prevent unauthorized individuals from obtaining such information, but does not include white hat security research or circumventing a technological measure that does not effectively control access to a computer. The term "without the express or implied permission" does not include access in violation of a duty, agreement, or contractual obligation, such as an acceptable use policy or terms of service agreement, with an internet service provider, internet web site, or employer. The term "circumvent technological access barriers" may include unauthorized elevation of privileges, such as allowing a normal user to execute code as administrator, or allowing a remote person without any privileges to run code.

Sec. 2. RCW 9A.90.080 and 2016 c 164 s 8 are each amended to read as follows:

(1) A person is guilty of electronic data tampering in the first degree if he or she maliciously and without authorization:

(a)(i) Alters data as it transmits between two data systems over an open or unsecure network; or

(ii) Introduces any malware into any electronic data, data system, or data network; and

(b)(i) Doing so is for the purpose of devising or executing any scheme to defraud, deceive, stalk, or extort, or commit any other crime in violation of a state law not included in this chapter, or of wrongfully controlling, gaining access to, or obtaining money, property, or electronic data; or

(ii) The electronic data, data system, or data network is maintained by a ((~~governmental [government]~~)) government agency.

(2) Electronic data tampering in the first degree is a class C felony.

--- END ---