
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)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

--- END ---