Chapter 9A.90 RCW
WASHINGTON CYBERCRIME ACT

Sections

RCW 9A.90.010 Findings—Intent—2016 c 164. The legislature finds that the rapid pace of technological change and information computerization in the digital age generates a never ending sequence of anxiety inducing reports highlighting how the latest device or innovation is being used to harm consumers. The legislature finds that this generates an ongoing pattern of legislation being proposed to regulate each new technology. The legislature finds that a more systemic approach is needed to better protect consumers and address these rapidly advancing technologies. The legislature finds that the application of traditional criminal enforcement measures that apply long-standing concepts of trespass, fraud, and theft to activities in the electronic frontier has not provided the essential clarity, certainty, and predictability that regulators, entrepreneurs, and innovators need. The legislature finds that an integrated, comprehensive methodology, rather than a piecemeal approach, will provide significant economic development benefits by providing certainty to the innovation community about the actions and activities that are prohibited. Therefore, the legislature intends to create a new chapter of crimes to the criminal code to punish and deter misuse or abuse of technology, rather than the perceived threats of individual technologies. This new chapter of crimes has been developed from an existing and proven system of computer security threat modeling known as the STRIDE system.

The legislature intends to strike a balance between public safety and civil liberties in the digital world, including creating sufficient space for white hat security research and whistleblowers. The state whistleblower and public record laws prevent this act from being used to hide any deleterious actions by government officials under the guise of security. Furthermore, this act is not intended to criminalize activity solely on the basis that it violates any terms of service.

The purpose of the Washington cybercrime act is to provide prosecutors the twenty-first century tools they need to combat twenty-first century crimes. [2016 c 164 § 1.]

RCW 9A.90.020 Short title—2016 c 164. This act may be known and cited as the Washington cybercrime act. [2016 c 164 § 2.]

RCW 9A.90.030 Definitions. 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, website 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) "Electronic tracking device" means an electronic device that permits a person to remotely determine or monitor the position and movement of another person, vehicle, device, or other personal possession. As used in this definition, "electronic device" includes computer code or other digital instructions that once installed on a digital device, allows a person to remotely track the position of that device.

(9) "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, user names, social media profiles, cryptographic keys, and biometric identifiers.

(10) "Malware" means any set of data instructions that are designed, without authorization and with malicious intent, to disrupt computer operations, 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.

(11) "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.

(12) "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 website, 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. [2022 c 231 § 2; 2016 c 164 § 3.]

RCW 9A.90.040 Computer trespass in the first degree. (1) A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another; and

(a) The access is made with the intent to commit another crime in violation of a state law not included in this chapter; or

(b) The violation involves a computer or database maintained by a government agency.

(2) Computer trespass in the first degree is a class C felony. [2016 c 164 § 4.]

RCW 9A.90.050 Computer trespass in the second degree. (1) A person is guilty of computer trespass in the second degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another under circumstances not constituting the offense in the first degree.

(2) Computer trespass in the second degree is a gross misdemeanor. [2016 c 164 § 5.]

RCW 9A.90.060 Electronic data service interference. (1) A person is guilty of electronic data service interference if the person maliciously and without authorization causes the transmission of data, data program, or other electronic command that intentionally interrupts or suspends access to or use of a data network or data service.

(2) Electronic data service interference is a class C felony. [2016 c 164 § 6.]

RCW 9A.90.070 Spoofing. (1) A person is guilty of spoofing if he or she, without authorization, knowingly initiates the

transmission, display, or receipt of the identifying information of another organization or person for the purpose of gaining unauthorized access to electronic data, a data system, or a data network, and with the intent to commit another crime in violation of a state law not included in this chapter.

(2) Spoofing is a gross misdemeanor. [2016 c 164 § 7.]

RCW 9A.90.080 Electronic data tampering in the first degree. (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, 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] agency.

(2) Electronic data tampering in the first degree is a class C felony. [2016 c 164 § 8.]

RCW 9A.90.090 Electronic data tampering in the second degree. (1) A person is guilty of electronic data tampering in the second degree if he or she maliciously and without authorization:

(a) Alters data as it transmits between two data systems over an open or unsecure network under circumstances not constituting the offense in the first degree; or

(b) Introduces any malware into any electronic data, data system, or data network under circumstances not constituting the offense in the first degree.

(2) Electronic data tampering in the second degree is a gross misdemeanor. [2016 c 164 § 9.]

RCW 9A.90.100 Electronic data theft. (1) A person is guilty of electronic data theft if he or she intentionally, without authorization, and without reasonable grounds to believe that he or she has such authorization, obtains any electronic data with the intent to:

(a) Devise or execute any scheme to defraud, deceive, extort, or commit any other crime in violation of a state law not included in this chapter; or

(b) Wrongfully control, gain access to, or obtain money, property, or electronic data.

(2) Electronic data theft is a class C felony. [2016 c 164 § 10.]

RCW 9A.90.110 Commission of other crime. A person who, in the commission of a crime under this chapter, commits any other crime may be punished for that other crime as well as for the crime under this

chapter and may be prosecuted for each crime separately. [2016 c 164 § 11.]

RCW 9A.90.120 Cyber harassment. (1) A person is guilty of cyber harassment if the person, with intent to harass or intimidate any other person, and under circumstances not constituting telephone harassment, makes an electronic communication to that person or a third party and the communication:

(a)(i) Uses any lewd, lascivious, indecent, or obscene words, images, or language, or suggests the commission of any lewd or lascivious act;

(ii) Is made anonymously or repeatedly;

(iii) Contains a threat to inflict bodily injury immediately or in the future on the person threatened or to any other person; or

(iv) Contains a threat to damage, immediately or in the future, the property of the person threatened or of any other person; and

(b) With respect to any offense committed under the circumstances identified in (a)(iii) or (iv) of this subsection:

(i) Would cause a reasonable person, with knowledge of the sender's history, to suffer emotional distress or to fear for the safety of the person threatened; or

(ii) Reasonably caused the threatened person to suffer emotional distress or fear for the threatened person's safety.

(2)(a) Except as provided in (b) of this subsection, cyber harassment is a gross misdemeanor.

(b) A person who commits cyber harassment is guilty of a class C felony if any of the following apply:

(i) The person has previously been convicted in this or any other state of any crime of harassment, as defined in RCW 9A.46.060, of the same victim or members of the victim's family or household or any person specifically named in a no-contact or no-harassment order;

(ii) The person cyber harasses another person under subsection (1)(a)(iii) of this section by threatening to kill the person threatened or any other person;

(iii) The person cyber harasses a criminal justice participant or election official who is performing the participant's official duties or election official's official duties at the time the communication is made;

(iv) The person cyber harasses a criminal justice participant or election official because of an action taken or decision made by the criminal justice participant or election official during the performance of the participant's official duties or election official's official duties; or

(v) The person commits cyber harassment in violation of any protective order protecting the victim.

(3) Any criminal justice participant or election official who is a target for threats or harassment prohibited under subsection (2)(b)(iii) or (iv) of this section, and any family members residing with the participant or election official, shall be eligible for the address confidentiality program created under RCW 40.24.030.

(4) For purposes of this section, a criminal justice participant includes any:

(a) Federal, state, or municipal court judge;

(b) Federal, state, or municipal court staff;

(c) Federal, state, or local law enforcement agency employee;

(d) Federal, state, or local prosecuting attorney or deputy prosecuting attorney;

(e) Staff member of any adult corrections institution or local adult detention facility;

(f) Staff member of any juvenile corrections institution or local juvenile detention facility;

(g) Community corrections officer, probation officer, or parole officer;

(h) Member of the indeterminate sentence review board;

(i) Advocate from a crime victim/witness program; or

(j) Defense attorney.

(5) For the purposes of this section, an election official includes any staff member of the office of the secretary of state or staff member of a county auditor's office, regardless of whether the member is employed on a temporary or part-time basis, whose duties relate to voter registration or the processing of votes as provided in Title 29A RCW.

(6) The penalties provided in this section for cyber harassment do not preclude the victim from seeking any other remedy otherwise available under law.

(7) Any offense committed under this section may be deemed to have been committed either at the place from which the communication was made or at the place where the communication was received.

(8) For purposes of this section, "electronic communication" means the transmission of information by wire, radio, optical cable, electromagnetic, or other similar means. "Electronic communication" includes, but is not limited to, email, internet-based communications, pager service, and electronic text messaging. [2022 c 231 § 1; 2004 c 94 § 1. Formerly RCW 9.61.260.]

Severability—2004 c 94: "If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected." [2004 c 94 § 6.]

Effective dates—2004 c 94: "This act is necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and takes effect immediately [March 24, 2004], except for section 3 of this act, which takes effect July 1, 2004." [2004 c 94 § 7.]