S-3252.2

# SENATE BILL 5628

**State of Washington 67th Legislature 2022 Regular Session**

**By** Senators Dhingra, Frockt, Kuderer, Stanford, Trudeau, Wellman, and C. Wilson

Prefiled 01/03/22. Read first time 01/10/22. Referred to Committee on Law & Justice.

AN ACT Relating to cyber harassment, addressing concerns in the case of Rynearson v. Ferguson, and adding a crime of cyberstalking; amending RCW 9.61.260 and 9A.90.030; adding new sections to chapter 9A.90 RCW; recodifying RCW 9.61.260; and prescribing penalties.

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

**Sec. 1.** RCW 9.61.260 and 2004 c 94 s 1 are each amended to read as follows:

(1) A person is guilty of ((~~cyberstalking~~)) cyber harassment if he or she, with intent to harass((~~,~~)) or intimidate((~~, torment, or embarrass~~)) any other person, and under circumstances not constituting telephone harassment, makes an electronic communication to ((~~such other~~)) that person or a third party and the communication:

(a) ((~~Using~~)) Uses any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act;

(b) ((~~Anonymously~~)) Is made anonymously or repeatedly whether or not conversation occurs; ((~~or~~))

(c) ((~~Threatening to inflict injury on the person or property of the person called or any member of his or her family or household~~)) Contains a threat to inflict bodily injury immediately or in the future on the person threatened or to any other person; or

(d) Contains a threat to damage, immediately or in the future, the property of the person threatened or of any other person.

(2) ((~~Cyberstalking is a gross misdemeanor, except as provided in subsection (3) of this section.~~

~~(3) Cyberstalking is a class C felony if either of the following applies:~~

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

~~(b) The perpetrator engages in the behavior prohibited under subsection (1)(c) of this section by threatening to kill the person threatened or any other person.~~

~~(4)~~)) (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) of this section by threatening to kill the person threatened or any other person;

(iii) The person cyber harasses a criminal justice participant who is performing his or her official duties at the time the threat is made;

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

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

For the purposes of (b)(iii) and (iv) of this subsection, the fear from the threat must be a fear that a reasonable criminal justice participant would have under all the circumstances. Threatening words do not constitute cyber harassment if it is apparent to the criminal justice participant that the person does not have the present and future ability to carry out the threat.

(3) Any criminal justice participant 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 him or her, 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 local law enforcement agency employee;

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

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

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

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

(f) Member of the indeterminate sentence review board;

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

(h) Defense attorney.

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

(6) 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.

((~~(5)~~)) (7) 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, ((~~electronic mail~~)) email, internet-based communications, pager service, and electronic text messaging.

**Sec. 2.** 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, 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. For this section, "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.

((~~(9)~~)) (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.

((~~(10)~~)) (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.

((~~(11)~~)) (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.

NEW SECTION. **Sec. 3.** A new section is added to chapter 9A.90 RCW to read as follows:

(1) A person commits the crime of cyberstalking if, without lawful authority and under circumstances not amounting to a felony attempt of another crime:

(a) He or she knowingly and without consent:

(i) Installs or monitors an electronic tracking device; or

(ii) Causes an electronic tracking device to be installed, placed, or used with the intent to track the location of another person; and

(b) The stalker knows or reasonably should know that knowledge of the installation or monitoring of the tracking device would cause the person stalked reasonable fear, or the stalker has notice that the person does not want to be contacted or monitored by the stalker, or there is a protective order in effect protecting the person being stalked from the cyberstalker.

(2)(a) It is not a defense to the crime of cyberstalking that the stalker was not given actual notice that the person did not want the stalker to contact or monitor the person; and

(b) It is not a defense to the crime of cyberstalking that the stalker did not intend to frighten, intimidate, or harass the person.

(3)(a) Except as provided in (b) of this subsection, a person who cyberstalks another person is guilty of a gross misdemeanor.

(b) A person who cyberstalks another is guilty of a class C felony if any of the following applies:

(i) The stalker has previously been convicted in this state 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 protective order;

(ii) There is a protective order in effect protecting the person being stalked from contact with the cyberstalker;

(iii) The stalker has previously been convicted of a gross misdemeanor or felony stalking offense for stalking another person;

(iv) The stalker was armed with a deadly weapon, as defined in RCW 9.94A.825, while stalking the person;

(v)(A) The stalker's victim is or was a law enforcement officer; judge; juror; attorney; victim advocate; legislator; community corrections' officer; an employee, contract staff person, or volunteer of a correctional agency; court employee, court clerk, or courthouse facilitator; or an employee of the child protective, child welfare, or adult protective services division within the department of social and health services; and

(B) The stalker stalked the victim to retaliate against the victim for an act the victim performed during the course of official duties or to influence the victim's performance of official duties; or

(vi) The stalker's victim is a current, former, or prospective witness in an adjudicative proceeding, and the stalker stalked the victim to retaliate against the victim as a result of the victim's testimony or potential testimony.

(4) The provisions of this section do not apply to the installation, placement, or use of an electronic tracking device by any of the following:

(a) A law enforcement officer, judicial officer, probation or parole officer, or other public employee when any such person is engaged in the lawful performance of official duties and in accordance with state or federal law;

(b) The installation, placement, or use of an electronic tracking device authorized by an order of a state or federal court;

(c) A legal guardian for a disabled adult or a legally authorized individual or organization designated to provide protective services to a disabled adult when the electronic tracking device is installed, placed, or used to track the location of the disabled adult for which the person is a legal guardian or the individual or organization is designated to provide protective services;

(d) A parent or legal guardian of a minor when the electronic tracking device is installed, placed, or used to track the location of that minor unless the parent or legal guardian is subject to a court order that orders the parent or legal guardian not to assault, threaten, harass, follow, or contact that minor;

(e) An employer, school, or other organization, who owns the device on which the tracking device is installed and provides the device to a person for use in connection with his or her involvement with the employer, school, or other organization and the use of the device is limited to recovering lost or stolen items; or

(f) The owner of fleet vehicles, when tracking such vehicles. For the purposes of this section, "fleet vehicle" means any of the following:

(i) One or more motor vehicles owned by a single entity and operated by employees or agents of the entity for business or government purposes;

(ii) Motor vehicles held for lease or rental to the general public; or

(iii) Motor vehicles held for sale, or used as demonstrators, test vehicles, or loaner vehicles, by motor vehicle dealers.

NEW SECTION. **Sec. 4.** RCW 9.61.260 is recodified as a new section in chapter 9A.90 RCW.

**--- END ---**