Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Public Safety Committee

HB 2678

Brief Description: Modifying cybercrime provisions.

Sponsors: Representatives Tarleton, Hudgins, Jinkins, Ortiz-Self and Irwin.

Brief Summary of Bill

- Expands the scope of the crimes of Computer Trespass, Electronic Data Tampering, and Spoofing.

Hearing Date: 1/23/18

Staff: Nate Hickner (786-7291) and Kelly Leonard (786-7147).

Background:

Computer Trespass.
A person commits Computer Trespass in the second degree if the person, without authorization, intentionally gains access to a computer or electronic database of another under circumstances not constituting the offense in the first degree. Computer Trespass in the second degree is a gross misdemeanor.

A person commits Computer Trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another, and:

- the access is made with the intent to commit another crime that is not a cybercrime; or
- the violation involves a computer or database maintained by a government agency.

Computer Trespass in the first degree is a class C felony and a level II offense.

"Computer" is not defined in the act. In previous cases pertaining to Computer Trespass, courts have interpreted the word "computer" to include a cellphone and a telephone company's long-distance switch.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

"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.

Electronic Data Tampering.
A person commits Electronic Data Tampering in the second degree if he or she maliciously and without authorization:

- 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
- introduces any malware into any electronic data, data system, or data network under circumstances not constituting the offense in the first degree.

Electronic Data Tampering in the second degree is a gross misdemeanor.

A person commits Electronic Data Tampering in the first degree if he or she commits acts constituting Electronic Data Tampering in the second degree, and:

- 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 that is not a cybercrime, or of wrongfully controlling, gaining access to, or obtaining money, property, or electronic data; or
- the electronic data, data system, or data network are maintained by a governmental agency.

Electronic Data Tampering in the first degree is a class C felony and a level II offense.

"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.

Spoofing.
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 that is not a cybercrime. Spoofing is a gross misdemeanor.

Summary of Bill:

Computer Trespass.
"Computer" is defined as an electronic device, which performs logical, arithmetic, and memory functions by manipulations of electronic or magnetic impulses and includes all equipment related to the computer in a system or network and includes without limitation, telecommunication, or mobile devices that access a network.

The crimes of Computer Trespass in the first and second degrees are expanded by way of the definition of computer to include unauthorized access to all electronic devices that perform logical, arithmetic, and memory functions and all equipment related to such a device in a system or network.

Computer Trespass in the first degree is also expanded to include a third category of conduct. In addition to current provisions, a person is guilty of Computer Trespass in the first degree when the person, without authorization, intentionally gains access to a computer system or electronic database of another and intentionally causes malware to be present on that computer system or electronic database.

Electronic Data Tampering.
The definition of "malware" is expanded to include, in addition to programs designed for certain improper purposes listed in current law, programs that are used or installed for such improper purposes. Additionally, the list of improper purposes is also expanded. Under current law, malware is a program that, without authorization, disrupts computer operations, gathers sensitive information, or gains access to private computer systems. The bill expands this list to include programs that, without authorization, monitor computer use.

An illustrative example is of malware is created within the definition. Malware includes a software application that enables a user to gather information about a person or organization without their knowledge, which may send such information to a third party with or without the person's consent, or which asserts control over a device without the person's knowledge.

Electronic Data Tampering in the first and second degrees are expanded by way of the definition of malware. A person is guilty of Electronic Data Tampering if the person has maliciously introduced data instructions to a computer, data, or network that are designed, installed or used with the intent to, without authorization, disrupt computer operations, gather sensitive information, gain access to private computer systems, or monitor computer use.

Additionally, the list of conduct that escalates Electronic Data Tampering in the second degree into Electronic Data Tampering in the first degree is expanded. In addition to current provisions, a person is guilty of Electronic Data Tampering in the first degree when the person maliciously introduces malware for the purpose of devising or executing any scheme to stalk or track.

Spoofing.
The crime of Spoofing is expanded. In addition to current provisions, a person is guilty of Spoofing when the person, 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 a person with the intent to commit a crime other than a cybercrime.

Computer Software.
"Computer software" is defined as a sequence of instructions written in any programming language and executed on a computer.

Appropriation: None.

Fiscal Note: Requested on January 19, 2018.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.