# Bill Proposal Summary
# Washington Cybercrime Act
# Rep. Magendanz
# January 2016



The title of the bill is, "AN ACT Relating to cybercrime." The law may be referred to as the "Washington Cybercrime Act."

**Computer Trespass**
The computer trespass provisions (first and second degree) are moved to a new chapter on cybercrime, but the language is left intact.

**Service Interference**
The crime of electronic data service interference is created. A person commits electronic data service interference if the person maliciously and without authorization causes the transmission of data, data program, or other electronic command designed to interrupt or suspend access to or use of a data network or data service. Electronic data service interference is a ranked class C felony with a seriousness level of II.

**Spoofing**
The crime of spoofing is created. A person commits spoofing if he or she, without authorization, knowingly initiates the transmission, display, or receipt, of another person's or fictitious person's electronic data for the purpose of gaining unauthorized access to electronic data, a data system, or data network, and with the intent to commit another crime. Spoofing is a gross misdemeanor.

**Electronic Data Tampering**
The crimes of electronic data tampering in the first and second degrees are created.
A person commits electronic data tampering in the first degree if he or she intentionally, without authorization, and without reasonable grounds to believe that he or she has such authorization, adds, alters, damages, deletes, or destroys any electronic data, data system, or data network, or introduces any contaminant into any electronic data, data system or data network, and:

- Doing so is for the purpose of devising or executing any scheme to defraud, deceive, or extort, or commit any other crime, or of wrongfully controlling, gaining access, 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 ranked class C felony with a seriousness level of II.

A person is guilty of electronic data tampering in the second degree if he or she intentionally, without authorization, and without reasonable grounds to believe that he or she has such authorization, adds, alters, damages, deletes, or destroys any electronic data, data system, or data network under circumstances not constituting the offense in the first degree, or introduces any contaminant 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.

**Electronic Data Theft**
The crime of electronic data theft is created. A person is guilty of electronic data theft in the first degree 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 devise or execute any scheme to defraud, deceive, extort, or commit any other crime, or wrongfully control, gain access, or obtain money, property, or electronic data. Electronic data theft is a ranked class C felony with a seriousness level of II.

**Prosecution of other crimes**
A person who, in the commission of a cybercrime, commits any other crime may be punished for that other crime as well as for the cybercrime and may be prosecuted for each crime separately.

**Definitions**
The following terms are defined: "access;" "cybercrime;" "contaminant;" "data;" "data network;" "data program;" "data services;" and "data system."

"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.

"Cybercrime" includes computer trespass, electronic data interference, spoofing, electronic data tampering, and electronic data theft.

"Contaminant" means any set of data instructions that are designed, with malicious intent, to modify, damage, destroy, record, or transmit information within a data, data system, or data network without the permission of the owner of the data, data system, or data network. They include, but are 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.

"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.

"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 .

"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.

"Data services" includes data processing, storage functions, Internet services, electronic mail services, electronic message services, webpage access, internet based electronic gaming services, and other similar system, network, or internet based services.

"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 definition does not include calculators that are not programmable and incapable of being used in conjunction with external files.