SENATE BILL REPORT
SB 6197

As Reported by Senate Committee On:
Law & Justice, January 25, 2016

Title: An act relating to cybercrime.

Brief Description: Concerning cybercrime.

Sponsors: Senators Miloscia, Roach, Hill and Benton.

Brief History:
Committee Activity: Law & Justice: 1/18/16, 1/25/16 [DP, w/oRec].

SENATE COMMITTEE ON LAW & JUSTICE

Majority Report: Do pass.
Signed by Senators Padden, Chair; O'Ban, Vice Chair; Pearson and Roach.

Minority Report: That it be referred without recommendation.
Signed by Senators Pedersen, Ranking Minority Member; Darneille and Frockt.

Staff: Lindsay Erickson (786-7465)

Background: Cyber Crimes Generally. Cybercrime is a broad term that refers to many different types of high-tech crimes committed through the use of electronic devices, including fraud, scams, theft, extortion, hacking, trespass, identity theft, espionage, terrorism, preying upon the elderly and children, and other crimes. As technology advances, people are storing more information electronically and sharing more information electronically on websites and with businesses, the government, and others. This increased connectivity brings greater risk of theft, fraud, and abuse.

Within the state of Washington, cyber threats are an increasingly unpredictable, dangerous, and proliferating hazard to state, local, and tribal governments, as well as private industry. Local and state governments have reported large, sensitive data breaches, as well as recent cyber heists, some larger than $1,000,000.

Computer Trespass. 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: either the access is made with the intent to commit another crime, or the

---

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.

violation involves a computer or database maintained by a government agency. Computer trespass in the first degree is a ranked Class C felony with a seriousness level of II.

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 offenses in the first degree. Computer trespass in the second degree is a gross misdemeanor.

Criminal Penalties. Class C felonies are punishable by up to five years in a state correctional institution, a fine of up to $10,000, or both confinement and a fine. Gross misdemeanors are punishable by up to 364 days in jail, a fine of up to $5,000, or both jail and a fine.

Summary of Bill: Computer trespass provisions in the first and second degrees and the commission of other crimes are moved to a new chapter on cybercrime in Title 9A RCW.

Electronic Data Service Interference. The crime of electronic data service interference is created. A person is guilty of electronic data service interference if the person maliciously and without authorization causes the transmission of data, data programs, or other electronic commands 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 a 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 the person intentionally, without authorization, and without reasonable grounds to believe that he or she has such authorization, adds, alters, damages, deletes, or destroys an electronic data, data system, or data network; or introduces any contaminant into any electronic data, data system, or data network, and:

- does so 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 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 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 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 to, 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; contaminant; cybercrime; data; data network; data program; data services; and data system.

Appropriation: None.

Fiscal Note: Available.

Committee/Commission/Task Force Created: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony: PRO: This is a bipartisan effort to update the statutes involving cyber security and cyber crime, and this bill attempts to address the behavior behind cyber crime. This sort of criminal activity could be prosecuted more on both the state and federal level. This bill could help to broaden the state's ability to prosecute these activities, and the bill is an improvement over our current statutes. Prosecutors have a concern, however, because this bill seems to carve out a greater role for prosecutors without specifying the new expectation on prosecuting attorneys or discussing additional resources. Retailers and their customers are victims of these crimes, and are concerned about having their data stolen and illegally used.

OTHER: A new draft is available that would address some industry concerns regarding "white hat" activities. Internet service providers are concerned that the bill could inadvertently cause issues when they destroy malware on their own websites and when they deploy necessary security updates. There is also apprehension around the broad definitions in the bill that could impact how providers deploy updates to partners.

Persons Testifying: PRO: Senator Miloscia, prime sponsor; Representative Magendanz, prime sponsor of House companion bill; Mark Johnson, WA Retail Assoc.; Tom McBride, WA Assoc. of Prosecuting Attorneys.

OTHER: Megan Schrader, TechNet.

Persons Signed In To Testify But Not Testifying: No one.