SENATE BILL REPORT
SHB 2678

As of February 19, 2018

Title: An act relating to modifying cybercrime provisions.

Brief Description: Modifying cybercrime provisions.

Sponsors: House Committee on Public Safety (originally sponsored by Representatives Tarleton, Hudgins, Jinkins, Ortiz-Self and Irwin).

Brief History: Passed House: 2/08/18, 97-1.
Committee Activity: Law & Justice: 2/16/18.

Brief Summary of Bill

- Expands the scope of the crime of Electronic Data Tampering.

SENATE COMMITTEE ON LAW & JUSTICE

Staff: Shani Bauer (786-7468)

Background: A person commits Electronic Data Tampering if he or she maliciously and without authorization:
- alters data as it transmits between two data systems over an open or unsecure network; or
- introduces any malware into any electronic data, data system, or data network.

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.

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.

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

Malware means any set of data instructions—such as a computer program—that are designed, without authorization and with malicious intent, for any of the following improper purposes:

- to disrupt computer operations;
- to gather sensitive information; or
- to 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.

Summary of Bill: The definition of malware is expanded to include any set of data instructions designed, installed or used without authorization and with malicious intent for one of the improper purposes outlined in statute. Additional activities that may qualify as an improper purpose include using the data instruction to monitor computer use or to gather information about a person or organization.

In addition to those provisions already in statute, a person will be guilty of Electronic Data Tampering in the first degree if the person commits acts constituting Electronic Data Tampering in the second degree and does so for the purpose of stalking.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: No.

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

Staff Summary of Public Testimony: PRO: In 2015, the Legislature passed extraordinary cybercrime provisions to protect citizens from cybercrimes. However, there are still concerns that laws are not keeping up with the pace of technology. This bill improves on the 2015 legislation. More and more networks allow private information to be exposed to people with malicious intent. We live in a world where personal privacy and security are constantly at risk and the tools criminals have to access that data is unprecedented. This bill expands protection of personal information by broadening tools to target individuals who steal data from the internet.

Persons Testifying: PRO: Representative Gael Tarleton, Prime Sponsor; Mark Johnson, Washington Retail Association.

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