HOUSE BILL REPORT
SHB 2678

As Passed House:
February 8, 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:
Committee Activity:
Public Safety: 1/23/18, 2/1/18 [DPS].
Floor Activity:
Passed House: 2/8/18, 97-1.

Brief Summary of Substitute Bill

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

HOUSE COMMITTEE ON PUBLIC SAFETY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 10 members: Representatives Goodman, Chair; Pellicciotti, Vice Chair; Klippert, Ranking Minority Member; Appleton, Chapman, Griffey, Holy, Orwall, Pettigrew and Van Werven.

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

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.

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.

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 (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 Substitute Bill:

The definition of "malware" is expanded to include data instructions that are, without authorization and with malicious intent, used or installed for the specified improper purposes. The list of improper purposes is expanded to include data instructions that monitor computer use or gather information about a person or organization.

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, without authorization and with malicious intent, to:

- disrupt computer operations;
- monitor computer use;
- gather information about a person or organization;
- gather sensitive information; or
- gain access to private computer systems.

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 alters data as it transmits between two data systems over an open or unsecure network or introduces malware to any electronic data, data system, or data network for the purpose of devising or executing any scheme to stalk.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) There is a gap in Washington law regarding the ability to track, stalk, and potentially commit crimes against individuals who have absolutely no knowledge that they are being tracked and stalked due to the accessibility of their personal data online.

Today, the technologies available to literally any person are akin to the intelligence that was previously only available to government intelligence officials. Information—about background, personal details, health, work records, knowledge of a person's family life, siblings' personal lives—is all available freely to anyone. This extends to imagery in the form of drones, satellites, and Google images, as well as tracking devices that not only pick up words, but can track what is typed into a computer.

All of this data can be manipulated with sophisticated data analysis tools to construct patterns of behavior, maps, and more. Everyone is vulnerable to being tracked or stalked without his or her knowledge. There are a few things that can be done to protect people and help them understand the risks and the ways they can protect themselves and the rest of society if there is malignant intent out there.

This bill represents a tune-up to the Cybercrime Act passed two years ago, and strengthens our laws in a manner that will help retail customers and employees, who are often victims of cybercrime.

(Opposed) None.

Persons Testifying: Representative Tarleton, prime sponsor; and Mark Johnson, Washington Retail Association.

Persons Signed In To Testify But Not Testifying: None.