HOUSE BILL REPORT
HB 2375

As Reported by House Committee On:
Public Safety

Title: An act relating to cybercrime.

Brief Description: Concerning cybercrime.

Sponsors: Representatives Magendanz, Orwall, Smith, Tarleton, MacEwen, Muri, Stanford and Wylie.

Brief History:
Committee Activity:
Public Safety: 1/20/16, 1/29/16 [DPS].

Brief Summary of Substitute Bill

- Creates the crimes of Electronic Data Interference, Electronic Data Theft, Spoofing, and Electronic Data Tampering in the first and second degree.

HOUSE COMMITTEE ON PUBLIC SAFETY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives Goodman, Chair; Orwall, Vice Chair; Klippert, Ranking Minority Member; Hayes, Assistant Ranking Minority Member; Appleton, Griffey, Moscoso, Pettigrew and Wilson.

Staff: Kelly Leonard (786-7147).

Background:

Computer Trespass. The Legislature created the crimes of Computer Trespass in the first and second degree in 1984. A person commits Computer Trespass in the first degree if he or she, 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; or
- the violation involves a computer or database maintained by a government 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.

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

Computer Trespass in the first degree is a class C felony with a seriousness level of II, and Computer Trespass in the second degree is a gross misdemeanor.

Sentencing. Crimes are classified as misdemeanors, gross misdemeanors, or felonies (of which there are class A, B, and C felonies). The classification of a crime generally determines the maximum term of confinement and/or fine for an offense. For each classification, the maximum terms of confinement and maximum fines are as follows:

Classification	*Maximum Confinement*	*Maximum Fine*
Misdemeanor	90 days	$1,000
Gross Misdemeanor	364 days	$5,000
Class C Felony	5 years	$10,000
Class B Felony	10 years	$20,000
Class A Felony	Life	$50,000

When a person is convicted of a felony, the Sentencing Reform Act (SRA) applies and determines a specific range of sentence within the statutory maximum. Under the SRA, sentences for felony offenses are determined by reference to a sentencing grid. The sentencing grid provides a standard range of months for the sentence, based on both the severity, or "seriousness level," of the offense and the convicted person's "offender score," which is based on the offender's criminal history.

Summary of Substitute Bill:

Definitions. The following terms are defined: "access;" "cybercrime;" "data;" "data network;" "data program;" "data services;" "data system;" "malware;" "white hat security research;" and "without authorization." The definition for "computer program" is removed.

Computer Trespass. Computer Trespass in the first degree is modified by specifying that access must be made with the intent to commit another crime that is not a cybercrime.

Electronic Data Interference. The crime of Electronic Data Interference is created. A person commits Electronic Data Interference if the person maliciously and without authorization causes the transmission of data, a data program, or other electronic command that intentionally interrupts or suspends access to or use of a data network or data service. Electronic Data Interference is a ranked class C felony with a seriousness level II.

Electronic Data Theft. The crime of Electronic Data Theft is created. A person commits 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, or obtain money, property, or electronic data. Electronic Data Theft is a ranked class C felony with a seriousness level II.

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 maliciously, without authorization, and without reasonable grounds to believe that he or she has such authorization, alters data as it transmits between two computers over an open network, or introduces any malware 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 that is not a cybercrime, 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.

A person commits Electronic Data Tampering in the second degree if he or she maliciously, without authorization, and without reasonable grounds to believe that he or she has such authorization, alters data as it transmits between two computers over an open 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 first degree is a ranked class C felony with a seriousness level of II, and Electronic Data Tampering in the second degree is a gross misdemeanor.

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

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.

Substitute Bill Compared to Original Bill:

Language is added to the intent section pertaining to white hat security research, whistleblowers, and terms of service. Definitions are added for "malware," "white hat security research," and "without authorization." The definition for "contaminant" is removed.

The substitute bill modifies certain cybercrimes containing an element regarding the intent to commit another crime by limiting those other crimes to those that are not cybercrimes.

The crime of Electronic Data Service Interference created in the bill is modified by specifying that the transmission or electronic command must intentionally interrupt or suspend access (rather than be designed to interrupt or suspend access). The crime of

Spoofing created in the bill is modified by specifying that the act is committed when a person initiates the transmission, display, or receipt of the identifying information of another organization or person (rather than another person or fictitious person's electronic data). The crime of Electronic Data Tampering in the first degree and second degree created in the bill is modified by: changing the mental culpable state standard to maliciously (from intentionally); and specifying that the crimes are committed when someone alters data as it transits between two computers over an open network or when someone introduces malware into any electronic data, data system, or data network (rather than 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).

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony:

(In support) This bill is an important step forward for addressing cybercrime in Washington. Washington has been fighting twenty-first century crimes with twentieth century tools. Most cybercrimes are not achieved through direct access, like traditional computer trespass, and are therefore not addressed in current law. Instead, criminals use phishing schemes and other methods where an unsuspecting person facilitates the criminal activity on their own device. Someone can breach a system for days and months before accessing it to harvest data. There are several examples of data breaches in recent years, including in private industry and government. Furthermore, denial of service attacks wreak havoc on industries. Someone can shut down a major corporation's website at very little cost. This creates an incentive for companies to use these nefarious practices to take out their competition.

Cybercrime costs retailers and other businesses millions of dollars each year, and such activities are extraordinarily disruptive. This bill goes after the activity, not the technology, which is a better approach to addressing cybercrime.

Partners in the industry and legal practitioners have been working to improve this legislation for several months. There are only a few lingering issues, which can be worked out with amendments. This includes language regarding ethical white hat efforts, whistleblowers, definitions, and security updates.

(Opposed) While the intentions behind the legislation are good, the Legislature should be careful to avoid violating First Amendment protected activities or other activities that are not inherently criminal in nature. The state should not criminalize anonymity on the Internet, which is particularly important for victims of abuse. The state should not criminalize or prohibit white hat efforts, which make the Internet safer. The state should not over-

criminalize activities that are already addressed in the criminal code, like fraud. Some of these concerns could possibly be addressed with amendments to the bill.

(Other) The bill should be amended to provide protections for white hat activities and valid security updates.

Persons Testifying: (In support) Representative Magendanz, prime sponsor; and Mark Johnson, Washington Retail Association.

(Opposed) Shankar Narayan, American Civil Liberties of Washington.

(Other) Megan Schrader, TechNet.

Persons Signed In To Testify But Not Testifying: None.