

# Judicial Impact Fiscal Note

<b>Bill Number:</b> 2375 HB	<b>Title:</b> Cybercrime	<b>Agency:</b> 055-Admin Office of the Courts
-----------------------------	--------------------------	---

## Part I: Estimates

**No Fiscal Impact**

**Estimated Cash Receipts to:**

**Non-zero but indeterminate cost. Please see discussion.**

**Estimated Expenditures from:**

**Non-zero but indeterminate cost. Please see discussion.**

*The revenue and expenditure estimates on this page represent the most likely fiscal impact. Responsibility for expenditures may be subject to the provisions of RCW 43.135.060.*

Check applicable boxes and follow corresponding instructions:

- If fiscal impact is greater than \$50,000 per fiscal year in the current biennium or in subsequent biennia, complete entire fiscal note form Parts I-V.
- If fiscal impact is less than \$50,000 per fiscal year in the current biennium or in subsequent biennia, complete this page only (Part I).
- Capital budget impact, complete Part IV.

Legislative Contact Kelly Leonard	Phone: 360-786-7147	Date: 01/18/2016
Agency Preparation: Sam Knutson	Phone: 3607045528	Date: 01/18/2016
Agency Approval: Ramsey Radwan	Phone: 360-357-2406	Date: 01/18/2016
OFM Review:	Phone:	Date:

Request # 2375 HB-1

## **Part II: Narrative Explanation**

**II. A - Brief Description Of What The Measure Does That Has Fiscal Impact on the Courts**

**II. B - Cash Receipts Impact**

**II. C - Expenditures**

## **Part III: Expenditure Detail**

## **Part IV: Capital Budget Impact**

## **Part II: Narrative Explanation**

This bill would establish the Washington Cybercrime Act, and would address the crimes of computer trespass, electronic data service interference, spoofing, electronic data tampering, and electronic data theft.

### **Part II.A – Brief Description of what the Measure does that has fiscal impact on the Courts**

This bill would create a new chapter of RCW 9A, establishing the Washington Cybercrimes Act. The Legislature intends to create a systemic approach to criminal enforcement efforts that address the rapidly advancing changes in computer technology.

If enacted, this bill:

Section 6 would establish the crime of computer trespass in the first degree for a person who is found guilty of intentionally gaining access, without authorization, to the computer system or database of another and the access is made with the (a) intent to commit another crime, or (b) the violation involves a computer or database maintained by a government agency. Computer trespass in the first degree would be defined as a class C felony.

Section 7 would establish the crime of computer trespass in the second degree if a person, 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 second degree would be defined as a gross misdemeanor.

Section 8 would establish the crime of electronic data service interference if a 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 a data network or data service. Electronic data service interference would be defined as a class C felony.

Section 9 would establish the crime of spoofing if a person, 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 would be defined as a gross misdemeanor.

Section 10 would establish the crime of electronic data tampering in the first degree if a person adds, alters, damages, deletes, or destroys electronic data, data system, or data network; 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, extort, or commit any other crime, or wrongfully controlling, gaining access to, or obtaining money, property or electronic data; or the electronic data, data system, or data network is maintained by a government agency. Electronic data tampering in the first degree would be defined as a class C felony.

Section 11 would establish the crime of electronic data tampering in the second degree if a person adds, alters, damages, deletes, or destroys electronic data, data system, or data network; 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, extort, or commit any other crime, or wrongfully controlling, gaining access to, or obtaining money, property or electronic data not constituting the offense in the first degree. Electronic data tampering in the second degree would be defined as a gross misdemeanor.

Section 12 would establish the crime 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: (a) devise or execute any scheme to defraud, deceive, extort, or commit any other crime; or (b) wrongfully control, gain access to, or obtain money, property, or electronic data. Electronic data theft would be defined as a class C felony.

Section 13 would allow for the prosecution of a person for each separate crime committed under this chapter RCW.

Section 14 would repeal the following acts: (1) RCW 9A.52.110 (computer trespass in the first degree); (2) 9A.52.120 (computer trespass in the second degree); (3) RCW 9A.52.130 (computer trespass – commission of other crime).

## **II.B - Cash Receipt Impact**

Indeterminate. The Administrative Office of the Courts (AOC) does not have data to estimate how many of these crimes might be committed.

## **II.C – Expenditures**

Indeterminate.

The AOC does not have data available to estimate the number of cases that may be prosecuted under this proposed bill, thus cannot estimate the number of hearings or trials that would result.

Judges will need education regarding the new cybercrimes and punishments. This would be handled during routine training opportunities.

Changes would be required to the law table and other system tables to repeal current crimes and penalties, and add new crimes and penalties. This would be handled during routine law table maintenance processes.