JUDICIAL IMPACT FISCAL NOTE

Bill Number:	Title:	Agency:
2678 SHB	Cybercrime	055 – Administrative Office of the Courts (AOC)

Part I: Estimates

☐ **No Fiscal Impact**

Estimated Cash Receipts to:

	FY 2018	FY 2019	2017-19	2019-21	2021-23
Total:					

Estimated Expenditures from:

STATE	FY 2018	FY 2019	2017-19	2019-21	2021-23
FTE – Staff Years					
Account					
General Fund – State (001-1)					
State Subtotal					
COUNTY					
County FTE Staff Years					
Account					
Local - Counties					
Counties Subtotal					
CITY					
City FTE Staff Years					
Account					
Local – Cities					
Cities Subtotal					
Local Subtotal					
Total Estimated Expenditures:					

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:	Phone:	Date:
Agency Preparation: Sam Knutson	Phone: 360-704-5528	Date: 2/7/2018
Agency Approval: Ramsey Radwan	Phone: 360-357-2406	Date:
OFM Review:	Phone:	Date:

Part II: Narrative Explanation

This bill would revise the Washington Cybercrimes Act.

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

This bill would expand the definition of "malware" 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: (1) disrupt computer operations; (2) monitor computer use; (3) gather information about a person or organization; (4) gather sensitive information; or (5) 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 would be expanded.

This bill differs from HB 2678:

- Provisions that expand the scope of the crimes of Computer Trespass and Spoofing are removed. Provisions that add or modify definitions of "computer", "access", "computer software", and "data" are removed.
- The purpose of devising or executing any scheme to track is removed from the list of motivations that escalate Electronic Data Tampering in the second degree to Electronic Data Tampering in the first degree.
- The malicious gathering of information about a person or organization is added to the list of improper purposes within the definition of "malware".

II.B - Cash Receipt Impact

None.

II.C – Expenditures

Indeterminate. The AOC does not have data available to estimate the number of trials/hearings that would result from this bill. However, it is assumed it would be minimal.