HOUSE BILL NO. 161

INTRODUCED BY F. NAVE

BY REQUEST OF THE DEPARTMENT OF JUSTICE

A BILL FOR AN ACT ENTITLED: "AN ACT GENERALLY REVISING COMPUTER CRIME LAWS; PROVIDING DEFINITIONS; REVISING THE OFFENSE OF UNLAWFUL USE OF A COMPUTER; PROVIDING EXCEPTIONS; AND AMENDING SECTIONS 45-6-310 AND 45-6-311, MCA."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

Section 1. Section 45-6-310, MCA, is amended to read:

"**45-6-310. ~~Definition~~ Definitions -- computer use.** As used in 45-6-311 and this section, the ~~term~~ following definitions apply:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, computer network, or electronic device.

(2) "Authorization" means a process ensuring that correctly authenticated users can access only those resources for which the owner of the resource has given the users explicit permission.

(3) "Computer" means an electronic device used to create, receive, transmit, store, or process data of any kind, or to run programs stored on hardware or software, and includes any device attached physically or connected intangibly to the computer.

(4) "Computer contaminant" means any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. The term includes but is not limited to a group of computer instructions, commonly called viruses or worms, that are self-replicating or self-propagating and that are designed to contaminate other computer programs or computer data, consume computer resources, modify destroy, record, or transmit data, or in some other fashion usurp or interfere with the normal operation of the computer, computer system, or computer network.

(5) "Computer credential" means:

(a) a password, token code, or other means of limiting access; or

(b) an account, address, username, handle, avatar, or other digital representation of a person.

(6) "Computer network" means a system that provides a medium for communication between one or more computer systems or electronic devices, including communication with an input or output device such as a display terminal, printer, or any other electronic equipment that is connected to the computer systems or electronic devices by physical or wireless technologies.

(7) "Computer system" means a device or collection of devices, including support or peripheral devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including but not limited to logic, arithmetic, data storage, data retrieval, data processing, communication, or control.

(8) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs, or instructions. Data may be in any form, in storage media or stored in the memory of the computer, or in transit or presented on a display device.

(9) "Electronic device" means a device or a portion of a device that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including but not limited to a cellular telephone, tablet, or other portable device designed for and capable of communicating with or across a computer network and that is actually used for that purpose.

(10) "Encrypt" means the use of any process of data encryption including but not limited to cryptography, enciphering, or encoding of data, programs, information, image, signal, sound, computer, computer networks, or other electronic devices.

(11) ~~"obtain~~ "Obtain the use of" means to instruct, communicate with, store data in, retrieve data from, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, or computer network or to cause another to instruct, communicate with, store data in, retrieve data from, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, or computer network.

(12) "Trade secret" has the meaning provided in 30-14-402."

Section 2. Section 45-6-311, MCA, is amended to read:

"**45-6-311. Unlawful use of a computer -- EXCEPTIONS.** (1) ~~A~~ EXCEPT AS PROVIDED IN SUBSECTIONS (3) ~~AND,~~ (4), (5), AND (7), A person commits the offense of unlawful use of a computer ~~if the~~ when ~~a~~ THE person knowingly or purposely and without authorization:

(a) destroys or renders inoperable a computer, computer system, ~~or~~ computer network or any part of a computer system or network with the purpose ~~to make~~ OF MAKING the device or system physically inaccessible or to render the data, programs, or supporting documentation inaccessible or unusable;

~~(a)~~(b) obtains the use or access of any computer, computer system, or computer network without ~~actual~~ consent of the owner;

~~(b) alters or destroys or causes another to alter or destroy a computer program or computer software without consent of the owner; or~~

~~(c) obtains the use of or alters or destroys a computer, computer system, computer network, or any part thereof as part of a deception for the purpose of obtaining money, property, or computer services from the owner of the computer, computer system, computer network, or part thereof or from any other person.~~

(c) introduces a computer contaminant that deletes, modifies, or renders unavailable data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, computer network, or electronic device;

(d) destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, computer network, or electronic device;

(e) discloses or takes data, programs, or supporting documentation that is a trade secret, confidential, or otherwise protected as provided by law or is data that materially compromises the security, confidentiality, or integrity of personal information as defined in 30-14-1704 residing or existing internal or external to a computer, computer system, computer network, or electronic device;

(f) introduces a computer contaminant to gain access to data, programs, supporting documentation, computer systems, including peripheral devices, or computer networks to delete, encrypt, modify, append, or otherwise render unavailable data, programs, supporting documentation, computer systems, including peripheral devices, computer networks, or electronic devices owned or operated by a governmental or private entity or person;

(g) uses or changes in any way another person's computer credentials without the person's permission; or

(h) uses another person's computer or computer credentials to track that person's movements or monitor that person's communications without that person's consent.

(2) A person convicted of the offense of unlawful use of a computer involving loss of property not exceeding $1,500 in value OR WHEN NO LOSS CAN BE ARTICULATED shall be fined not to exceed $1,500 or be imprisoned in the county jail for a term not to exceed 6 months, or both. A person convicted of the offense of unlawful use of a computer involving loss of property exceeding $1,500 in value shall be fined not more than 2 1/2 times the value of the property used, altered, destroyed, or obtained or be imprisoned in the state prison for a term not to exceed 10 years, or both.

(3) A PERSON IS NOT IN VIOLATION OF THIS SECTION IF THE PERSON ENCRYPTS OR MODIFIES ANOTHER PERSON'S COMPUTER, COMPUTER SYSTEM, ELECTRONIC DEVICE, OR COMPUTER CREDENTIALS WITHOUT PERMISSION OR CONSENT FOR THE PURPOSES OF~~:~~

~~(A) RESPONDING TO A NONPAYMENT OR A VIOLATION OF THE TERMS OF A LEGAL CONTRACT BETWEEN THE PERSONS;~~

~~(B)~~(A) COMPLYING WITH A COURT ORDER OR A WARRANT FROM FEDERAL, STATE, OR LOCAL LAW ENFORCEMENT~~;~~ ~~OR~~.

~~(C)~~(B) ~~USING~~ ~~SECURITY, FRAUD PREVENTION, OR~~ ~~OTHER~~ ~~TOOLS DESIGNED TO ENSURE THE INTEGRITY OF COMMUNICATIONS FROM THE USER TO OTHER AUTHORIZED SYSTEMS.~~

(4) THIS SECTION DOES NOT APPLY TO AN INDIVIDUAL WHO MODIFIES, ACCESSES, OR DESTROYS THE INDIVIDUAL'S PERSONAL COMPUTER, COMPUTER NETWORK, COMPUTER SYSTEM, OR ELECTRONIC DEVICE.

(5) A PERSON MAY NOT:

(A) ENCRYPT OR MODIFY ANOTHER PERSON'S COMPUTER, COMPUTER SYSTEM, OR ELECTRONIC DEVICE;

(B) RESTRICT ACCESS TO PERSONAL DATA BY ANY MEANS; OR

(C) RESTRICT ACCESS TO A PRODUCT OR SERVICE BECAUSE THE CONSUMER DID NOT AUTHORIZE THE USE OR COLLECTION OF DATA.

(6) EXCEPT AS PROVIDED IN SUBSECTION (5) AND (7), A PERSON MAY ENFORCE THE TERMS OF A LEGAL CONTRACT BETWEEN THE PERSONS.

(7) A PERSON MAY ONLY ENFORCE NONPAYMENT UNDER THE TERMS OF A LEGAL CONTRACT CONCERNING DIGITAL SOFTWARE THROUGH MODIFICATION OF CREDENTIALS."

- END -