OHIO LEGISLATIVE SERVICE COMMISSION

www.lsc.ohio.gov

Office of Research and Drafting

Legislative Budget Office

H.B. 368
133rd General Assembly

Bill Analysis

Click here for H.B. 368's Fiscal Note

Version: As Reported by Senate Judiciary

Primary Sponsor: Rep. Baldridge

Carla Napolitano, Attorney

SUMMARY

- Creates the crime of electronic computer service interference that prohibits a person from knowingly, and without authorization, gaining access to, attempting to gain access to, or permitting access to be gained to a computer, computer system, or computer network.
- Creates the crimes of electronic data tampering and electronic data manipulation that prohibit a person from knowingly and without authorization altering, or attempting to alter, data as it travels between two computer systems or introducing malware into any electronic data or computer system under certain circumstances.
- Creates the crime of computer trespass that prohibits a person from knowingly and without authorization gaining access, attempting to gain access, or causing access to be gained to a computer, computer system, or computer network without authorization and increases penalties under certain circumstances.
- Creates the crime of electronic data theft that prohibits a person from knowingly and without authorization obtaining, or attempting to obtain, electronic data without authorization and with the intent to either (1) revise or execute any scheme to defraud, deceive, extort, or commit any crime or (2) wrongfully control or obtain property or wrongfully gain access to electronic data.
- Creates the crime of unauthorized data disclosure that prohibits a person from knowingly and without authorization doing or attempting to do either of the following:
  - Making or causing to be made an unauthorized use, disclosure, or copy of data residing in, communicated by, or produced by a computer system;
  - Without authorization, disclosing a password, personal identification number, or other confidential information used as a means of access to a computer system or computer service.

- Revises the existing offenses of criminal mischief and unauthorized use of computer, cable, or telecommunications property to limit overlap with the new offenses.
- Excludes from the bill's prohibitions actions by a person within the scope of the person's lawful employment when the person performs acts that are reasonably necessary to the performance of the person's work assignments or duties, even if the person mistakenly goes beyond the scope of the person's lawful employment.
- Allows a person affected by the commission of any of the above crimes to bring a civil action within two years of the violation or discovery of the damage, whichever is later.

DETAILED ANALYSIS

Overview

Existing law contains two offenses to cover computer-related crimes: (1) criminal mischief and (2) unauthorized use of a computer.[1] The bill partially revises these offenses and adds several new felony-level, computer-related offenses, including electronic data tampering and electronic data manipulation, electronic computer service interference, computer trespass, electronic data theft, and unauthorized data disclosure. The bill also allows victims of cybercrime to file a civil lawsuit against a person who violates the bill's provisions. Lastly, the bill protects a person acting within the scope of the person's lawful employment, such that a person does not commit an offense under the bill when the person performs acts that are reasonably necessary to the performance of the person's work assignments or duties, even if the person mistakenly goes beyond the scope of the person's lawful employment.[2]

Criminal mischief and computer service interference and tampering

Criminal mischief – eliminated as it applies to computers

Under existing law, the offense of criminal mischief prohibits a person, without privilege to do so, from knowingly impairing the functioning of a computer, computer system, computer network, computer software, or computer program. The penalty for criminal mischief ranges from a first degree misdemeanor to a fourth degree felony depending on the value of the property involved and whether the property involved was an aircraft. The bill eliminates this manner of committing criminal mischief.[3]

Electronic computer service interference – new

Under the bill, a person is prohibited from knowingly, and without authorization, causing or attempting to cause the transmission of data, a computer program, or an electronic

[1] R.C. 2909.07(A)(6) and 2913.04(B).

[2] R.C. 2913.93 and 2913.94.

[3] R.C. 2909.07(A)(6) and (C).

command that interrupts or suspends access to or use of a computer network or computer service without authorization and with the intent to impair the functioning of a computer network or computer service. A person who violates this provision is guilty of electronic computer service interference, a fourth degree felony.[4]

As used in the bill, **computer services** includes data processing, storage functions, internet services, email services, electronic message services, website access, internet-based electronic gaming services, and other similar computer system, computer network, and internet-based services.[5]

Electronic data tampering and electronic data manipulation – new

A person may not knowingly, and without authorization, alter or attempt to alter data as it travels between two computer systems over an open or unsecure network or introduce or attempt to introduce malware into any electronic data, computer, computer system, or computer network. A person who violates this provision is guilty of electronic data manipulation, a fourth degree felony. A person is guilty of electronic data tampering, a third degree felony, when, in addition to the above, any of the following applies:

- The person intended to devise or execute a scheme to defraud, deceive, or extort.
- The person intended to commit any other crime in violation of a state law.
- The person intended to wrongfully control or obtain property or wrongfully gain access to electronic data.
- The electronic data, computer, computer system, or computer network is maintained by the state or a political subdivision.

As used in the bill, **malware** means a set of computer instructions that is designed or used to do any of the following to a computer, computer system, or computer network without the authorization of the owner or other person authorized to give consent:

- Modify, damage, destroy, disable, deny, or degrade access to it;
- Gain access to it;
- Functionally impair it;
- Record or transmit information within it.[6]

[4] R.C. 2913.88.

[5] R.C. 2923.86(A).

[6] R.C. 2913.86(C), 2913.89, and 2913.90.

Unauthorized access, data theft, and unauthorized disclosure

Unauthorized computer use – eliminated in part

The current offense of unauthorized use of computer, cable, or telecommunications property (unauthorized computer use) prohibits, among other things, unauthorized access to another's computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service. The penalty for violating this prohibition ranges from a fifth degree felony to a second degree felony, depending on the value of the loss to the victim, whether the access was used to commit another offense, and whether the victim is an elderly person or disabled adult.[7]

The bill limits this existing prohibition to a cable service, cable system, telecommunications device, telecommunications service, or information service and enacts a number of new prohibitions that encompass unauthorized computer use and other computer-related activities. Continuing law, unchanged by the bill, continues to prohibit a person from knowingly using or operating the property of another without consent.[8] It appears possible that to some extent the continuing prohibitions might duplicate the newly enacted offenses. But, the bill provides that a person cannot be convicted of violating both unauthorized computer use and the new offense of computer trespass for the same underlying action.[9]

Computer trespass – new

The bill prohibits a person from knowingly and without authorization gaining access to, attempting to gain access to, or causing access to be gained to a computer, computer system, or computer network. A person who violates this provision is guilty of computer trespass, a fifth degree felony.[10]

A person who commits computer trespass is guilty of a fourth degree felony when either of the following applies:

- The violation is with the intent to commit a crime in violation of state law.
- The computer, computer system, or computer network is maintained by the state or a political subdivision.[11]

If the computer, computer system, or computer network involved in a violation is used or intended to be used in the operation of an aircraft, and the violation creates a substantial risk of physical harm to any person or the aircraft in question is an occupied aircraft, then the

[7] R.C. 2913.04(B) and (G).

[8] R.C. 2913.04(A).

[9] R.C. 2913.04(K).

[10] R.C. 2913.87(B), (C)(1), and (C)(2)(b).

[11] R.C. 2913.87(A), (C)(1), and (C)(2)(a).

violation is a third degree felony (under existing law, this penalty relates to criminal mischief, see "**Criminal mischief**," above).[12]

Except as provided in the subsequent paragraph, if a person commits computer trespass for the purpose of doing any of the following, and the value of the property or services involved or the loss to the victim is $150,000 or more, then the violation is a felony of the third degree:

- Devising or executing a scheme to defraud or to obtain property or services;
- Obtaining money, property, or services by false or fraudulent pretenses;
- Committing any other criminal offense.[13]

Lastly, if the offender acted recklessly with regard to the status of the victim as an elderly person or disabled adult, and the value of the property or services or loss to the victim is $7,500 or more and less than $37,500, the violation is a third degree felony. If the value is $37,500 or more, the violation is a second degree felony.[14]

A person commits a separate violation with regard to each computer trespass.[15]

Electronic data theft – new

The bill prohibits a person from knowingly and without authorization obtaining, or attempting to obtain electronic data without authorization and with the intent to do either of the following:

- Devise or execute any scheme to defraud, deceive, extort, or commit any crime in violation of state law;
- Wrongfully control or obtain property or wrongfully gain access to electronic data.

A person who violates these provisions is guilty of electronic data theft, a third degree felony.[16]

Unauthorized data disclosure – new

Under the bill, a person may not knowingly and without authorization do or attempt to do either of the following:

- Make or cause to be made a display, use, disclosure, or copy of data residing in, communicated by, or produced by a computer, computer system, or computer network;

[12] R.C. 2913.04 and 2913.87(C)(3).

[13] R.C. 2913.87(C)(4).

[14] R.C. 2913.87(C)(5).

[15] R.C. 2913.87(D).

[16] R.C. 2913.91.

- Disclose a password, identifying code, personal identification number, or other confidential information that is used as a means of access to a computer, computer system, computer network, or computer service.

A violation of these provisions constitutes unauthorized data disclosure, a third degree felony.[17]

Scope of employment

The bill's new computer crimes are not to be construed to prohibit actions by a person within the scope of that person's lawful employment. A person acts within the scope of the person's lawful employment when the person performs acts that are reasonably necessary to the performance of the person's work assignments or duties. A person does not violate the new computer crimes by mistakenly going beyond the scope of the person's lawful employment.[18]

Civil action

In addition to any other civil remedy available, the bill allows the owner or lessee of any electronic data, computer, computer system, or computer network who suffers damage or loss because of a violation of any of the above provisions to sue the person who committed the violation for compensatory damages and injunctive or other equitable relief. The bill specifies that a victim of cybercrime is entitled to the civil action regardless of whether there has been a criminal conviction relating to the violation. Compensatory damages must include any cost reasonably and necessarily incurred by the owner or lessee to verify that the electronic data, computer, computer system, or computer network, was not altered, damaged, or deleted by the violation. In any such lawsuit, the court may award reasonable attorney's fees to the owner or lessee that suffered a loss. An owner must bring such a lawsuit within two years of the date of the violation or discovery of the damage, whichever is later.[19]

Conforming changes

As noted above, the existing offense of criminal mischief as it relates to computer systems overlaps elements of electronic computer service interference, electronic data tampering, and electronic data manipulation. To a lesser extent, it overlaps the offenses of computer trespass, electronic data theft, and unauthorized data disclosure.

Similarly, the existing offense of unauthorized use of computer, cable, or telecommunications property (unauthorized computer use) most closely parallels the new offense of computer trespass, but it also overlaps elements of the new offenses of electronic data theft and unauthorized data disclosure. To a lesser extent, it also overlaps the new offenses of electronic computer service interference, electronic data tampering, and electronic data manipulation.

---

[17] R.C. 2913.92.

[18] R.C. 2913.94.

[19] R.C. 2913.93 and 2307.60, not in the bill.

The bill makes a number of conforming changes throughout the Revised Code adding or replacing the reference to these existing offenses with reference to one or more of the bill's new offenses. The following table describes these changes.

R.C. section	Topic	Current reference	Reference under the bill
Investigation of crimes			
R.C. 109.88	Allows the Attorney General to investigate alleged violations of specified offenses for reasonable cause.	Includes unauthorized computer use as a specified offense.	Adds electronic computer service interference, electronic data tampering, electronic data manipulation, computer trespass, electronic data theft, and unauthorized data disclosure.
R.C. 2921.22	Requires a person who knows of a violation of specified offenses to report the violation to law enforcement.	Includes unauthorized computer use as a specified offense.	Adds computer trespass.
R.C. 2933.51	Designates offenses for which law enforcement may obtain an interception warrant to surveil persons.	Includes unauthorized computer use as a designated offense.	Adds electronic computer service interference, electronic data tampering, electronic data manipulation, computer trespass, electronic data theft, and unauthorized data disclosure.
Elements of crimes			
R.C. 901.511	Prohibits the commission of both unauthorized computer use and criminal mischief with the intent to intimidate or coerce a civilian population or government or interfere with agricultural activities.	n/a	Adds electronic computer service interference, electronic data tampering, electronic data manipulation, computer trespass, electronic data theft, and unauthorized data disclosure.
R.C. 2913.01	Definition of "theft offense."	Includes unauthorized computer use.	Adds electronic computer service interference, electronic data tampering, electronic data manipulation, computer

R.C. section	Topic	Current reference	Reference under the bill
			trespass, electronic data theft, and unauthorized data disclosure.
R.C. 2927.12	Prohibits the commission of specified offenses by reason of the victim's race, color, religion, or national origin.	Includes criminal mischief as a specified offense.	Adds electronic computer service interference.
Enhancement of penalties			
R.C. 2913.05	Allows a court, in determining the degree of offense for telecommunications fraud, to aggregate the value of the benefit obtained in that violation with the benefit obtain for violations of other specified offenses.	Includes unauthorized computer use as a specified offense.	Adds electronic computer service interference, electronic data tampering, electronic data manipulation, computer trespass, electronic data theft, and unauthorized data disclosure.
R.C. 2913.49	Allows a court, in determining the degree of offense for identity theft, to aggregate the value of violations of other specified offenses.	Includes unauthorized computer use as a specified offense.	Adds electronic computer service interference, electronic data tampering, electronic data manipulation, computer trespass, electronic data theft, and unauthorized data disclosure.
Domestic violence			
R.C. 109.42	Requires the Attorney General to publish a pamphlet that explains the rights of a victim of specified offenses who is a family or household member of the offender to seek the issuance of a temporary protection order.	Includes criminal mischief as a specified offense.	Adds electronic computer service interference.

R.C. section	Topic	Current reference	Reference under the bill
R.C. 2919.25	Enhances the penalty for a person who commits domestic violence if the offender also had previously been convicted of specified offenses and the victim was a family or household member at the time of the violation.	Includes having been convicted of criminal mischief as a specified offense.	Adds electronic computer service interference.
R.C. 2919.251	Requires a person charged with an offense of violence against a family or household member to appear at a bail hearing if that person also had been previously convicted of committing specified offenses against a family or household member.	Includes criminal mischief as a specified offense.	Adds electronic computer service interference.
R.C. 2919.26	Allows, in the case of a complaint alleging the commission of specified offenses against a family or household member, a person to request a temporary protection order against the alleged offender.	Includes criminal mischief as a specified offense.	Adds electronic computer service interference, electronic data tampering, and electronic data manipulation.
Employment – criminal records checks			
R.C. 109.572 (A)(2), (3), (5), and (12)	Requires the Bureau of Criminal Identification and Investigation to conduct a criminal records check upon request in regard to occupational license applicants and certain prospective employees.	Requires a search for records relating to unauthorized computer use.	Expands to also require a search for records relating to electronic computer service interference, electronic data tampering, electronic data manipulation, computer trespass, electronic data theft, and unauthorized data disclosure.

R.C. section	Topic	Current reference	Reference under the bill
R.C. 3712.09 and 109.572(A)(2)	Prohibits a hospice care or pediatric respite care program from employing a person to provide direct care to patients if that person was convicted of specified offenses.	Includes unauthorized computer use as a specified offense.	Adds electronic computer service interference, electronic data tampering, electronic data manipulation, computer trespass, electronic data theft, and unauthorized data disclosure.
R.C. 3721.121 and 109.572(A)(2)	Prohibits a home or adult day-care program from employing a person to provide direct care to an older adult if that person was convicted of specified offenses.	Includes unauthorized computer use as a specified offense.	Adds electronic computer service interference, electronic data tampering, electronic data manipulation, computer trespass, electronic data theft, and unauthorized data disclosure.
Employment – authority and obligations			
R.C. 2137.14	Provides that a fiduciary with access to the digital assets of a decedent, ward, principal, or settlor is an authorized user for purposes of specified computer-related laws.	Includes unauthorized computer use as a specified law.	Replaces the reference to unauthorized computer use with a reference to computer trespass.
R.C. 2923.129	Provides that a person who violates the prohibition on releasing confidential information obtained through the Law Enforcement Automated Data System (LEADS) is guilty of unauthorized computer use and may be civilly liable.	n/a	Expands to also apply to computer trespass, electronic data theft, and unauthorized data disclosure.
R.C. 3750.09	Provides that a person who violates the prohibition on releasing confidential business information obtained as part of the person's role with the State Emergency Response	n/a	Expands to also apply to computer trespass, electronic data theft, and unauthorized data disclosure.

R.C. section	Topic	Current reference	Reference under the bill
	Commission is not also guilty of unauthorized computer use.		
R.C. 3751.04	Provides that a person who violates the prohibition on releasing confidential business information obtained under the Emergency Planning and Community Right-to-Know Act is not also guilty of unauthorized computer use.	n/a	Expands to also apply to computer trespass, electronic data theft, and unauthorized data disclosure.
R.C. 5503.101	Provides that, notwithstanding the unauthorized computer use law, a prosecutor or person assisting a prosecutor in providing discovery will not be held liable for disclosing information obtained from LEADS so long as the information was lawfully obtained.	n/a	Expands to also notwithstand computer trespass, electronic data theft, and unauthorized data disclosure.

HISTORY

Action	Date
Introduced	10-16-19
Reported, H. Criminal Justice	02-20-20
Passed House (93-1)	05-13-20
Reported, S. Judiciary	12-02-20

H0368-RS-133/ar