



www.lsc.ohio.gov

OHIO LEGISLATIVE SERVICE COMMISSION

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 House Criminal Justice

Primary Sponsor: Rep. Baldridge

Yosef Schiff, Attorney

SUMMARY

- 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.

- Allows a person affected by the commission of any of the above crimes to bring a civil action against the convicted person within two years of the violation or discovery of the damage, whichever is later.

DETAILED ANALYSIS

Overview

Current law contains two main prohibitions of certain computer-related activities: (1) the offense of criminal mischief, which, among other things, prohibits impairing the functioning of a computer, computer system, computer network, computer software, or computer program, and (2) the offense of unauthorized use of computer, cable, or telecommunications property, which prohibits, among other things, unauthorized access to another's computer, computer system, computer network, or information service.¹ The bill revises and relocates these existing prohibitions and adds a number of new prohibitions that encompass other types of computer-related activities. It also provides for civil remedies to persons harmed by any violations.

Criminal mischief and computer service interference and tampering

Criminal mischief – eliminated as it applies to computers

The existing offense of criminal mischief prohibits a person from 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.²

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 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.³

As used in the bill, **computer services** includes data processing, storage functions, internet services, email services, electronic message services, website access, internet-based

¹ R.C. 2909.07(A)(6) and 2913.04(B).

² R.C. 2909.07(A)(6) and (C).

³ R.C. 2913.88.

electronic gaming services, and other similar computer system, computer network, and internet-based services.⁴

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.⁵

Unauthorized access, data theft, and unauthorized disclosure

Unauthorized use of computer property – eliminated in part

The current offense of unauthorized use of computer, cable, or telecommunications property 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.⁶

⁴ R.C. 2923.86(A).

⁵ R.C. 2913.86(C), 2913.89, and 2913.90.

⁶ R.C. 2913.04(B) and (G).

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 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.⁷ It appears possible that to some extent the continuing prohibitions might duplicate the newly enacted offenses.

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.⁸

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.⁹

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 violation is a third degree felony (under existing law, this penalty relates to criminal mischief, see “**Criminal mischief**,” above).¹⁰

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.¹¹

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 R.C. 2913.04(A).

⁸ R.C. 2913.87(B), (C)(1), and (C)(2)(b).

⁹ R.C. 2913.87(A), (C)(1), and (C)(2)(a).

¹⁰ R.C. 2913.04 and 2913.87(C)(3).

¹¹ R.C. 2913.87(C)(4).

\$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.¹²

A person commits a separate violation with regard to each computer trespass.¹³

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.¹⁴

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 an unauthorized display, use, disclosure, or copy of data residing in, communicated by, or produced by a computer, computer system, or computer network;
- 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 without authorization.

A violation of these provisions constitutes unauthorized data disclosure, a third degree felony.¹⁵

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.¹⁶

¹² R.C. 2913.87(C)(5).

¹³ R.C. 2913.87(D).

¹⁴ R.C. 2913.91.

¹⁵ R.C. 2913.92.

¹⁶ R.C. 2913.94.

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 convicted of the violation for compensatory damages and injunctive or other equitable relief. 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. An owner must bring such a lawsuit within two years of the date of the violation or discovery of the damage, whichever is later.¹⁷

Conforming changes

Criminal mischief

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.

In the following provisions, where existing law refers to the offense of criminal mischief, the bill adds reference to electronic computer service interference:

- R.C. 109.42, which requires the Attorney General to publish a pamphlet that explains the rights of a victim of a number of offenses, including criminal mischief.
- R.C. 2919.25, which provides for a mandatory prison term for a person who commits domestic violence if that person also meets other conditions including having been convicted of or having pled guilty to criminal mischief.
- R.C. 2919.251, which requires a person charged with domestic violence to appear in court for the setting of bail if that person was also previously convicted of or pleaded guilty to committing criminal mischief against a family or household member.
- R.C. 2927.12, which prohibits the commission of certain offenses, including criminal mischief, by reason of the race, color, religion, or national origin of the victim. A violation of R.C. 2927.12 raises the penalty of the underlying offense by one degree.

In addition, R.C. 2919.26 allows a person, in the case of a complaint alleging the commission of criminal mischief against a family or household member, to request a temporary protection order against the alleged offender. The bill retains the reference to criminal mischief and adds reference to electronic computer service interference, electronic data tampering, and electronic data manipulation.

¹⁷ R.C. 2913.93.

Computer, cable, or telecommunications property

The existing offense of unauthorized use of computer, cable, or telecommunications property 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.

In R.C. 2137.14, which provides that a fiduciary with access to the digital assets of a decedent, ward, principal, or settlor is an authorized user for purposes of applicable computer-related laws, including unauthorized use of computer, cable, or telecommunications property, the bill replaces the reference to unauthorized access with a reference to computer trespass.

In R.C. 2921.22, which requires a person who knows of a violation of unauthorized use of computer, cable, or telecommunications property to report the violation to law enforcement, the bill retains the reference to unauthorized use and adds a reference to computer trespass.

In the following provisions, where existing law refers to the offense of unauthorized use of computer, cable, or telecommunications property, the bill adds reference to computer trespass, electronic data theft, and unauthorized data disclosure:

- R.C. 2923.129, which 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 use of computer, cable, or telecommunications property;
- R.C. 3750.09, which provides that a person who violates the prohibition on releasing trade secrets or other confidential business information obtained as part of the person's role with the State Emergency Response Commission is not also guilty of unauthorized use of computer, cable, or telecommunications property;
- R.C. 3751.04, which provides that a person who violates the prohibition on releasing trade secrets or other confidential business information obtained under the Emergency Planning and Community Right-to-Know Act is not also guilty of unauthorized use of computer, cable, or telecommunications property;
- R.C. 5503.101, which provides that, notwithstanding the unauthorized 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.

In the following provisions, where existing law refers to the offense of unauthorized use of computer, cable, or telecommunications property, the bill adds reference to all of the new offenses created by the bill:

- R.C. 109.572, which 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;

- R.C. 109.88, which allows the Attorney General to investigate an alleged violation of the prohibition on unauthorized use of computer, cable, or telecommunications property for reasonable cause;
- R.C. 2913.01, which defines “theft offense” to include a violation of the prohibition on unauthorized use of computer, cable, or telecommunications property;
- R.C. 2913.05, which allows a court to aggregate the value of a violation of the prohibition against telecommunications fraud with violations of other laws, including the unauthorized use law, in determining the degree of offense;
- R.C. 2913.49, which allows a court to aggregate the value of a violation of the prohibitions against identity fraud with violations of other laws, including the unauthorized use law, in determining the degree of offense;
- R.C. 2933.51, which includes unauthorized use of computer, cable, or telecommunications property as a “designated offense” for which law enforcement may obtain an interception warrant to surveil persons;
- R.C. 3712.09, which 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 or pleaded guilty to certain crimes including unauthorized use of computer, cable, or telecommunications property;
- R.C. 3721.121, which 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 or pleaded guilty to certain crimes including unauthorized use of computer, cable, or telecommunications property.

Both criminal mischief and unauthorized use of computer, cable, or telecommunications property

R.C. 901.511 prohibits the commission of both unauthorized use and criminal mischief with the intent to intimidate or coerce a civilian population or government or interfere with agricultural activities. The bill retains the references to these offenses and adds reference to all of the new offenses created by the bill.

HISTORY

Action	Date
Introduced	10-16-19
Reported, H. Criminal Justice	02-20-20
