CHAPTER 18

COMPUTER CRIMES

§431. Definitions

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings. [PL 1989, c. 620 (NEW).]

1. "Access" means to gain logical entry into, instruct, communicate with, store data in or retrieve data from any computer resource.
[PL 1989, c. 620 (NEW).]

2. "Computer" means an electronic, magnetic, optical, electrochemical or other high-speed data processing device performing logical, arithmetic or storage functions and includes any data storage device or communications facility directly related to or operating in conjunction with the device.
[PL 2013, c. 297, §1 (AMD).]

3. "Computer information" means a representation of information, knowledge, facts, concepts or instructions that are confidential or proprietary, are being prepared or have been prepared from an organized set of data and are located in computer memory or on magnetic, optical or mechanical media transferable directly to or useable directly by a computer as a source of data or instructions.
[PL 1989, c. 620 (NEW).]

4. "Computer network" means a combination of one or more computers and communication facilities with the capability to transmit information among the devices or computers.
[PL 1989, c. 620 (NEW).]

5. "Computer program" means an ordered set of data representing coded instructions or statements that, when executed by a computer, cause the computer to process data.
[PL 1989, c. 620 (NEW).]

6. "Computer software" means a set of computer programs, procedures and associated documentation used in the operation of a computer system.
[PL 1989, c. 620 (NEW).]

7. "Computer system" means any combination of a computer or computers with the documentation, computer software or physical facilities supporting the computer.
[PL 1989, c. 620 (NEW).]

8. "Computer resource" means a computer program, computer software, computer system, computer network, computer information or any combination thereof.
[PL 1989, c. 620 (NEW).]

9. "Computer virus" means any computer instruction, information, data or program that degrades the performance of a computer resource; disables, damages or destroys a computer resource; or attaches itself to another computer resource and executes when the host computer program, data or instruction is executed or when some other event takes place in the host computer resource, data or instruction.
[PL 1989, c. 620 (NEW).]

9-A. "Criminal justice agency" means a governmental agency of the State or any subunit of a governmental agency of the State at any governmental level that performs the administration of criminal justice pursuant to statute. "Criminal justice agency" includes the Department of the Attorney General and district attorneys' offices. As used in this subsection, "administration of criminal justice" means activities relating to the investigation of all or specific crimes and the prosecution of offenders.
[PL 2013, c. 519, §7 (NEW).]

10. "Damage" means to destroy, alter, disrupt, delete, add, modify, or rearrange any computer resource by any means.
[PL 1989, c. 620 (NEW).]

10-A. "Data storage device" means any computer or accessory device, designed for or capable of storing digital media or data, including, but not limited to, installed or transportable hard drives, memory cards and servers.
[PL 2013, c. 297, §2 (NEW).]

11. "Not authorized" and "unauthorized" mean not having consent or permission of the owner, or person licensed or authorized by the owner to grant consent or permission, to access or use any computer resource, or accessing or using any computer resource in a manner exceeding the consent or permission.
[PL 1989, c. 620 (NEW).]

SECTION HISTORY

PL 1989, c. 620 (NEW). PL 2013, c. 297, §§1, 2 (AMD). PL 2013, c. 519, §7 (AMD).

§432. Criminal invasion of computer privacy

1. A person is guilty of criminal invasion of computer privacy if the person intentionally accesses any computer resource knowing that the person is not authorized to do so.
[PL 1989, c. 620 (NEW).]

2. Criminal invasion of computer privacy is a Class D crime.
[PL 1989, c. 620 (NEW).]

SECTION HISTORY

PL 1989, c. 620 (NEW).

§433. Aggravated criminal invasion of computer privacy

1. A person is guilty of aggravated criminal invasion of computer privacy if the person:

A. Intentionally makes an unauthorized copy of any computer program, computer software or computer information, knowing that the person is not authorized to do so; [PL 1989, c. 620 (NEW).]

B. Intentionally or knowingly damages any computer resource of another person, having no reasonable ground to believe that the person has the right to do so; or [PL 1989, c. 620 (NEW).]

C. Intentionally or knowingly introduces or allows the introduction of a computer virus into any computer resource, having no reasonable ground to believe that the person has the right to do so. [PL 1989, c. 620 (NEW).]
[PL 1989, c. 620 (NEW).]

2. Aggravated criminal invasion of computer privacy is a Class C crime.
[PL 1989, c. 620 (NEW).]

SECTION HISTORY

PL 1989, c. 620 (NEW).

§434. Prosecution of invasion of computer privacy

1. The crime of criminal invasion of computer privacy as defined in section 432 may be prosecuted and punished in:

A. The county in which the defendant was located when the defendant accessed the computer resource; or [PL 2011, c. 133, §1 (NEW).]

B. A county in which the computer resource was located. [PL 2011, c. 133, §1 (NEW).]
[PL 2011, c. 133, §1 (NEW).]

2. The crime of aggravated criminal invasion of computer privacy as defined in section 433 may be prosecuted and punished in:

A. The county in which the defendant was located when the defendant copied the computer program, computer software or computer information; [PL 2011, c. 133, §1 (NEW).]

B. The county in which the defendant was located when the defendant damaged the computer resource; [PL 2011, c. 133, §1 (NEW).]

C. The county in which the defendant was located when the defendant introduced or allowed the introduction of a computer virus into the computer resource; or [PL 2011, c. 133, §1 (NEW).]

D. A county in which the computer resource was located. [PL 2011, c. 133, §1 (NEW).]
[PL 2011, c. 133, §1 (NEW).]

SECTION HISTORY

PL 2011, c. 133, §1 (NEW).

§435. Added jurisdiction to prosecute

1. In addition to the State's having jurisdiction pursuant to section 7 to convict a person under section 432 or 433, the State has jurisdiction to convict a person under this chapter when that person is physically located outside of this State and the prohibited conduct:

A. Occurs outside of this State and the victim of the crime is a resident of this State at the time of the crime; and [PL 2011, c. 377, §1 (NEW).]

B. Is sufficient under this section to constitute a crime in this State. [PL 2011, c. 377, §1 (NEW).]
[PL 2011, c. 377, §1 (NEW).]

2. As used in this section, "resident" means a person who lives in this State either permanently or for an extended period. "Extended period" includes, but is not limited to, the period of time a student attends a school or college and the period of time a person serving in the Armed Forces of the United States is stationed in this State.
[PL 2011, c. 377, §1 (NEW).]

SECTION HISTORY

PL 2011, c. 377, §1 (NEW).

§436. Permanent destruction of computer data on a computer used in the commission of a crime

1. If a person is convicted upon a finding of guilt or upon the acceptance of a plea of guilty or nolo contendere or found not criminally responsible of a violation of this Title, the State, after all appeal periods have run and those proceedings have concluded, may permanently destroy the computer data on any computer that was used to commit or facilitate the commission of that violation or cause the computer data to be permanently destroyed through the removal and destruction of any part of the computer in the possession of the State on which the computer data are stored.
[PL 2013, c. 297, §3 (NEW).]

2. Notwithstanding subsection 1, a criminal justice agency, prior to the destruction of computer data, may extract and provide computer data to a person if:

A. Prior to the conclusion of criminal prosecution in the matter involving the computer data, the person provides written notification to the criminal justice agency having custody of the computer on which the computer data are stored that the person is interested in obtaining that computer data; [PL 2013, c. 297, §3 (NEW).]

B. The person either has an ownership interest in the computer data or wants the computer data only for the sentimental value of the data. When computer data are requested only for the sentimental value of the data, the person must state such in a written affidavit; [PL 2013, c. 297, §3 (NEW).]

C. The computer data that are the subject of the person's request may be lawfully disseminated; [PL 2013, c. 297, §3 (NEW).]

D. The computer data that are the subject of the person's request are not confidential by law; [PL 2013, c. 297, §3 (NEW).]

E. The computer data that are the subject of the request are specifically identified by the person making the request. For the purposes of this paragraph, "specifically identified" means identified with reasonable precision and not merely categorically; [PL 2013, c. 297, §3 (NEW).]

F. The criminal justice agency, in the judgment of the chief officer of the agency, determines the agency has the technological expertise, resources and personnel available to accommodate the request or to cause the request to be accommodated. The chief officer of the agency may consider whether there is a 3rd-party vendor that can accommodate the request if the chief officer determines the agency cannot accommodate the request for reasons provided in this paragraph. The chief officer of the agency subject to the request shall refer the request to an appropriate 3rd-party vendor for processing upon receipt by the chief officer of the agency of full payment from the requestor for the amount charged by the vendor to accommodate the request for information; and [PL 2013, c. 297, §3 (NEW).]

G. Notwithstanding any provision of law to the contrary, the person requesting the computer data makes advance payment for the time and costs that the criminal justice agency estimates will be needed for the requested computer data to be extracted and provided by the agency or caused by the agency to be extracted and provided to the person. [PL 2013, c. 297, §3 (NEW).]

If the conditions identified in paragraphs A to G of this subsection are not met, the computer data that are the subject of the request may be permanently destroyed in accordance with subsection 1.

The chief officer of the criminal justice agency that is subject to a request under this subsection shall respond to the requestor within 60 days from the date the request was received by the chief officer. The chief officer's response must include but is not limited to what actions if any the agency will take regarding the computer data identified in the request.
[PL 2013, c. 297, §3 (NEW).]

SECTION HISTORY

PL 2013, c. 297, §3 (NEW).

§437. Permissible destruction or transfer of ownership to the State of a computer used in the commission of a crime

1. Notwithstanding any provision of law to the contrary and except as provided in subsection 3, the State may either permanently destroy or assume ownership of a computer that was used in the commission of a crime or that facilitated the commission of a crime if:

A. A person is convicted upon a finding of guilt or upon the acceptance of a plea of guilty or nolo contendere or is found not criminally responsible of a crime committed using, or that was facilitated through the use of, the computer and all appeal periods have run and those proceedings have concluded; [PL 2013, c. 297, §3 (NEW).]

B. The opportunity for the computer to be forfeited to the State through proceedings at the presentencing stage has passed; and [PL 2013, c. 297, §3 (NEW).]

C. A person having a lawful property interest in the computer has not notified the State in writing within 6 months following a conviction upon a finding of guilt or upon the acceptance of a plea of guilty or nolo contendere or a finding of not criminally responsible that the person wants to take possession of the computer. The written notification must be made to the criminal justice agency having custody of the computer. [PL 2013, c. 297, §3 (NEW).]

If the State assumes ownership of a computer pursuant to this subsection, all computer data stored on the computer must be permanently destroyed by the State, or caused by the State to be permanently destroyed, in accordance with section 436.
[PL 2013, c. 297, §3 (NEW).]

2. A person who has a lawful property interest in a computer that was used to commit a crime or that facilitated the commission of a crime may take possession of the computer if:

A. The person notifies the State in writing within 6 months following a conviction upon a finding of guilt or upon the acceptance of a plea of guilty or nolo contendere or a finding of not criminally responsible that a person committed a crime using, or that was facilitated by the use of, the computer and all appeal periods have run and those proceedings have concluded, that the person wants to take possession of that computer. The written notification must be made to the criminal justice agency having custody of the computer; [PL 2013, c. 297, §3 (NEW).]

B. The crime that was committed using, or that was facilitated through the use of, the computer is not a crime identified in chapter 12; and [PL 2013, c. 297, §3 (NEW).]

C. All computer data stored on the computer have been permanently destroyed pursuant to section 436. [PL 2013, c. 297, §3 (NEW).]
[PL 2013, c. 297, §3 (NEW).]

3. Notwithstanding subsection 2, a person having a lawful property interest in a computer may not take possession of that computer if the crime that was committed using, or that was facilitated through the use of, the computer is a crime identified in chapter 12. Notwithstanding subsection 1, the computer may be permanently destroyed by the State, or caused by the State to be permanently destroyed, in accordance with section 436 if the crime that was committed using, or that was facilitated through the use of, the computer is a crime identified in chapter 12.

When the State receives a notification from a person who wishes to take possession of a computer pursuant to subsection 2, the State must respond to that notification within 60 days from the date the notification was received by the State. The State's response must include but is not limited to what actions, if any, the State will take regarding the computer identified in the notification.
[PL 2013, c. 297, §3 (NEW).]

SECTION HISTORY

PL 2013, c. 297, §3 (NEW).

The State of Maine claims a copyright in its codified statutes. If you intend to republish this material, we require that you include the following disclaimer in your publication:

All copyrights and other rights to statutory text are reserved by the State of Maine. The text included in this publication reflects changes made through the Second Regular Session of the 129th Maine Legislature and is current through October 1, 2020. The text is subject to change without notice. It is a version that has not been officially certified by the Secretary of State. Refer to the Maine Revised Statutes Annotated and supplements for certified text.

The Office of the Revisor of Statutes also requests that you send us one copy of any statutory publication you may produce. Our goal is not to restrict publishing activity, but to keep track of who is publishing what, to identify any needless duplication and to preserve the State's copyright rights.

PLEASE NOTE: The Revisor's Office cannot perform research for or provide legal advice or interpretation of Maine law to the public. If you need legal assistance, please contact a qualified attorney.