

**DOXING PROHIBITION AMENDMENTS**

2017 GENERAL SESSION

STATE OF UTAH

**Chief Sponsor: Howard A. Stephenson**

House Sponsor: Lee B. Perry

---

---

**LONG TITLE**

**General Description:**

This bill prohibits the dissemination of personal information without authorization.

**Highlighted Provisions:**

This bill:

- ▶ prohibits the disclosure or dissemination of identifying information with the intent or knowledge that the information will be further disseminated;
- ▶ defines identifying information; and
- ▶ provides that if the information is used to harass the person, it is a second degree felony.

**Money Appropriated in this Bill:**

None

**Other Special Clauses:**

None

**Utah Code Sections Affected:**

AMENDS:

**76-6-702**, as last amended by Laws of Utah 2005, Chapter 72

**76-6-703**, as last amended by Laws of Utah 2010, Chapter 193

---

---

*Be it enacted by the Legislature of the state of Utah:*

Section 1. Section **76-6-702** is amended to read:



28 **76-6-702. Definitions.**

29 As used in this part:

30 (1) "Access" means to directly or indirectly use, attempt to use, instruct, communicate  
31 with, cause input to, cause output from, or otherwise make use of any resources of a computer,  
32 computer system, computer network, or any means of communication with any of them.33 (2) "Authorization" means having the express or implied consent or permission of the  
34 owner, or of the person authorized by the owner to give consent or permission to access a  
35 computer, computer system, or computer network in a manner not exceeding the consent or  
36 permission.37 (3) "Computer" means any electronic device or communication facility that stores,  
38 retrieves, processes, or transmits data.39 [~~(5)~~] (4) "Computer network" means:

40 (a) the interconnection of communication or telecommunication lines between:

41 (i) computers; or

42 (ii) computers and remote terminals; or

43 (b) the interconnection by wireless technology between:

44 (i) computers; or

45 (ii) computers and remote terminals.

46 [~~(6)~~] (5) "Computer property" includes electronic impulses, electronically produced  
47 data, information, financial instruments, software, or programs, in either machine or human  
48 readable form, any other tangible or intangible item relating to a computer, computer system,  
49 computer network, and copies of any of them.50 [~~(4)~~] (6) "Computer system" means a set of related, connected or unconnected, devices,  
51 software, or other related computer equipment.52 (7) "Confidential" means data, text, or computer property that is protected by a security  
53 system that clearly evidences that the owner or custodian intends that it not be available to  
54 others without the owner's or custodian's permission.55 [~~(12)~~] (8) "Financial instrument" includes any check, draft, money order, certificate of  
56 deposit, letter of credit, bill of exchange, electronic fund transfer, automated clearing house  
57 transaction, credit card, or marketable security.58 (9) (a) "Identifying information" means any personal information, including the

59 person's:

60 (i) address or other location;

61 (ii) social security number;

62 (iii) driver license number;

63 (iv) nondriver governmental identification number;

64 (v) telephone number;

65 (vi) bank account number;

66 (vii) student identification number;

67 (viii) credit or debit card number;

68 (ix) personal identification number;

69 (x) unique biometric data;

70 (xi) employee or payroll number;

71 (xii) automated or electronic signature;

72 (xiii) computer image file;

73 (xiv) photograph;

74 (xv) computer screen name or password; or

75 (xvi) information in which the person has a reasonable expectation of privacy.

76 (b) "Identifying information" does not include information that is lawfully available

77 from publicly available information, or from federal, state, or local government records

78 lawfully made available to the general public.

79 [~~8~~] (10) "Information" does not include information obtained:

80 (a) through use of:

81 (i) an electronic product identification or tracking system; or

82 (ii) other technology used by a retailer to identify, track, or price goods; and

83 (b) by a retailer through the use of equipment designed to read the electronic product

84 identification or tracking system data located within the retailer's location.

85 [~~9~~] (11) "License or entitlement" includes:

86 (a) licenses, certificates, and permits granted by governments;

87 (b) degrees, diplomas, and grades awarded by educational institutions;

88 (c) military ranks, grades, decorations, and awards;

89 (d) membership and standing in organizations and religious institutions;

- 90 (e) certification as a peace officer;
- 91 (f) credit reports; and
- 92 (g) another record or datum upon which a person may be reasonably expected to rely in
- 93 making decisions that will have a direct benefit or detriment to another.

94 ~~[(11)]~~ (12) "Security system" means a computer, computer system, network, or

95 computer property that has some form of access control technology implemented, such as

96 encryption, password protection, other forced authentication, or access control designed to keep

97 out unauthorized persons.

98 ~~[(11)]~~ (13) "Services" include computer time, data manipulation, and storage functions.

99 ~~[(13)]~~ (14) "Software" or "program" means a series of instructions or statements in a

100 form acceptable to a computer, relating to the operations of the computer, or permitting the

101 functioning of a computer system in a manner designed to provide results including system

102 control programs, application programs, or copies of any of them.

103 Section 2. Section **76-6-703** is amended to read:

104 **76-6-703. Computer crimes and penalties.**

105 (1) A person who without authorization gains or attempts to gain access to and alters,

106 damages, destroys, discloses, or modifies any computer, computer network, computer property,

107 computer system, computer program, computer data or software, and thereby causes damage to

108 another, or obtains money, property, information, or a benefit for any person without legal

109 right, is guilty of:

110 (a) a class B misdemeanor when:

111 (i) the damage caused or the value of the money, property, or benefit obtained or

112 sought to be obtained is less than \$500; or

113 (ii) the information obtained is not confidential;

114 (b) a class A misdemeanor when the damage caused or the value of the money,

115 property, or benefit obtained or sought to be obtained is or exceeds \$500 but is less than

116 \$1,500;

117 (c) a third degree felony when the damage caused or the value of the money, property,

118 or benefit obtained or sought to be obtained is or exceeds \$1,500 but is less than \$5,000;

119 (d) a second degree felony when the damage caused or the value of the money,

120 property, or benefit obtained or sought to be obtained is or exceeds \$5,000; or

- 121 (e) a third degree felony when:
- 122 (i) the property or benefit obtained or sought to be obtained is a license or entitlement;
- 123 (ii) the damage is to the license or entitlement of another person; [~~or~~]
- 124 (iii) the information obtained is confidential or identifying information; or
- 125 (iv) in gaining access the person breaches or breaks through a security system.

126 (2) (a) Except as provided in Subsection (2)(b), a person who intentionally or

127 knowingly and without authorization gains or attempts to gain access to a computer, computer

128 network, computer property, or computer system under circumstances not otherwise

129 constituting an offense under this section is guilty of a class B misdemeanor.

130 (b) Notwithstanding Subsection (2)(a), a retailer that uses an electronic product

131 identification or tracking system, or other technology to identify, track, or price goods is not

132 guilty of a violation of Subsection (2)(a) if the equipment designed to read the electronic

133 product identification or tracking system data and used by the retailer to identify, track, or price

134 goods is located within the retailer's location.

135 (3) (a) A person who discloses or disseminates another person's identifying information

136 with the intention or knowledge that others will further disseminate or use the person's

137 identifying information is guilty of a third degree felony.

138 (b) If the disclosure or dissemination of another person's identifying information results

139 in electronic communication harassment, as described in Section 76-9-201, of the person

140 whose identifying information is disseminated, the person disseminating the information is

141 guilty of:

142 (i) a class B misdemeanor if the person whose identifying information is disseminated

143 is an adult; or

144 (ii) a class A misdemeanor if the person whose identifying information is disseminated

145 is a minor.

146 (c) A second offense under Subsection (3)(b)(i) is a class A misdemeanor.

147 (d) A second offense under Subsection (3)(b)(ii), and a third or subsequent offense

148 under this Subsection (3)(b), is a third degree felony.

149 [~~(3)~~] (4) A person who uses or knowingly allows another person to use any computer,

150 computer network, computer property, or computer system, program, or software to devise or

151 execute any artifice or scheme to defraud or to obtain money, property, services, or other things

152 of value by false pretenses, promises, or representations, is guilty of an offense based on the  
153 value of the money, property, services, or things of value, in the degree set forth in Subsection  
154 [76-10-1801\(1\)](#).

155 ~~[(4)]~~ (5) A person who intentionally or knowingly and without authorization, interferes  
156 with or interrupts computer services to another authorized to receive the services is guilty of a  
157 class A misdemeanor.

158 ~~[(5)]~~ (6) It is an affirmative defense to Subsections (1) and (2) that a person obtained  
159 access or attempted to obtain access in response to, and for the purpose of protecting against or  
160 investigating, a prior attempted or successful breach of security of a computer, computer  
161 network, computer property, computer system whose security the person is authorized or  
162 entitled to protect, and the access attempted or obtained was no greater than reasonably  
163 necessary for that purpose.

164 (7) Subsections (3)(a) and (b) do not apply to a person who provides information in  
165 conjunction with a report under Title 34A, Chapter 6, Utah Occupational Safety and Health  
166 Act, or Title 67, Chapter 21, Utah Protection of Public Employees Act.

---

---

**Legislative Review Note**  
**Office of Legislative Research and General Counsel**