LEGISLATIVE GENERAL COUNSEL
₵ Approved for Filing: E. Chelsea-McCarty ₵
₵ 02-15-17 10:52 AM ₵

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:

S.B. 227

76-6-702. Definitions.

As used in this part:

(1) "Access" means to directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

(2) "Authorization" means having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

(3) "Computer" means any electronic device or communication facility that stores, retrieves, processes, or transmits data.

[~~(5)~~] (4) "Computer network" means:

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

(i) computers; or

(ii) computers and remote terminals; or

(b) the interconnection by wireless technology between:

(i) computers; or

(ii) computers and remote terminals.

[~~(6)~~] (5) "Computer property" includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

[~~(4)~~] (6) "Computer system" means a set of related, connected or unconnected, devices, software, or other related computer equipment.

(7) "Confidential" means data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

[~~(12)~~] (8) "Financial instrument" includes any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, electronic fund transfer, automated clearing house transaction, credit card, or marketable security.

(9) (a) "Identifying information" means Ĥ→ **[~~any personal information, including the~~] a** ←Ĥ

person's:

Ŝ→ **[~~(i) address or other location;~~]** ←Ŝ

Ŝ→ **[~~(ii)~~] (i)** ←Ŝ social security number;

Ŝ→ **[~~(iii)~~] (ii)** ←Ŝ driver license number;

Ŝ→ **[~~(iv)~~] (iii)** ←Ŝ nondriver governmental identification number;

Ŝ→ **[~~(v) telephone number;~~]** ←Ŝ

Ŝ→ **[~~(vi)~~] (iv)** ←Ŝ bank account number;

Ŝ→ **[~~(vii)~~] (v)** ←Ŝ student identification number;

Ŝ→ **[~~(viii)~~] (vi)** ←Ŝ credit or debit card number;

Ŝ→ **[~~(ix)~~] (vii)** ←Ŝ personal identification number;

Ŝ→ **[~~(x)~~] (viii)** ←Ŝ unique biometric data;

Ŝ→ **[~~(xi)~~] (ix)** ←Ŝ employee or payroll number;

Ŝ→ **[~~(xii)~~] (x)** ←Ŝ automated or electronic signature; Ŝ→ **or** ←Ŝ

Ŝ→ **[~~(xiii) computer image file;~~]** ←Ŝ

Ŝ→ **[~~(xiv) photograph;~~]** ←Ŝ

Ŝ→ **[~~(xv) computer screen name or~~]** ←Ŝ Ĥ→ **computer** ←Ĥ password Ŝ→ **[~~; or~~**

~~(xvi) information in which the person has a reasonable expectation of privacy~~] ←Ŝ .

(b) "Identifying information" does not include information that is lawfully available from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

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

(a) through use of:

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

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

(b) by a retailer through the use of equipment designed to read the electronic product identification or tracking system data located within the retailer's location.

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

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

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

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

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

(e) certification as a peace officer;

(f) credit reports; and

(g) another record or datum upon which a person may be reasonably expected to rely in making decisions that will have a direct benefit or detriment to another.

[~~(10)~~] (12) "Security system" means a computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

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

[~~(13)~~] (14) "Software" or "program" means a series of instructions or statements in a form acceptable to a computer, relating to the operations of the computer, or permitting the functioning of a computer system in a manner designed to provide results including system control programs, application programs, or copies of any of them.

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

76-6-703. Computer crimes and penalties.

(1) A person who without authorization gains or attempts to gain access to and alters, damages, destroys, discloses, or modifies any computer, computer network, computer property, computer system, computer program, computer data or software, and thereby causes damage to another, or obtains money, property, information, or a benefit for any person without legal right, is guilty of:

(a) a class B misdemeanor when:

(i) the damage caused or the value of the money, property, or benefit obtained or sought to be obtained is less than $500; or

(ii) the information obtained is not confidential;

(b) a class A misdemeanor when the damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds $500 but is less than $1,500;

(c) a third degree felony when the damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds $1,500 but is less than $5,000;

(d) a second degree felony when the damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds $5,000; or

(e) a third degree felony when:

(i) the property or benefit obtained or sought to be obtained is a license or entitlement;

(ii) the damage is to the license or entitlement of another person; [~~or~~]

(iii) the information obtained is confidential or identifying information; or

(iv) in gaining access the person breaches or breaks through a security system.

(2) (a) Except as provided in Subsection (2)(b), a person who intentionally or knowingly and without authorization gains or attempts to gain access to a computer, computer network, computer property, or computer system under circumstances not otherwise constituting an offense under this section is guilty of a class B misdemeanor.

(b) Notwithstanding Subsection (2)(a), a retailer that uses an electronic product identification or tracking system, or other technology to identify, track, or price goods is not guilty of a violation of Subsection (2)(a) if the equipment designed to read the electronic product identification or tracking system data and used by the retailer to identify, track, or price goods is located within the retailer's location.

(3) (a) A person who Ŝ→ **, with intent that electronic communication harassment occur,** ←Ŝ discloses or disseminates another person's identifying information with the Ŝ→ **[~~intention or knowledge~~] expectation** ←Ŝ that others will further disseminate or use the person's identifying information is Ŝ→ **[~~guilty of a third degree felony~~] subject to the penalties outlined in Subsection (3)(b)** ←Ŝ .

(b) If the disclosure or dissemination of another person's identifying information results in electronic communication harassment, as described in Section 76-9-201, of the person whose identifying information is disseminated, the person disseminating the information is guilty of:

(i) a class B misdemeanor if the person whose identifying information is disseminated is an adult; or

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

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

(d) A second offense under Subsection (3)(b)(ii), and a third or subsequent offense under this Subsection (3)(b), is a third degree felony.

[~~(3)~~] (4) A person who uses or knowingly allows another person to use any computer, computer network, computer property, or computer system, program, or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things

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

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

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

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

Ŝ→ **(8) In accordance with 47 U.S.C.A. Sec. 230, this section may not apply to, and nothing in this section may be construed to impose liability or culpability on, an interactive computer service for content provided by another person.** ←Ŝ

Ĥ→ **(9) This section does not affect, limit, or apply to any activitiy or conduct that is protected by the constitution or laws of this state or by the constitution or laws of the United States.** ←Ĥ

Legislative Review Note
Office of Legislative Research and General Counsel