Chapter 39
Child Protection Registry

Part 1
General Provisions

13-39-101 Title.

This chapter is known as the "Child Protection Registry."

Enacted by Chapter 338, 2004 General Session

13-39-102 Definitions.

As used in this chapter:

(1) "Attorney general" means the same as that term is defined in Section 77-42-102.

(2) "Contact point" means an electronic identification to which a communication may be sent, including:

(a) an email address;

(b) an instant message identity, subject to rules made by the unit under Subsection 13-39-203(1);

(c) a mobile or other telephone number;

(d) a facsimile number; or

(e) an electronic address:

(i) similar to a contact point listed in this Subsection (2); and

(ii) defined as a contact point by rule made by the unit under Subsection 13-39-203(1).

(3) "Registry" means the child protection registry established in Section 13-39-201.

(4) "Unit" means the Internet Crimes Against Children unit within the Office of the Attorney General created in Section 67-5-21.

Amended by Chapter 356, 2019 General Session

Part 2
Operation of the Child Protection Registry

13-39-201 Establishment of child protection registry.

(1) The unit shall:

(a) establish and operate a child protection registry to compile and secure a list of contact points the unit has received pursuant to this section; or

(b) contract with a third party to establish and secure the registry described in Subsection (1)(a).

(2)

(a) A person may register a contact point with the unit pursuant to rules established by the unit under Subsection 13-39-203(1) if:

(i) the contact point belongs to a minor;

(ii) a minor has access to the contact point; or

(iii) the contact point is used in a household in which a minor is present.

(b) A school or other institution that primarily serves minors may register its domain name with the unit pursuant to rules made by the unit under Subsection 13-39-203(1).

(c) The unit shall provide a disclosure in a confirmation message sent to a person who registers a contact point under this section that reads: "No solution is completely secure. The most effective way to protect children on the Internet is to supervise use and review all email messages and other correspondence. Under law, theft of a contact point from the Child Protection Registry is a second degree felony. While every attempt will be made to secure the Child Protection Registry, registrants and their guardians should be aware that their contact points may be at a greater risk of being misappropriated by marketers who choose to disobey the law."

(3) A person desiring to send a communication described in Subsection 13-39-202(1) to a contact point or domain shall:

(a) use a mechanism established by rule made by the unit under Subsection 13-39-203(2); and

(b) pay a fee for use of the mechanism described in Subsection (3)(a) determined by the unit in accordance with Section 63J-1-504.

(4) The unit may implement a program to offer discounted compliance fees to senders who meet enhanced security conditions established and verified by the division, the third party registry provider, or a designee.

(5) The contents of the registry, and any complaint filed about a sender who violates this chapter, are not subject to public disclosure under Title 63G, Chapter 2, Government Records Access and Management Act.

(6) The state shall promote the registry on the state's official Internet website.

Amended by Chapter 356, 2019 General Session

13-39-202 Prohibition of sending certain materials to a registered contact point -- Exception for consent.

(1) A person may not send, cause to be sent, or conspire with a third party to send a communication to a contact point or domain that has been registered for more than 30 calendar days with the unit under Section 13-39-201 if the communication:

(a) has the primary purpose of advertising or promoting a product or service that a minor is prohibited by law from purchasing; or

(b) contains or has the primary purpose of advertising or promoting material that is harmful to minors, as defined in Section 76-10-1201.

(2) Except as provided in Subsection (4), consent of a minor is not a defense to a violation of this section.

(3) An Internet service provider does not violate this section for solely transmitting a message across the network of the Internet service provider.

(4)

(a) Notwithstanding Subsection (1), a person may send a communication to a contact point if, before sending the communication, the person sending the communication receives consent from an adult who controls the contact point.

(b) Any person who proposes to send a communication under Subsection (4)(a) shall:

(i) verify the age of the adult who controls the contact point by inspecting the adult's government-issued identification card in a face-to-face transaction;

(ii) obtain a written record indicating the adult's consent that is signed by the adult;

(iii) include in each communication:

(A) a notice that the adult may rescind the consent; and

(B) information that allows the adult to opt out of receiving future communications; and

(iv) notify the unit that the person intends to send communications under this Subsection (4).

(c) The unit shall implement rules to verify that a person providing notification under Subsection (4)(b)(iv) complies with this Subsection (4).

Amended by Chapter 356, 2019 General Session

13-39-203 Rulemaking authority.

In accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, the unit shall make rules to establish procedures under which:

(1)

(a) a person may register a contact point with the unit under Section 13-39-201, including:

(i) the information necessary to register an instant message identity; and

(ii) for purposes of Subsection 13-39-102(2)(e), an electronic address that is similar to a contact point listed in Subsection 13-39-102(2); and

(b) a school or other institution that primarily serves minors may register its domain name with the unit under Section 13-39-201;

(2) the unit shall:

(a) provide a mechanism under which a person described in Subsection 13-39-201(3) may verify compliance with the registry to remove registered contact points from the person's communications; and

(b) establish the mechanism described in Subsection (2)(a) in a manner that protects the privacy and security of a contact point registered with the unit under Section 13-39-201; and

(3) the unit may:

(a) implement a program offering discounted fees to a sender who meets enhanced security conditions established and verified by the unit, the third party registry provider, or a designee; and

(b) allow the third party registry provider to assist in any public or industry awareness campaign promoting the registry.

Amended by Chapter 356, 2019 General Session

Part 3
Enforcement

13-39-301 Criminal penalty.

(1) A person who violates Section 13-39-202 commits a computer crime and is guilty of a:

(a) class B misdemeanor for a first offense with respect to a contact point registered with the unit under Subsection 13-39-201(2)(a); and

(b) class A misdemeanor:

(i) for each subsequent violation with respect to a contact point registered with the unit under Subsection 13-39-201(2)(a); or

(ii) for each violation with respect to a domain name registered with the unit under Subsection 13-39-201(2)(b).

(2) A person commits a computer crime and is guilty of a second degree felony if the person:

(a) uses information obtained from the unit under this chapter to violate Section 13-39-202;

(b) improperly:

(i) obtains contact points from the registry; or

(ii) attempts to obtain contact points from the registry; or
(c) uses, or transfers to a third party to use, information from the registry to send a solicitation.
(3) A criminal conviction or penalty under this section does not relieve a person from civil liability in an action under Section 13-39-302.
(4) Each communication sent in violation of Section 13-39-202 is a separate offense under this section.

Amended by Chapter 356, 2019 General Session

13-39-302 Civil action for violation.
(1) For a violation of Section 13-39-202, an action may be brought by:
(a) a user of a contact point or domain name registered with the division under Section 13-39-201; or
(b) a legal guardian of a user described in Subsection (1)(a).
(2) In each action under Subsection (1):
(a) a person described in Subsection (1) may recover the greater of:
(i) actual damages; or
(ii) $1,000 for each communication sent in violation of Section 13-39-202; and
(b) the prevailing party shall be awarded costs and reasonable attorney fees.

Enacted by Chapter 338, 2004 General Session

13-39-303 Administrative enforcement.
(1) The attorney general:
(a) shall investigate violations of this chapter; and
(b) may bring an action against a person who violates this chapter.
(2) A person who violates this chapter is subject to:
(a) a cease and desist order or other injunctive relief; and
(b) a fine of not more than $2,500 for each separate communication sent in violation of Section 13-39-202.
(3)
(a) A person who intentionally violates this chapter is subject to a fine of not more than $5,000 for each communication intentionally sent in violation of Section 13-39-202.
(b) For purposes of this section, a person intentionally violates this chapter if the violation occurs after the attorney general or a district or county attorney notifies the person by certified mail that the person is in violation of this chapter.

Amended by Chapter 356, 2019 General Session

13-39-304 Defenses.
It is a defense to an action brought under this chapter that a person:
(1) reasonably relied on the mechanism established by the unit under Subsection 13-39-203(2); and
(2) took reasonable measures to comply with this chapter.

Amended by Chapter 356, 2019 General Session