Chapter 19.300 RCW
ELECTRONIC COMMUNICATION DEVICES

Sections

RCW 19.300.010 Definitions. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Affiliate" means any company that controls, is controlled by, or is under common control with another company. Affiliate may also include a supplier, distributor, business partner, or any entity that effects, administers, or enforces a government or business transaction.

(2) "Identification device" means an item that uses radio frequency identification technology or facial recognition technology.

(3) "Issued" means either:

(a) To have provided the identification device to a person; or

(b) To have placed, requested the placement, or be the intended beneficiary of the placement of, the identification device in a product, product packaging, or product inventory mechanism.

(4) "Person" means a natural person who resides in Washington.

(5) "Personal information" has the same meaning as in RCW 19.255.010.

(6) "Radio frequency identification" means the use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it.

(7) "Remotely reading" means that no physical contact is required between the identification device and the mechanical device that captures data.

(8) "Unique personal identifier number" means a randomly assigned string of numbers or symbols that is encoded on the identification device and is intended to identify the identification device. [2009 c 66 § 1; 2008 c 138 § 2.]

Conflict with federal requirements—2009 c 66: "If any provision of this act is found to be in conflict with federal law or regulations, the conflicting provision of this act is declared to be inoperative solely to the extent of the conflict, and that finding or determination shall not affect the operation of the remainder of this act." [2009 c 66 § 4.]

Findings—2008 c 138: "The legislature finds that Washington state, from its inception, has recognized the importance of maintaining individual privacy. The legislature further finds that protecting the confidentiality and privacy of an individual's personal information, especially when collected from the individual without his or her knowledge or consent, is critical to maintaining the safety and well-being of its citizens. The legislature recognizes that inclusion of identification devices that broadcast data or enable data or

information to be collected or scanned either secretly or remotely, or both, may greatly magnify the potential risk to individual privacy, safety, and economic well-being that can occur from unauthorized interception and use of personal information. The legislature further recognizes that these types of technologies, whether offered by the private sector or issued by the government, can be pervasive." [2008 c 138 § 1.]

Conflict with federal requirements—2008 c 138: "If any provision of this act is found to be in conflict with federal law or regulations, the conflicting provision of this act is declared to be inoperative solely to the extent of the conflict, and that finding or determination shall not affect the operation of the remainder of this act." [2008 c 138 § 4.]

RCW 19.300.020 Identity theft or fraud—Penalty. A person that intentionally scans another person's identification device remotely, without that person's prior knowledge and prior consent, for the purpose of fraud, identity theft, or for any other illegal purpose, shall be guilty of a class C felony. [2008 c 138 § 3.]

Findings—Conflict with federal requirements—2008 c 138: See notes following RCW 19.300.010.

RCW 19.300.030 Prohibited practices—Exceptions—Application of consumer protection act. (1) Except as provided in subsection (2) of this section, a governmental or business entity may not remotely read an identification device using radio frequency identification technology for commercial purposes, unless that governmental or business entity, or one of their affiliates, is the same governmental or business entity that issued the identification device.

(2) This section does not apply to the following:

(a) Remotely reading or storing data from an identification device as part of a commercial transaction initiated by the person in possession of the identification device;

(b) Remotely reading or storing data from an identification device for triage or medical care during a disaster and immediate hospitalization or immediate outpatient care directly relating to a disaster;

(c) Remotely reading or storing data from an identification device by an emergency responder or health care professional for reasons relating to the health or safety of that person;

(d) Remotely reading or storing data from a person's identification device issued to a patient for emergency purposes;

(e) Remotely reading or storing data from an identification device of a person pursuant to court-ordered electronic monitoring;

(f) Remotely reading or storing data from an identification device of a person who is incarcerated in a correctional institution, juvenile detention facility, or mental health facility;

(g) Remotely reading or storing data from an identification device by law enforcement or government personnel who need to read a lost identification device when the owner is unavailable for notice, knowledge, or consent, or those parties specifically authorized by law enforcement or government personnel for the limited purpose of reading

a lost identification device when the owner is unavailable for notice, knowledge, or consent;

(h) Remotely reading or storing data from an identification device by law enforcement personnel who need to read a person's identification device after an accident in which the person is unavailable for notice, knowledge, or consent;

(i) Remotely reading or storing data from an identification device by a person or entity that in the course of operating its own identification device system collects data from another identification device, provided that the inadvertently received data comports with all of the following:

(i) The data is not disclosed to any other party;

(ii) The data is not used for any purpose; and

(iii) The data is not stored or is promptly destroyed;

(j) Remotely reading or storing data from a person's identification device in the course of an act of good faith security research, experimentation, or scientific inquiry including, but not limited to, activities useful in identifying and analyzing security flaws and vulnerabilities;

(k) Remotely reading or storing data from an identification device by law enforcement personnel who need to scan a person's identification device pursuant to a search warrant; and

(l) Remotely reading or storing data from an identification device by a business if it is necessary to complete a transaction.

(3) The legislature finds that the practices covered by this section are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW. [2009 c 66 § 2.]

Conflict with federal requirements—2009 c 66: See note following RCW 19.300.010.