**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.