

---

**SUBSTITUTE HOUSE BILL 1011**

---

**State of Washington**

**61st Legislature**

**2009 Regular Session**

**By** House Technology, Energy & Communications (originally sponsored by Representatives Morris, Chase, Hasegawa, Kagi, Darneille, Upthegrove, Hudgins, and Moeller)

READ FIRST TIME 02/19/09.

1           AN ACT Relating to regulating the use of identification devices;  
2 amending RCW 19.300.010; adding new sections to chapter 19.300 RCW; and  
3 creating a new section.

4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

5           **Sec. 1.** RCW 19.300.010 and 2008 c 138 s 2 are each amended to read  
6 as follows:

7           The definitions in this section apply throughout this chapter  
8 unless the context clearly requires otherwise.

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

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

15           ~~((+2))~~ (3) "Issued" means either:

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

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

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

2 ((+3)) (5) "Personal information" has the same meaning as in RCW  
3 19.255.010.

4 ((+4) "Data" means personal information, numerical values  
5 associated with a person's facial features, or unique personal  
6 identifier numbers stored on an identification device.

7 (+5)) (6) "Radio frequency identification" means ((a technology  
8 that uses radio waves to transmit data remotely to readers)) the use of  
9 electromagnetic radiating waves or reactive field coupling in the radio  
10 frequency portion of the spectrum to communicate to or from a tag  
11 through a variety of modulation and encoding schemes to uniquely read  
12 the identity of a radio frequency tag or other data stored on it.

13 ((+6) "Reader" means a scanning device that is capable of using  
14 radio waves to communicate with an identification device and read the  
15 data transmitted by that identification device.))

16 (7) "Remotely reading" means that no physical contact is required  
17 between the identification device and the ((reader is necessary in  
18 order to transmit)) mechanical device that captures data.

19 (8) "Unique personal identifier number" means a randomly assigned  
20 string of numbers or symbols that is encoded on the identification  
21 device and is intended to identify the identification device.

22 NEW SECTION. Sec. 2. A new section is added to chapter 19.300 RCW  
23 to read as follows:

24 (1) Except as provided in subsection (2) of this section, a  
25 governmental or business entity may not remotely read an identification  
26 device using radio frequency identification technology for commercial  
27 purposes, unless that governmental or business entity, or one of their  
28 affiliates, is the same governmental or business entity that issued the  
29 identification device.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 (3) The legislature finds that the practices covered by this  
4 section are matters vitally affecting the public interest for the  
5 purpose of applying the consumer protection act, chapter 19.86 RCW. A  
6 violation of this chapter is not reasonable in relation to the  
7 development and preservation of business and is an unfair or deceptive  
8 act in trade or commerce and an unfair method of competition for the  
9 purpose of applying the consumer protection act, chapter 19.86 RCW.

10 NEW SECTION. **Sec. 3.** A new section is added to chapter 19.300 RCW  
11 to read as follows:

12 The office of the attorney general shall, on an annual basis, make  
13 recommendations to the legislature on other personally invasive  
14 technologies that may warrant further legislative action.

15 NEW SECTION. **Sec. 4.** If any provision of this act is found to be  
16 in conflict with federal law or regulations, the conflicting provision  
17 of this act is declared to be inoperative solely to the extent of the  
18 conflict, and that finding or determination shall not affect the  
19 operation of the remainder of this act.

--- END ---