


FOURTEENTH CONGRESS OF THE REPUBLIC)
OF THE PHILIPPINES)
Third Regular Session)

OFFICE OF THE SECRETARY

9 NOV 25 11 08

SENATE
S.B. No. **3544**

RECEIVED BY: 

Introduced by Senator Miriam Defensor Santiago

EXPLANATORY NOTE

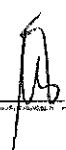
Radio frequency identification (RFID) tags, which consist of silicon chips and an antenna that can transmit data to a wireless receiver, could one day be used to track everything from soda cans to cereal boxes. Unlike bar codes, which need to be scanned manually and read individually, radio ID tags do not require line-of-sight for reading. Within the field of a wireless reading device, it is possible to automatically read hundreds of tags a second. Not only can these tags be read faster than bar codes, they also contain more information, so they can recall items more efficiently.

The applications for this technology are seemingly endless. Radio ID tags can be installed in clothing labels, books, packaging, or even implanted beneath skin. Retailers in the United States are investing heavily in RFID technology to improve supply-chain efficiency and track products from the warehouse to the consumer's doorstep. With this technology increasingly becoming available in our country, there is a need to protect the consumers from the dangers that may come from its use. This bill seeks to provide safeguards in the use of radio frequency identification devices.


MIRIAM DEFENSOR SANTIAGO

9 NOV 25 12:08

SENATE
S.B. No. 3544

RECEIVED BY: 

Introduced by Senator Miriam Defensor Santiago

1 AN ACT
2 PROTECTING THE USERS OF
3 RADIO FREQUENCY IDENTIFICATION DEVICES

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

4 SECTION 1. *Short Title.* – This Act shall be referred to as the “RFID Users
5 Protection Act of 2009.”

6 SECTION 2. *Definition of Terms.* – As used in this Act, the following terms shall
7 mean:

8 (a) “Identification device” means an item that uses radio frequency identification
9 technology;

10 (b) “Personal information” includes any of the following information associated with
11 an individual: (1) Social security number; (2) driver’s license number; (3) bank
12 account number; (4) credit card or debit card number; (5) personal identification
13 number; (6) automated or electronic signature; (7) unique biometric data; (8)
14 account passwords; (9) telephone number; (10) address; (11) date of birth; or (12)
15 any other piece of information that can be used to access an individual’s financial
16 accounts or to obtain goods or services, or offer goods or services based on that
17 information without an individual’s consent;

18 (c) “Radio frequency identification” or RFID means a technology that uses radio
19 waves to transmit data remotely to readers;

1 (d) "Reader" means a scanning device that is capable of using radio waves to
2 communicate with an identification device and read the data transmitted by that
3 identification device;

4 (e) "Remotely" means that no physical contact between the identification device and
5 the reader is necessary in order to transmit data;

6 (f) "Data" means personal information, numerical values associated with a person's
7 facial features, or unique personal identifier numbers stored on an identification
8 device;

9 (g) "Unique personal identifier number" means a randomly assigned string of
10 numbers or symbols that is encoded on the identification device and is intended to
11 identify the identification device.

12 SECTION 3. *Notice requirement.* – Any person who sells, issues, or distributes
13 items containing an electronic communication device must post a notice informing the
14 consumer of the use of such technology. The notice must disclose the following
15 information:

16 (a) The item contains or may contain an electronic communication device;

17 (b) The consumer has the legal right to request that an item containing an
18 electronic communication device be removed or deactivated before the item
19 leaves the premises; and

20 (c) The consumer has the right to request a copy of all personal information
21 collected about himself or herself through an electronic communication
22 device, including the identity of any person who has had access to the
23 consumer's personal information.

24 SECTION 4. *Labelling requirement.* – A person must not sell, use or distribute an
25 item that contains an electronic communication device without labelling the item with a
26 notice stating that:

1 (a) The item contains an electronic communication device capable of engaging in
2 electronic communication; and

3 (b) The device can transmit personal information to an independent reader or
4 scanner both before and after purchase or issuance.

5 SECTION 5. *Requesting review of personal information.* – A consumer may
6 request all stored personal information pertaining to himself or herself, including the
7 identity of any individual or entity who has had access to the consumer's personal
8 information. After reviewing one's personal information, the consumer must be given the
9 opportunity to contest the accuracy of his or her personal data, correct or amend the data,
10 and request that the information be removed or destroyed from the database, unless such
11 removal or destruction is prohibited by law.

12 SECTION 6. *Removal or deactivation.* – Upon request by a consumer, a person
13 who sells, issues or distributes an item containing an electronic communication device
14 must remove or deactivate the device before the consumer leaves the premises. Any costs
15 associated with removal or deactivation cannot be passed on to the consumer. Once
16 deactivated, it must not be reactivated without the express written consent of the
17 consumer associated with the item.

18 SECTION 7. *Security measures.* – Any person who sells or utilizes an electronic
19 communication device must implement adequate security measures to ensure that
20 information is secure from unauthorized access, loss or tampering. These security
21 measures should be consistent with industry standards that are commensurate with the
22 amount and sensitivity of the information being stored on the system.

23 SECTION 8. *Unauthorized scanning and other prohibited uses.* – A person may
24 not use an electronic communication device to remotely scan, or attempt to scan, an item
25 associated with a consumer without the consumer's knowledge. A person may not
26 disclose, either directly or through an affiliate, a consumer's personal information
27 associated with information gathered by, or contained within, a device capable of

1 engaging in electronic communication. A person may not use, either directly or through
2 an affiliate or non-affiliated third party, information gathered by, or contained within, a
3 device capable of engaging in electronic communication in order to identify a consumer.

4 SECTION 9. *Penalty for unlawful scanning.* – A person that intentionally scans
5 another person’s identification device remotely, without that person’s prior knowledge
6 and prior consent, for the purpose of fraud, identity theft, or for any other purpose, shall
7 be subject to a fine of not less than Fifty Thousand Pesos (P50,000.00) but not more than
8 Five Hundred Thousand Pesos (P500,000.00);

9 SECTION 10. *Separability Clause.* – If any part or provision of this Act is held
10 invalid or unconstitutional, the other parts or provisions of this Act shall remain valid and
11 effective.

12 SECTION 11. *Repealing Clause.* – All laws, decrees, orders, proclamations, rules
13 and regulations or parts thereof, inconsistent with the provisions of this Act are hereby
14 repealed, amended or modified accordingly.

15 SECTION 12. *Effectivity Clause.* – This Act shall take effect fifteen (15) days
16 from its publication in at least two (2) newspapers of general circulation.

Approved,