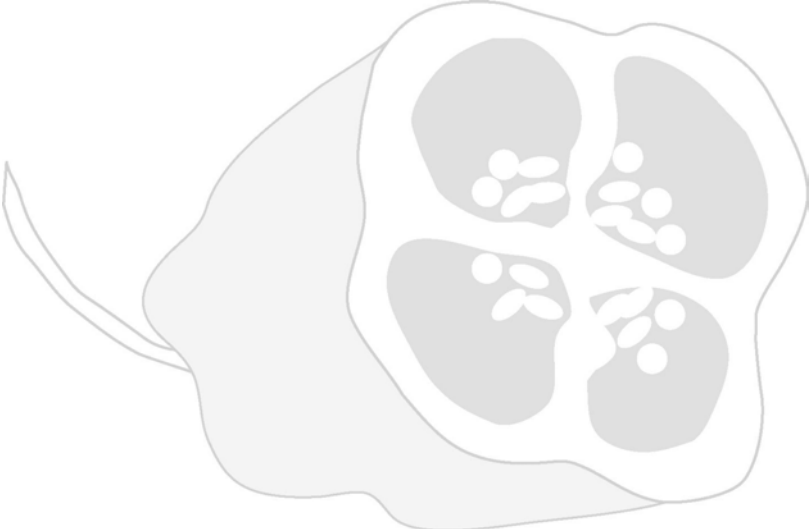


# RFID & Privacy

---

Two incidents inspired me to write this brief about RFID and Privacy. First one is a morning television show where a woman was being interviewed about how pet owners can take care of their pets while traveling. An interesting item she talked about was about how a veterinarian could assist travelers with pets, by embedding a chip on their pet that will allow the pet owners to continuously be aware its whereabouts. The second incident is from a while back. Not long ago, I wrote a paper highlighting how RFID could help Enterprise Supply Chain Management. While the paper's focus was on identifying the key areas within an enterprise where RFID could be applied to enable effective tracking of the supply chain, it only introduced the drawbacks of what could happen if such an implementation is not carefully monitored. The latest mandates by business houses such as Wal-Mart and Target, and government bodies, such as Department of Defense (DoD) have added hype to this already touted technology. While the enterprises are seemingly embracing the idea of using RFID in their supply chain systems, there is a range of issues that are associated with such deployments, which need to be addressed through society and policy. The most prominent issue is Privacy.

The intent of this brief is to highlight the privacy issues that may affect the potential consumers of RFID-tagged items. It also attempts to highlight how policies can enable positive adoption of RFID. The intent is clearly not to discourage consumers, but only to bring awareness to aid a more conscious adoption by the society.



---

## Radio Frequency IDentification

Radio Frequency IDentification (RFID) is a technology through which any object can be tracked in order to obtain information associated with it. Such objects differ based on the context in which RFID is used. For instance, in an enterprise supply chain system, raw materials could be tagged to enable effective tracking thereby smoothening the operations. Another example of RFID-tagged products includes consumer items ranging from a bag of chips, to toiletries, to personal products.

An RFID system consists of:

- Tags,
- Readers, and
- Data Processing System

The tags store information about the product such as the Electronic Product Code (EPC), and other stored values. The information in the tag is read using an RFID tag reader that has a read range of approximately 30 feet. It is not unusual for a reader to interface with a data processing system. The tag reader sends out radio frequency (RF) signals to activate the tags in the vicinity. Such activation would allow for the reader to access the information on the tag. In general, tags may either be self-activated, or would require an external power source to activate them.

RFID has been known to address several problems that involve “item tracking” through automatic data collection and processing of such data for business purposes. Some examples of where RFID can be of positive use are within an enterprise supply chain, or inside a retailer’s shop floor [8]. However, there are many issues that arise if such data collection is not governed by appropriate policies. Some issues of that nature are listed in the following section. A paper on this topic can also be found on the EFF web site [1].

*there are many  
issues that arise if  
such data  
collection is not  
governed by  
appropriate  
policies*

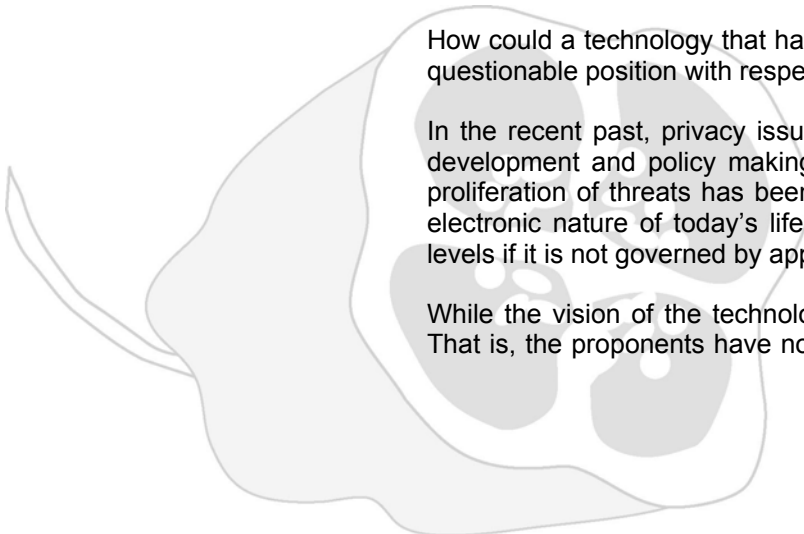
---

## RFID and Privacy Issues

How could a technology that has been in existence for several years end up in a questionable position with respect to privacy?

In the recent past, privacy issues have been in the forefront of any technology development and policy making. While the reasons for these are obvious, the proliferation of threats has been enhanced to higher degrees mainly due to the electronic nature of today’s life. RFID is believed take it to even more serious levels if it is not governed by appropriate regulations and policies.

While the vision of the technology is excellent, its focus appears to be narrow. That is, the proponents have not applied adequate thought to the privacy issues



involved in RFID deployments and adoption. Embracing RFID does not in itself translate to any form of threat to privacy. However, it is important to know when and where it could become a threat to the security and privacy of the embracing society. Some of the intangible threats come in the form of [5]:

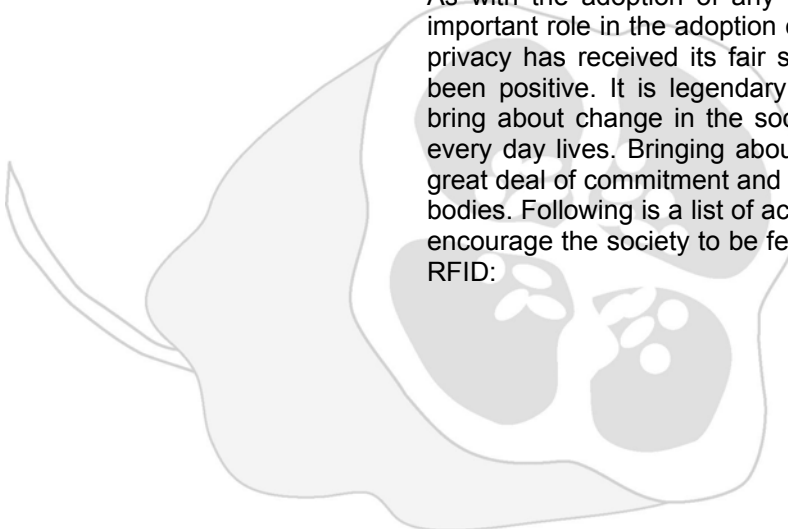
*Embracing RFID does not in itself translate to any form of threat to privacy. However, it is important to know when and where it could become a threat to the security and privacy of the embracing society.*

- Invisible tag readers that would activate tags on consumer goods. Examples include tags on personal products, prescription drugs, etc. A malicious reader would gain an unauthenticated access to your private information.
- Invisible tags in goods purchased by consumers. Such hidden tags could be the source of many different kinds of information about the consumers. Some examples include, analyzing buyer's behavior without the knowledge of the buyer, associating the information with consumer's identity information, etc.
- According to RFID's vision, every item will have its own identification code/number. It is highly likely that the users may not be concerned with the use of RFID due to the misrepresentation of the technology with respect to bar codes. The key difference is that bar codes are uniformly applied to all the products of a single type, while RFID tags are applied to each product. That is, every bag of a particular brand of potato chips will have the same bar code, while with RFID each such bag will have its own tag. This would allow a reader and a data processing system to get unique information about the buyer of a bag of potato chips. Such information may include the credit card number the consumer used to buy the snack.
- RFID tags are used in *contactless* payments where the user taps his credit card on a reader that will process the payment. While it is a convenient way to pay at the checkout, a hidden reader can read the details of the consumer from his tag. Examples of real life pilots of RFID in financial institutions are available through Glenbrook Partners [2].

---

### How can policies help?

As with the adoption of any technology, regulations and policies can play an important role in the adoption of RFID. It is only in the recent past that electronic privacy has received its fair share of hearing from the government, and it has been positive. It is legendary to note how laws, regulations, and policies can bring about change in the society, and these changes can be observed in our every day lives. Bringing about change in the electronic/online world requires a great deal of commitment and enforcement from the government and law-making bodies. Following is a list of activities in terms of regulations and policies that can encourage the society to be fearless about their privacy violations while adopting RFID:



*While the technology is still in its infancy, watch out for the developments in terms of the technology, privacy issues, and regulations that are being considered.*

- Enforce policies around RFID deployment in enterprises. Such policies should definitively help define the scope of the implementation of the technology to harness the benefits of the technology to both providers and consumers. An example can be industry-wide policy that the tags be removed at the point of sale, thereby avoiding any camouflaged tracking of the consumer.
- Policy to be transparent to the consumers about the usage of tags. This is much like the 'Privacy Policy' commonly found on websites that detail the use of personal information through 'cookies'. This would allow the user to make an informed judgment while participating in adopting the technology.
- Policy to define the content of the tag. Not every product is alike, and so is the information about them in a tag. Hence, each tag should contain only information pertaining to the product it is associated with.
- The readers must be placed in a secure environment and should have appropriate access controls while reading the tags.
- Policies and standards around reader to tag authentication will limit the inappropriate access to information on the tags.

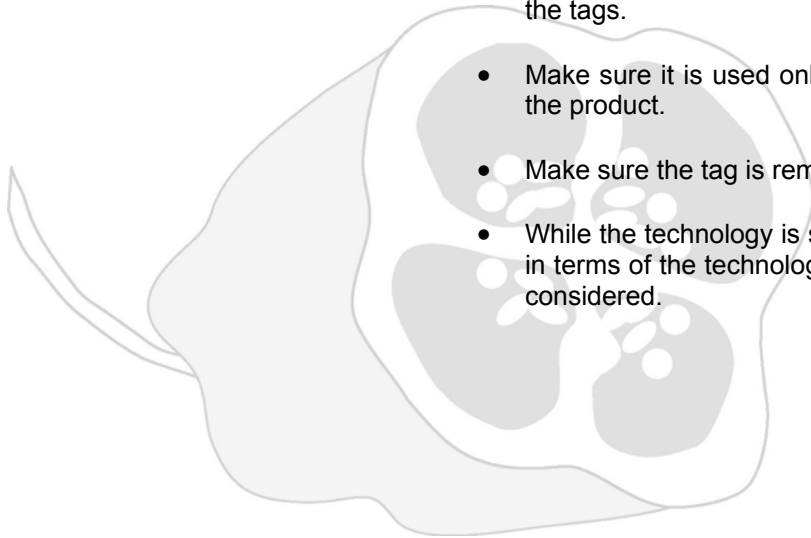
Despite regulations and policies, the society still bears the brunt of malpractices. The next section discusses what a consumer can do to avoid privacy violations.

---

### How can I avoid RFID violating my privacy?

As a consumer, you have a set of rights that you may want to exercise in case you are in doubt about the usage of RFID in a particular situation [2][3][5].

- Do not let your provider to force adopting active or passive RFID tags attached to the goods you purchase.
- Demand the provider for more information about the usage policies of the tags.
- Make sure it is used only for tracking the product, and not the bearer of the product.
- Make sure the tag is removed at the point of sale.
- While the technology is still in its infancy, watch out for the developments in terms of the technology, privacy issues, and regulations that are being considered.



---

## Conclusion

This brief introduced the readers to technology behind RFID. It provided the user an aggregated view of the privacy issues. The brief also discussed how policies could affect the adoption of RFID. It concluded with a discussion on how consumers could exercise their right in order to avoid privacy violations.

---

## Reference

- [1] Position Statement on the Use of RFID on Consumer Products (<http://www.eff.org>)
- [2] RFID in Financial Services (<http://www.glenbrook.com/opinions/rfid.html>)
- [3] <http://www.spy.org.uk/cgi-bin/rfid.pl>
- [4] <http://www.epcglobalinc.org/>
- [5] <http://www.stoprfid.org>
- [6] <http://www.epic.org/>
- [7] <http://news.com.com/2010-1069-980325.html>
- [8] <http://www.mietus.net>



---

**About the author:**

The author is a Program Manager, and a lead Architect at Identrus LLC, a global banking consortium specializing in authentication, document signing, and trust network solutions.

