Bonson, K. & Fenlon, W. (2015). How RDIF works (First of 10 pages). Retrieved on 23 Oct 2015\* from <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm>

How RFID Works

Long checkout lines at the grocery store are one of the biggest complaints about the shopping experience. Soon, these lines could disappear when the ubiquitous Universal Product Code (UPC) bar code is replaced by smart labels, also called radio frequency identification (RFID) tags. RFID tags are intelligent bar codes that can talk to a networked system to track every product that you put in your shopping cart.

Imagine going to the grocery store, filling up your cart and walking right out the door. No longer will you have to wait as someone rings up each item in your cart one at a time. Instead, these RFID tags will communicate with an electronic reader that will detect every item in the cart and ring each up almost instantly. The reader will be connected to a large network that will send information on your products to the retailer and product manufacturers. Your bank will then be notified and the amount of the bill will be deducted from your account. No lines, no waiting.

RFID tags, a technology once limited to tracking cattle, are tracking consumer products worldwide. Many manufacturers use the tags to track the location of each product they make from the time it's made until it's pulled off the shelf and tossed in a shopping cart.

Outside the realm of retail merchandise, RFID tags are tracking vehicles, airline passengers, Alzheimer's patients and pets. Soon, they may even track your preference for chunky or creamy peanut butter. Some critics say RFID technology is becoming too much a part of our lives -- that is, if we're even aware of all the parts of our lives that it affects.

In this article, you'll learn about the types of RFID tags and how these tags can be tracked through the entire supply chain. We'll also look at the noncommercial uses of RFID tags and how the Departments of State and Homeland Security are using them. Lastly, we'll examine what some critics consider an Orwellian application of RFID tags in animals, humans and our society.

Reinventing the Bar Code

Almost everything that you buy from retailers has a UPC bar code printed on it. These bar codes help manufacturers and retailers keep track of inventory. They also give valuable ­information about the quantity of products being bought and, to some extent, the consumers buying them. These codes serve as product fingerprints made of machine-readable parallel bars that store binary code.

Created in the early 1970s to speed up the check out process, bar codes have a few disadvantages:

•In order to keep up with inventories, companies must scan each bar code on every box of a particular product.

•Going through the checkout line involves the same process of scanning each bar code on each item.

•Bar code is a read-only technology, meaning that it cannot send out any information.

RFID tags are an improvement over bar codes because the tags have read and write capabilities. Data stored on RFID tags can be changed, updated and locked. Some stores that have begun using RFID tags have found that the technology offers a better way to track merchandise for stocking and marketing purposes. Through RFID tags, stores can see how quickly the products leave the shelves and which shoppers are buying them.

RFID tags won't entirely replace bar codes in the near future -- far too many retail outlets currently use UPC scanners in billions of transactions every year. But as time goes on we'll definitely see more products tagged with RFIDs and an increased focus on seamless wireless transactions like that rosy instant checkout picture painted in the introduction. In fact, the world is already moving toward using RFID technology in payments through special credit cards and smart phones -- we'll get into that later.

In addition to retail merchandise, RFID tags have also been added to transportation devices like highway toll passcards and subway passes. Because of their ability to store data so efficiently, RFID tags can tabulate the cost of tolls and fares and deduct the cost electronically from the amount of money that the user places on the card. Rather than waiting to pay a toll at a tollbooth or shelling out coins at a token counter, passengers use RFID chip-embedded passes like debit cards.

But would you entrust your medical history to an RFID tag? How about your home address or your baby's safety? Let's look at two types of RFID tags and how they store and transmit data before we move past grocery store purchase­s to human lives.

RFID Tags Past and Present

RFID technology has been around since 1970, but until recently, it has been too expensive to use on a large scale. Originally, RFID tags were used to track large items, like cows, railroad cars and airline luggage, that were shipped over long distances. These original tags, called inductively coupled RFID tags, were complex systems of metal coils, antennae and glass.

Inductively coupled RFID tags were powered by a magnetic field generated by the RFID reader. Electrical current has an electrical component and a magnetic component -- it is electromagnetic. Because of this, you can create a magnetic field with electricity, and you can create electrical current with a magnetic field. The name "inductively coupled" comes from this process -- the magnetic field inducts a current in the wire. You can learn more in How Electromagnets Work.

Capacitively coupled tags were created next in an attempt to lower the technology's cost. These were meant to be disposable tags that could be applied to less expensive merchandise and made as universal as bar codes. Capacitively coupled tags used conductive carbon ink instead of metal coils to transmit data. The ink was printed on paper labels and scanned by readers. Motorola's BiStatix RFID tags were the frontrunners in this technology. They used a silicon chip that was only 3millimeters wide and stored 96 bits of information. This technology didn't catch on with retailers, and BiStatix was shut down in 2001 [source: RFID Journal].

Newer innovations in the RFID industry include active, semi-active and passive RFID tags. These tags can store up to 2 kilobytes of data and are composed of a microchip, antenna and, in the case of active and semi-passive tags, a battery. The tag's components are enclosed within plastic, silicon or sometimes glass.

At a basic level, each tag works in the same way:

•Data­ stored within an RFID tag's microchip waits to be read.

•The tag's antenna receives electromagnetic energy from an RFID reader's antenna.

•Using power from its internal battery or power harvested from the reader's electromagnetic field, the tag sends radio waves back to the reader.

•The reader picks up the tag's radio waves and interprets the frequencies as meaningful data.

Inductively coupled and capacitively coupled RFID tags aren't used as commonly today because they are expensive and bulky. In the next section, we'll learn more about active, semi-passive and passive RFID tags.

Active, Semi-passive and Passive RFID Tags

Active, semi-passive and passive RFID tags are making RFID technology more accessible and prominent in our world. These tags are less expensive to produce, and they can be made small enough to fit on almost any product.

Active and semi-passive RFID tags use internal batteries to power their circuits. An active tag also uses its battery to broadcast radio waves to a reader, whereas a semi-passive tag relies on the reader to supply its power for broadcasting. Because these tags contain more hardware than passive RFID tags, they are more expensive. Active and semi-passive tags are reserved for costly items that are read over greater distances -- they broadcast high frequencies from 850 to 950 MHz that can be read 100 feet (30.5 meters) or more away. If it is necessary to read the tags from even farther away, additional batteries can boost a tag's range to over 300 feet (100 meters) [source: RFID Journal].

Like other wireless devices, RFID tags broadcast over a portion of the electromagnetic spectrum. The exact frequency is variable and can be chosen to avoid interference with other electronics or among RFID tags and readers in the form of tag interference or reader interference. RFID systems can use a cellular system called Time Division Multiple Access (TDMA) to make sure the wireless communication is handled properly [source: RFID Journal].

Passive RFID tags rely entirely on the reader as their power source. These tags are read up to 20 feet (six meters) away, and they have lower production costs, meaning that they can be applied to less expensive merchandise. These tags are manufactured to be disposable, along with the disposable consumer goods on which they are placed. Whereas a railway car would have an active RFID tag, a bottle of shampoo would have a passive tag.

Another factor that influences the cost of RFID tags is data storage. There are three storage types: read-write, read-only and WORM (write once, read many). A read-write tag's data can be added to or overwritten. Read-only tags cannot be added to or overwritten -- they contain only the data that is stored in them when they were made. WORM tags can have additional data (like another serial number) added once, but they cannot be overwritten.

Most pass­ive RFID tags cost between seven and 20 cents U.S. each [source: RFID Journal]. Active and semi-passive tags are more expensive, and RFID manufacturers typically do not quote prices for these tags without first determining their range, ­storage type and quantity. The RFID industry's goal is to get the cost of a passive RFID tag down to five cents each once more merchandisers adopt it.

In the next section, we'll learn how this technology could be used to create a global system of RFID tags that link to the Internet.

Talking Tags

When the RFID industry is able to lower the price of tags, it will lead to a ubiquitous network of smart packages that track every phase of the supply chain. Store ­shelves will be full of smart-labeled products that can be tracked from purchase to trash can. The shelves themselves will communicate wirelessly with the network. The tags will be just one component of this large product-tracking network.

The other two pieces to this network will be the readers that communicate with the tags and the Internet, which will provide communications lines for the network.

Let's look at a real-world scenario of this system:

•At the grocery store, you buy a carton of milk. The milk containers will have an RFID tag that stores the milk's expiration date and price. When you lift the milk from the shelf, the shelf may display the milk's specific expiration date, or the information could be wirelessly sent to your personal digital assistant or cell phone.

•As you exit the store, you pass through doors with an embedded tag reader. This reader tabulates the cost of all the items in your shopping cart and sends the grocery bill to your bank, which deducts the amount from your account. Product manufacturers know that you've bought their product, and the store's computers know exactly how many of each product need to be reordered.

•Once you get home, you put your milk in the refrigerator, which is also equipped with a tag reader. This smart refrigerator is capable of tracking all of the groceries stored in it. It can track the foods you use and how often you restock your refrigerator, and can let you know when that milk and other foods spoil.

•Products are also tracked when they are thrown into a trash can or recycle bin. At this point, your refrigerator could add milk to your grocery list, or you could program the fridge to order these items automatically.

•Based on the products you buy, your grocery store gets to know your unique preferences. Instead of receiving generic newsletters with weekly grocery specials, you might receive one created just for you. If you have two school-age children and a puppy, your grocery store can use customer-specific marketing by sending you coupons for items like juice boxes and dog food.

In order for this system to work, each product will be given a unique product number. MIT's Auto-ID Center is working on an Electronic Product Code (EPC) identifier that could replace the UPC. Every smart label could contain 96 bits of information, including the product manufacturer, product name and a 40-bit serial number. Using this system, a smart label would communicate with a network called the Object Naming Service. This database would retrieve information about a product and then direct information to the manufacturer's computers.

The information stored on the smart labels would be written in a Product Markup Language (PML), which is based on the eXtensible Markup Language (XML). PML would allow all computers to communicate with any computer system similar to the way that Web servers read Hyper Text Markup Language (HTML), the common language used to create Web pages.

We're not at this point yet, but RFID tags are more prominent in your life than you may realize. Wal-Mart and Best Buy are just two major merchandisers that use RFID tags for stocking and marketing purposes. Automated systems called intelligent software agents manage all the data coming in and going out from RFID tags and will carry out a specific course of action like sorting items [source: RFID Journal].

The United States retail market is on the cusp of embracing a major implementation of RFID technology through payment systems that use Near Field Communication. These are the credit cards of the future.

Near Field Communication, Smart Phones and RFID

NFC technology is promising because it presents the next evolution of convenient payment with an added layer of security. Some credit cards have NFC chips embedded in them and can be tapped against NFC payment terminals instead of swiped, which eliminates the possibility that someone could skim your data via the magnetic strip. This same system works with cellular phones, too: read up on how cellular electronic payments work to dig into the technology.

Google is one company pushing NFC payments with Google Wallet. The application stores credit card information under multiple layers of security and allows for quick tap payments at NFC terminals. That means the technology's usefulness is limited by the number of NFC payment terminals available in retail locations and the number of phones that support the technology -- at launch, Google Wallet only works with the Android Nexus S smart phone.

So what does this have to do with RFID? Near Field Communication devices can read passive RFID tags and extract the information stored in them. This technology is being used in modern advertising. For example, picture a normal poster advertising a pair of jeans, the kind of paper you'd see plastered on a wall in a shopping mall. Advertisers can make "smart" posters with RFID tags that add a new level of interaction with customers. Tap an NFC phone against a "smart" poster equipped with an RFID tag, and you may get a 10 percent off coupon for those jeans at Macy's. Passive RFID tags are cheap enough to be used in promotional materials just to engage customers.

NFC and RFID technologies have huge futures ahead of them in the retail world, but security remains a common concern. Some critics find the idea of merchandisers tracking and recording purchases to be alarming. Retail isn't the only industry using RFID technology: In the next section, we'll learn how the government is putting RFID tags to use.

Government-issued RFIDs

While many consumers happily -- or obliviously -- buy merchandise tracked with RFID tags, some people are up in arms about the U.S. government's legislation mandating that passports be embedded with RFID microchips.

On Aug. 14, 2006, the U.S. Department of State began issuing electronic passports, or e-passports. Prompted by the terrorist attacks of Sept.11, 2001 the Department of Homeland Security (DHS) proposed the e-passport as a security measure for air travel safety, border security and more efficient customs procedures at airports in the United States. The e-passport's enhanced security features -- a chip identification number, digital signature and photograph that acts as a biometric identifier -- make the passport impossible to forge.

The e-passport will help improve security, but with so much personal information embedded in the document, there have been many concerns raised about the e-passport's potential for identity theft. Two possible forms of identity theft that could occur with e-passports are:

•Skimming: when someone uses an RFID reader to scan data from an RFID chip without the e-passport holder's knowledge.

•Eavesdropping: when someone reads the frequencies emitted from the RFID chip as it is scanned by an official reader.

However, the DHS insists that the e-passport is perfectly safe to use and that proper precautions have been taken to ensure user confidentiality.

•For protection against skimming, the e-passport contains a metallic anti-skimming device. This device is a radio shield inserted between the passport's cover and first page. When the e-passport is closed, it can't be scanned at all; when it's open, it can only be read by a scanner that is less than 3.9 inches (10 centimeters) away [source: Department of State].

•To guard against eavesdropping, DHS has mandated that all areas where the e-passport is scanned be thoroughly covered and enclosed so that signals cannot be picked up beyond the authorized RFID reader.

The e-passport costs $97. While the cost may seem steep, the cost of installing RFID readers in airports is even more staggering. Adopting the e-passport will require gradual change, but aut­horities are already discussing what added security features and improved biometrics the next series of e-passports will have.

The debate over e-passports pales in comparison to debates over human chipping. Next, we'll learn what RFID microchips are doing in livi­ng things.

Animal and Human Chipping

Animal chipping is nothing new -- farmers have been tracking livestock for years using RFID technology. But companies are turning animal chipping for pets into big business, and some companies are offering options for human chipping.

RFID pet recovery systems rely on tiny microchips the size of a grain of rice that contains the pet owner's contact information and sometimes an animal's medical history. Veterinarians scan lost pets with an RFID reader to determine whether or not the pet has a microchip. But the system can break down here. There are many competing pet recovery systems and consequently, many pet microchips. The Humane Society of the United States has been campaigning for development of a universal RFID reader that vets could use to read a pet's microchip, no matter its manufacturer or year of manufacture. In November 2005, President George Bush signed a bill for the standardization of pet microchips and a national database of pet owner information [source: RFID Journal].

Even though the FDA approved the implantation of RFID microchips in animals and humans in 2004, research from as far back as 1996 shows that these implants can cause cancerous tumors in lab rats and mice [source: Washington Post]. Specifically, the implants caused sarcomas, which affect body tissue. No studies have proven yet that cancer can form in animals other than lab rats and mice, and it's still too early to tell what effects the chips can have on humans. No negative health effects have been linked to the radio waves emanating from RFID chips. Despite this evidence, or lack thereof, other disadvantages of human chipping may outweigh its advantages.

VeriChip Corp. is leading the human chipping business. The company makes microchips with unique identification numbers that link to a VeriChip medical database. The VeriChip database contains emergency contact information and medical histories. Patients with serious medical issues like Alzheimer's are ideal candidates for the VeriChip. In addition to a one-time implantation fee, VeriChip charges annual fees based on how much information you want in the database -- you can choose to have just your name and contact information or your full medical history. VeriChip is still growing, so there are not RFID readers in every hospital. Also, doctors might not scan every patient to check for a chip, so depending on the hospital or doctor, your VeriChip could prove useless.­

­­One VeriChip with greater rates of success is the Hugs Infant Protection Program. Under this RFID monitoring system, newborns in some hospital nurseries wear ankle bracelets with RFID chips. If an unauthorized person tries to remove a baby from the hospital, an alarm is sounded at the nurses' station and at exit doors. You can read more about successful infant abduction prevention on the VeriChip Web site.

RFID Criticism

As with many new technologies, people fear what they don't understand. In the case of RFID, consumers have many fears, some of which may be justified. This debate may be one of the few in which you'll find the American Civil Liberties Union and Christian Coalition on the same side.

Human chipping has seemingly higher stakes than merchandise tagging, and RFID critics are concerned that human chipping may one day become mandatory. When the company CityWatcher.com chipped two of its employees in 2006, these fears spun out of control. CityWatcher.com insisted that the employees were not forced to be chipped -- they volunteered for the microchip implants for easier access to secured vaults where confidential documents are stored. Other employees declined the implants, and their positions with the company were unaffected.

­Aside from the limitations of VeriChip scanning discussed in the last section, human chipping has profound religious and civil liberty implications for some people. Some believe that human chipping is foretelling a biblical prophecy from the Book of Revelation, interpreting the chip as the "Mark of the Beast." To others concerned with civil liberties, the chip is bringing us one step closer to an Orwellian society, in which our every action and thought will be controlled by Big Brother.

While we can choose whether or not to put RFID chips in ourselves or our pets, we have little control over tags being placed on commercial products that we buy. In the book "Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID," Katherine Albrecht and Liz McIntyre describe the most extreme implications of RFID tags. They describe how RFID tags could be used to gauge your spending habits and bank account to determine how much you should be charged for the products you buy. This may sound paranoid, but hackers have proven that some RFID tags can be tampered with, including disabling their anti-theft features and changing the price that corresponds to their product. Better encryption is needed to ensure that hackers can't pick up RFID frequencies with super-sensitive antennae.

What's more, some critics say that relying on RFID as the primary means of security could make human security checkpoints lazy and ineffective. If security guards rely solely on the RFID anti-theft devices in merchandise and RFID technology of government-issued identification to screen for criminals or terrorists, they might miss the criminal activity happening right in front of their eyes.