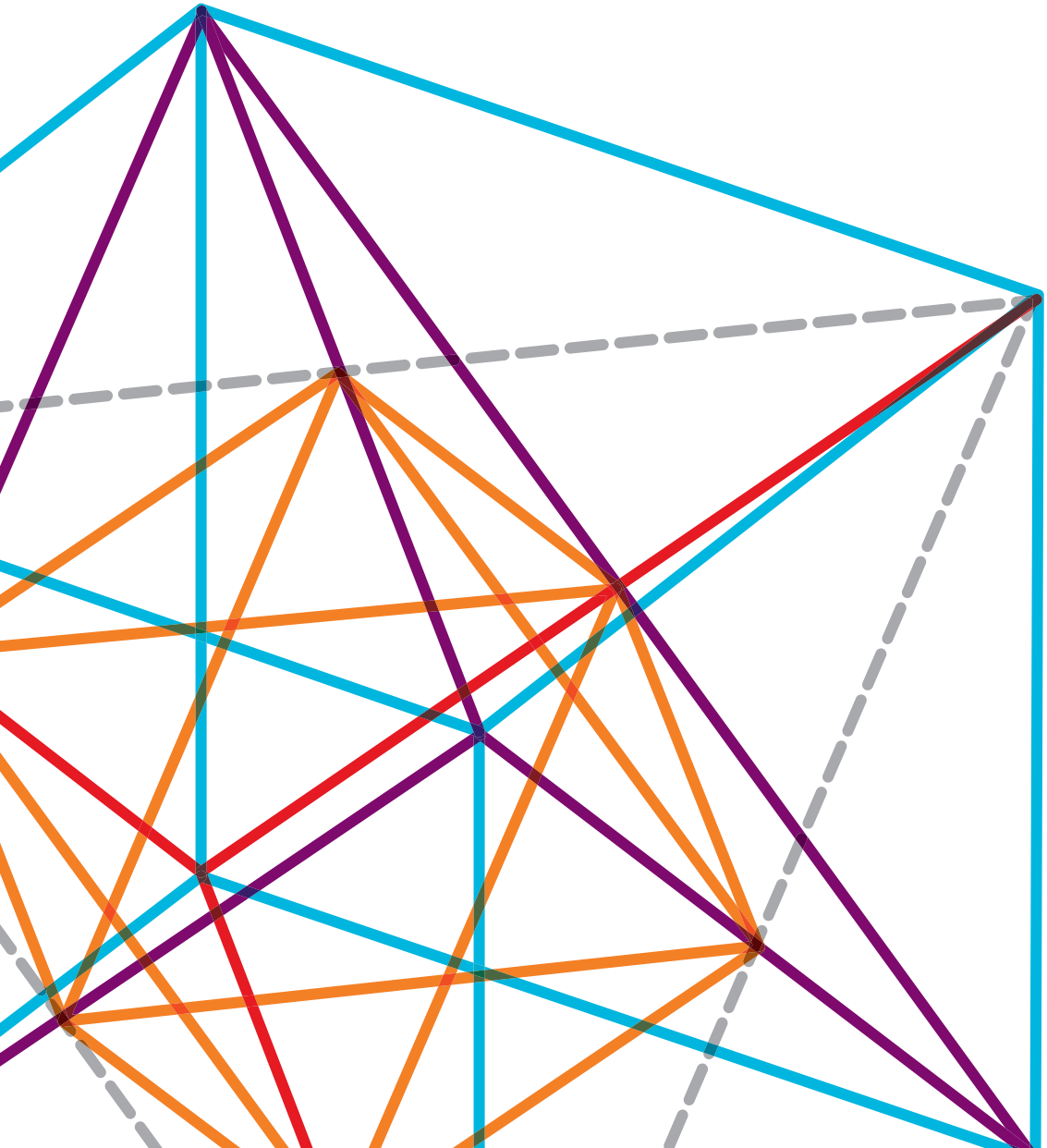
RFID AND YOUR PRIVACY—
Myths and Facts

ZEBRA TECHNOLOGIES

SEE MORE. DO MORE.



EXECUTIVE SUMMARY

Businesses and consumers today are asking, "Does radio frequency identification (RFID) invade the public's right to privacy?" With any emerging technology, this is certainly a valid question to ask. And now is the time to answer that question.

Fact is RFID has become a critical technology for a wide range of industries—from the supply chain, through manufacturing, all the way to the retail store and beyond. The return on investment (ROI) RFID delivers comes from reducing the time and labor required to track assets and materials, decreasing losses and theft, improving maintenance operations, and streamlining efficiency through better asset availability and utilization.

Even though RFID offers unprecedented value, some people have viewed RFID as a threat to privacy.

However, like any wireless technology, including cell phones, wireless networks and Bluetooth® connections, RFID devices provide remote readability. In theory, any technology that relies on radio frequency (RF) is inherently insecure. As a result, businesses and legislative bodies continuously seek ways to understand and lock down wireless security issues, while protecting the public's privacy—and RFID is no different.

This white paper presents the facts about RFID and dispels the myths that RFID is invasive to privacy. The discussion that follows provides an overview of RFID, the primary consumer privacy concerns, and measures that are currently or that will soon be in place to protect businesses and consumers from misuse of this vital technology.

INTRODUCTION

RFID is transforming global commerce in many unique ways. RFID provides many benefits for manufacturers and non-manufacturers alike. Businesses can use RFID to automate most processes for identifying objects and recording their location or movements. The technology often creates value by automatically recording these activities, reducing labor costs, and providing more complete and accurate information than manual record keeping. Automated RFID readers can ensure the recording of all asset movements and can issue alerts if unauthorized material movement occurs.

Given this remote reading ability, privacy advocates and government legislators within the E.U. and the U.S are voicing concerns that the ability to track people, products, vehicles and even currency could create a "Big Brother" world. Businesses and government agencies could pry into every aspect of consumer buying habits, travel routines and lifestyle. Businesses and organized crime could remotely track consumers who purchased RFID-tagged merchandise and use that information maliciously. In addition, insecure RFID technologies could expose both the private and public sector to security and safety risks.

According to Supply Chain Management Digest, legitimate RFID privacy questions do exist:

"Should a retailer be able to track a consumer's movements in a store, perhaps even without he or she being aware of it, through a reader network that monitored a tagged shopping cart, or even worse, an RFID-tagged credit card? Could a thief use a reader outside your home, and one day know there is a recently purchased laptop inside?"[1]

These concerns have triggered the RFID industry, retailers and public servants to take notice, raise awareness and promote measures to protect consumer privacy and information.

[1] Supply Chain Digest, "Is RFID being Singled Out by Privacy Advocates and Legislators?" April 7, 2009.

UNDERSTANDING RFID

One of the myths about RFID is that governments developed these systems specifically to track people. However, history shows that the precursor to RFID technology began back in WWII as a military effort to identify if an aircraft was friendly or belonged to the enemy. Under a secret project, the British developed the first active identify friend or foe (IFF) system that used a transmitter installed on each plane. When the transmitter received signals from ground-based radar stations, it transmitted a signal that identified the aircraft as friendly.

Today's RFID systems operate using the same principle. A reader sends an RF signal to a transponder, which turns on and either reflects back a signal (passive RFID) or transmits a signal (active RFID).[2] The first development of true RFID occurred in the early 1970s.[3] Engineers intended this early device for use as a toll device with the New York Port Authority.

Today's RFID systems are actually quite simple and rely on proven silicon, RF and database technologies. There are two types of RFID tags in use today. Passive tags target high-volume operations where tag cost is the primary consideration, such as in supply chain management (SCM) and retail. Active tags find their primary use in low-volume, high-value applications where the environmental conditions, range and data security are the primary concerns.

Classes of RFID Tags

Passive RFID tags contain a low-power integrated circuit (IC) attached to an antenna and enclosed with protective material (label media) as determined by the application. The most compact RFID devices use an IC as small as half a millimeter square, about the size of a tiny seed. On-board memory within the IC stores data, while the IC then transmits/receives information through the antenna to an external reader.

Passive tags receive all of their power from the external tag reader, allowing the tag to "wake up" and transmit data. Specifically, tags can be read-only (stored data can be read but not changed), read/write (stored data can be altered or rewritten), or a combination, in which some data is permanently stored while other memory remains accessible for later encoding and updates.

The vast number of passive RFID tags used in supply chain applications (such as asset management, inventory monitoring, access control and item-level tracking) comply with the UHF Gen 2 standard developed by EPCglobal. Passive tags use Electronic Product Code™ technology, which enables users to accurately identify multiple items at distances not possible with earlier generations of RFID tags. For more information about the Gen 2 standard, visit www.gs1.org/epcglobal.

A passive RFID tag is capable of transmitting a unique serial number anywhere from five to 30 feet in response to a query from a reading device. RFID readers connect through networks to computer systems that associate, or match, the RFID data to an internal database. The tag serial number acts as a pointer to the information about the product.

UHF Gen 2 tags target applications that require low cost, long range, and limited or no security. Other RFID technologies like the MIFARE® group of proprietary technologies based upon the ISO/IEC 14443 Type A 13.56 MHz contactless smart card standard, offer strong encryption, higher per-unit costs and very short (inches) read ranges. MIFARE finds use in payment card and ticketing applications where secure data transactions are required. The U.S. government's electronic passport program leverages both ISO/IEC 1444 and 7816, which also uses of a form of Public Key Infrastructure (PKI) that allows digital signatures to protect the data from tampering.[4]

[2] RFID Journal, "The History of RFID," http://www.rfidjournal.com/article/view/1338.
[3] Cardullo et al. "Transponder apparatus and system," U.S. Patent 3,713,148 (1973).
[4] U.S. Department of State, "Electronic Passport," http://edocket.access.gpo.gov/2005/05-21284.htm.

The cost to manufacture and deploy both active and passive RFID tags continues to drop, making them cost-effective solutions for many applications. For example, businesses embed RFID in proximity cards so employees can gain access to facilities. Entities at the state level use RFID to automate toll payment (e.g., TxTag, Speedpass™ and E-ZPass® systems). Another growing application includes animal tagging. Pet owners surgically embed active RFID tags into their dogs, cats, and livestock around the world, making it easier to identify stray animals should they get loose. The bottom line is that RFID is already in widespread use throughout the world, across a wide range of applications.

Remote Readability Realities

To keep costs low, RFID tags used in consumer applications rely on the EPCglobal standard, which does not require detailed data storage. The RFID reader must query the tag and then transmit the tag identifier to a host-level computing system. The host system then associates the identifier to a database entry. Simply put, the RFID tag itself contains no usable consumer data; the reader must have the ability to associate the tag information to a database. Then, application software must interpret the information and present it to the user. By default, this decoupling provides a minimal layer of compartmentalization from the actual information. The reader of the RFID tag must have access to both the tag and the database to gather information about which item the RFID was associated with. This is similar to determining who owns a vehicle; simply having the license plate number is not enough. One must associate the license plate to the actual registered user—two discrete pieces of information that are only linked within the state's motor vehicle databases.

Disabling RFID at the Point of Sale

Basic RFID technology already contains measures for protecting privacy. The EPCglobal standard supports "kill" codes for RFID tags. These password-protected commands force the RFID tag to permanently disable the IC logic, making them unreadable. For example, retailers can use "kill software" to disable an RFID tag before it leaves the store. Once a consumer purchases the item, the checkout clerk disables the RFID so the item does not alert the security sensors at the store entryway. As a result, the readers cannot track the tag post purchase.

While the RFID kill provision is widely available, not all retailers use the feature. The reason is that the tag can find use later on for product life cycle tracking, such as proof of purchase, warranty, item returns and product authentication. Given this reality, the vast majority of privacy concerns focus on the assumption that RFID tags attached to products remain functional even after the consumer purchases the merchandise and takes them home. In the case of retail, the information contained within the RFID tag is simply an extension of the UPC barcode that is already on the item, which contains no personal information and thus presents no risk of abuse. Moreover, all deployments of RFID in retail today rely on easily identifiable and removable tags—providing the consumer notice that RFID is in use and offering the choice to remove the tag if desired. Standards development at EPCglobal is addressing exactly these issues with the understanding that RFID usage in retail is still in its infancy.

Table 1: Common RFID Myths and Facts

Myth	Fact
When a consumer purchases an item tagged with RFID, someone with a reader could track the purchase.	Item-level tags used in retail contain the product UPC (identical to the barcode), with an additional 38-bit serial number. With that information, someone could only identify the item details (manufacturer, product type, etc.). If that's a concern, the retailer can encourage consumers to simply remove the tag prior to leaving the retail store.
If a consumer pays for a tagged item with a credit card, or uses a loyalty card, then someone could determine the purchaser's identity by reading the tag ID.	RFID used on retail items operate similar to a UPC code—there is no data written to the tag at the point of purchase that could identify a person.
When a consumer purchases an item tagged with RFID, someone with a reader could trace the person to his or her place of residence.	The read range of tagged items inside a car would not be useful as a tracking mechanism. A criminal would have an easier time tracking a cell phone signal, or even the vehicle license plate.
After the consumer unpacks their products and throws the packaging in the garbage, eavesdroppers and criminals could determine what the consumer purchased—a high-end stereo, for example—and then target the residence for theft.	Someone could potentially scan the trash for RFID tags, but being able to read them assumes the tags remained functional after the purchase. However, product-packaging materials present more information about merchandise than the item-level RFID tag. Product boxes, manuals and other labels have always presented an easy target for thieves since the beginning of the mass-market retail revolution.
RFID tags can be read from hundreds or thousands of meters away.	While highly specialized active RFID systems are capable of very long read distances, they are expensive and therefore used primarily in mission-critical applications. RFID tags commonly used in retail and supply chain applications are passive tags, costing less than $0.10 per tag. Passive tags have limited memory space and features and most commonly contain no more information than the barcode or label already on the item.

ADDRESSING PRIVACY CONCERNS

Technical Solutions

The heightened awareness over consumer privacy, coupled with the enormous benefits RFID delivers, is helping to create new opportunities for enhanced security. For example, Impinj, Inc., and NXP, N.V., recently announced new privacy features that not only contain the legacy "kill" feature, but also enable a retailer to replace the Electronic Product Code (EPC) with a random serial number. This adds another layer of protection and renders the RFID useless after the point of sale.

In May 2009, the European Commission (EC) approved a set of official recommendations that outlines data privacy objectives for use throughout the European Union's member states. The EC advises that retailers inform consumers if products contain RFID tags and that the tags require removal or deactivation at the point of sale. In addition, the EC recommendations help create a data-protection framework and specific guidance for industries that chose to opt-in or out. The EC objectives, along with the parallel efforts endorsed by the EPCglobal Public Policy Steering Committee, received support from industry and consumer groups alike, which will drive wider adoption of RFID technology.

Retailers, brand owners and technology providers continue to research technical solutions and address public privacy concerns.

Legislative Initiatives

Regardless of the need to associate the tag to a database, implementations of kill codes, and other emerging security measures, several legislative initiatives have gained momentum to protect citizens from misuse of RFID technology. In 2009, New York, New Hampshire, Nevada, Washington state and Massachusetts introduced RFID-related legislation regarding consumer privacy and use of data. At the Federal level, lawmakers proposed legislation that would require the consumer to provide explicit consent before a retailer could read data from RFID-tagged merchandise. Retailers do not have to ask permission to scan a cart of tagged merchandise a consumer plans to purchase, since the merchandise is part of the retailer's existing inventory. However, the retailer cannot read tags already in the consumer's possession, such as their driver's license, etc.

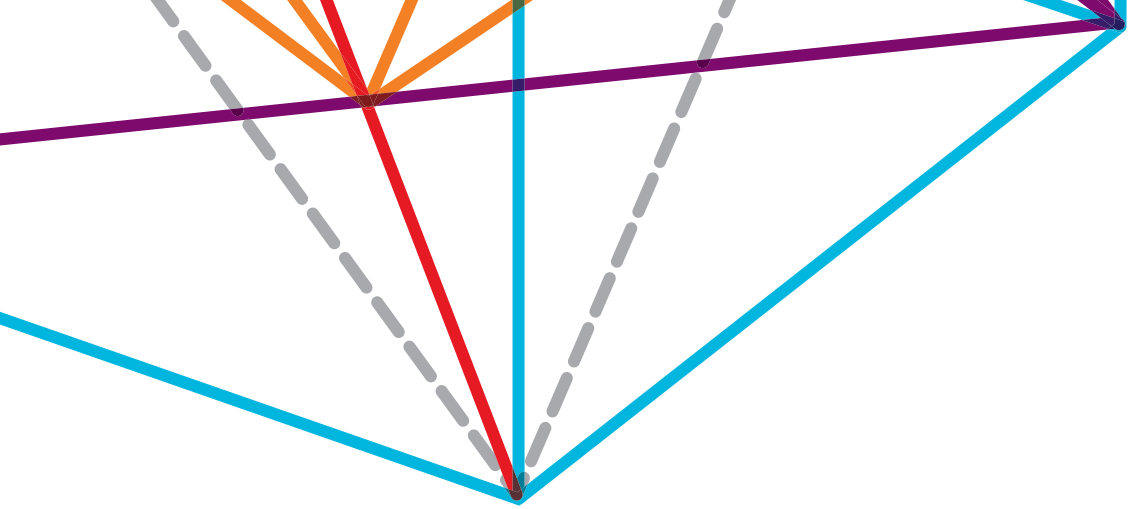
While legislators have paid attention to RFID privacy, the retail industry has been proactive to meet the public's concerns. The industry is facing these challenges on its own, so legislative restrictions have not been necessary thus far.

CONCLUSION

The examples above are just a few of the ways the industry is addressing RFID privacy concerns. Like any emerging technology, the implications to privacy are not always readily apparent. With RFID, a wide range of enterprises in both the private and public sector gain a flexible solution that complements an existing barcode infrastructure and creates new opportunities for reducing costs and improving operational efficiencies. When deployed with attention to personal privacy, RFID stands poised as a transformative, enabling technology.

A global leader respected for innovation and reliability, Zebra offers technologies that illuminate organizations' operational events involving their assets, people and transactions, allowing them to see opportunities to create new value. We call it the Visible Value Chain.

Zebra's extensive portfolio of marking and printing technologies, including barcode, RFID, GPS and sensoring, turns the physical into the digital to give operational events a virtual voice. This enables organizations to know in real-time the location, condition, timing and accuracy of the events occurring throughout their value chain. Once the events are seen, organizations can create new value from what is already there. For more information about Zebra's solutions, visit www.zebra.com.



Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
apacchannelmarketing@zebra.com

EMEA Headquarters
+44 (0)1628 556000
mseurope@zebra.com

Latin America Headquarters
+1 847 955 2283
inquiry4@zebra.com

Other Locations / USA: California, Georgia, Illinois, Rhode Island, Texas, Wisconsin **Europe:** France, Germany, Italy, the Netherlands, Poland, Spain, Sweden, Turkey, United Kingdom **Asia Pacific:** Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, Philippines, Singapore, South Korea, Taiwan, Thailand, Vietnam **Latin America:** Argentina, Brazil, Colombia, Florida (LA Headquarters in USA), Mexico **Africa/Middle East:** Dubai, South Africa

P1036727 Rev. 1 (06/13)