Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment version 1.4b, Option 1
Steve Hankel
Submitted 12/16/2003

Overcoming the Consumer Privacy Concerns of Product Tracking Through RFID Tags

Abstract

We are currently on the eve of another amazing technological revolution. Not since the introduction of the barcode has there been so much hype in the Manufacturing, Distribution, Defense, and Retail industries. The cost savings potential through greater supply chain efficiencies is enormous. Radio Frequency Identification (RFID) is about to bring about a huge transformation in the way products get to our favorite stores. With the wide-spread use of RFID right around the corner, privacy is becoming a major concern. This paper will introduce you to RFID, uncover the consumer privacy concerns, and come to a conclusion on what needs to be done to satisfy these concerns. Along the way it will explain the use of RFID historically, the technology behind it, and the greatest emerging concern of product tracking; people tracking.

What is RFID?

There has been a lot of talk recently in the press about Radio Frequency Identification (RFID), but in the general public not much is known about it. RFID is a wireless technology that allows a product RFID tag to be queried from a distance through the air by radio waves, as opposed to a product bar code which must be scanned directly by a laser. According to the MIT Auto-ID Center:

> *All RFID systems are comprised of three main components:*
>
> *--the RFID tag, or transponder, which is located on the object to be identified and is the data carrier in the RFID system,*
>
> *--the RFID reader, or transceiver, which may be able to both read data from and write data to a transponder, and*
>
> *--the data processing subsystem which utilizes the data obtained from the transceiver in some useful manner* (Sarma, Weis, and Engels, p.4).

There are two types of RFID tags; Active and Passive. The Active tags have their own power, are larger, and more expensive. Their range currently can be

up to 100 yards. Passive tags are powered by the RFID reader, can be as small as a human hair, and are relatively cheap. Their range currently is about 3-5 feet. Passive tags can be embedded in labels, or hidden in the packaging materials, or the product itself. Zebra Technologies makes a printer that will print RFID tags out on the fly. Figure 2 is a good example of just how small these Transponder Chips and Antennas actually are.

Some companies are claiming they have washable tags that can be embedded in clothing. They are working with appliance manufacturers to develop specialized washing machines, which can automatically read them and adjust the washing cycles accordingly. The tags are getting smaller and smaller, and the range is getting greater and greater. Economies of Scale are starting to develop with the increased demand, bringing costs to a more reasonable level. Alien Technology, one of the largest of the tag producers, was to produce half a billion tags for Gillette. Matrics, a Maryland company, offers fully packaged solutions, and claims they are the fastest and most powerful.

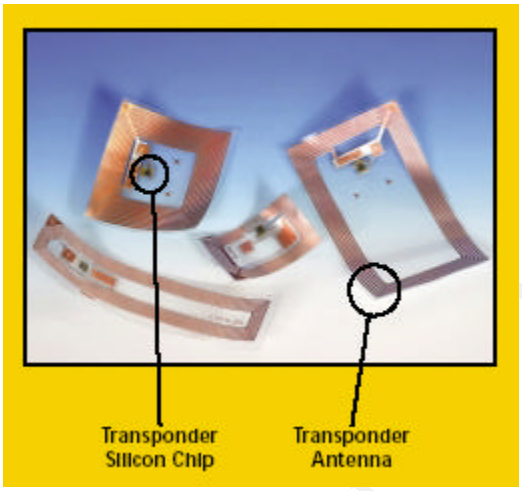

Figure 2 (http://www.scanplanet.com/solutions/RFID.asp)

Currently there are two major standards for RFID tags being used for product tracking. Both standards operate on the UHF frequency; currently 915 MHz in the US. International Standards Organization's ISO 18000 is the current globally approved standard. The Electronic Product Code (EPC), which was developed by the MIT Auto-ID Center, is the up and coming standard for the retail supply chain. The ISO 18000 standard is a generic; one size fits all standard, for use in different RFID applications, including supply chain product tracking. It primarily deals with the information going through the air. The newest version in development is ISO 18000 version 6, which should be released next year.

The newer EPC standard was developed specifically for commercial supply chain product tracking, with low cost, and wide-spread use in mind. It is divided into classes. "The current Class 0 and Class 1 specifications of the EPC protocol are

open standards….but they are not interoperable. The second version of Class 1 is expected to incorporate the specifications for both Class 0 (currently a factory programmable tag, but a read-write version is in the works) and Class 1 (a tag that lets the end user write the serial number to it.) Some are also pushing for Class 1, V2 to be interoperable with ISO018000 -6….." ("Wal-Mart," p.1). The newer standards also call for a global convergence to 915 MHz, since currently there are different frequencies used in Europe and Asia.

The Department of Defense has been using the ISO 18000 standard, and is requiring all of their over 23,000 suppliers to do the same. Wal-Mart and the rest of the retail business world are focusing on the EPC standard. This could cause trouble down the road, if companies have to supply to both Government and Business environments. Imagine being a company that supplies to both Government and Business. That may not be an issue, since there are over half a dozen standards for barcodes currently being used every day. It may of course slow down wide spread acceptance or adaptation into other industries. As mentioned above, some RFID equipment vendors are urging the Auto-ID Center to build backward compatibility into the EPC standard, claiming the latest implementation of ISO 18000 allows for this. There needs to be a convergence of the two standards, and more information shared on their interoperability. With all of the money at stake, I'm sure it will be a matter of time before this issue is resolved, and things are back on track.

Since Consumer Privacy issues are a big concern, the technology that we are most interested in is the EPC standard. As I stated earlier, one of the goals of the Auto-ID Center was to develop a low cost standard. This was achieved through putting as little as possible of the total system onto the RFID tag. On the tag is an Electronic Product Code (EPC), which is like a barcode, in the fact that it is a unique identifier. An Object Name Service (ONS) is used to associate the EPCs with a database IP. A transponder is used to both power and read the tags. Product Markup Language (PML) is used to describe the product. For the retail environment, we're talking about millions of possible serial numbers. How can all of the pieces fit together? A chief piece to the puzzle is the Savant system. According to the Auto-ID Center, "The Savant system is a hierarchical control and data management building block that can be used to provide automated control functionality and manage the large volumes of data generated by the RFID readers" (Sarma, Weis, and Engels, p.10). This should allow for the amazingly large amounts of data that may be collected.

RFID Uses

Historically, Radio Frequency (RF) systems have been a major piece of the puzzle with barcode systems. Barcodes are read by a laser which scans it, records the information, i.e. UPC symbol, and compares it with a database that resolves the symbol with a product description. RF systems have allowed for

wireless infrastructures to be built that allow for remote scanning of barcodes. Workers would use a handheld scanner that was connected wirelessly to a network server which kept the product information. You have probably seen employees at your favorite retail store scanning products for price checks, or doing inventory. The scanner reads the barcode, and then transmits the information through the air to the database. RFID eliminates this step, by having the product broadcast its information directly to the database, whenever it is queried. Instead of walking around the store or warehouse, scanning each item, you simply query all of the products remotely, and run a report.

RFID up until now has had a wide, but uncontroversial use. Ask anyone on the street, and the odds are they will have no idea of what it is, or what its uses are. The truth is, many of these same people use RFID day after day with little thought. Many security badges that you wave in front of a reader are based on RFID technology. The microchips that are used to identify our favorite lost pets are also. The keyless entry on your favorite car is based on RFID technology. In farm communities they're used to track livestock from farm to processing plant. In certain parts of the country it's being used to get gas, speed by the toll booth, cruise through the fast food drive thru, and to track prisoners and patients. Though these use RFID technology, they don't use it in quite the same way as is being proposed with the EPC system.

The military has used RFID for years to track weapons, ammo, supplies, and troops. Currently the Department of Defense's Total Asset Visibility network "…features RFID tracking of cargo containers, electronic event-driven alerts, anti-tamper systems, virtual inspections and authenticated audit trails" ("Ports," p.1). They are using RFID technology to keep a close eye on everything from bullets to bratwurst, as it makes its way around the world. They use both active and passive systems. The active systems can be tracked through GPS technology virtually anywhere in the world. If something is stolen, it can be detected before it leaves the base, or as it arrives somewhere else. If they are in short supply, the right people already know, and are ordering more. You can imagine how much money is already being saved by taxpayers. They are currently trying to drive this technology out to all of their suppliers.

The greatest anticipated use for RFID technology, and the one I will shift my focus to, is for tracking products through the supply chain. Instead of hand scanning each item, case, pallet, container, etc., you could have a real-time inventory report of exactly what is on the truck as it pulls into the drive bay. You could even note minor discrepancies, such as item substitutions, or missing items within a case. Stores will be able to have up-to-the-minute inventory tracking, which will help reduce shrinkage and overhead, and limit the number of times a product is handled, saving millions of dollars. Store shelves could tell the supplier when the shelf is empty, and automatically place an order for more merchandise.

Couple this with RFID swipe and carry technology for your credit card and imagine where it can take us. Customers may eventually be able to skip the check out line, while your credit card tells the store who you are, and your items tell them what you bought. The Las Vegas airport recently announced that they were going to start using a RFID system to tag all baggage going through the entire airport. This could virtually eliminate the chance of losing your suitcase, and may possibly speed up your time through the airport. It seems that the possibilities are endless. "Now RFID is about to reach ubiquity, bringing its ability to track everything, everywhere, all the time from the factory right into your home" (Booth-Thomas, p.1). You can start to see how privacy groups started to get worried. Will I be tracked along with my groceries or my baggage around the world?

The biggest promoter of RFID for commercial applications is Wal-Mart, who was the company that got barcodes off the ground in the early 80s. Barcodes had been around for years not really going anywhere. Wal-Mart has such a tremendous customer-base that suppliers will jump through any hoops to have access to all of the potential revenues. They recently announced they were requiring their top 100 suppliers be RFID ready by January, 2005 and the rest by the end of that year. They even detailed the specifications to be used, the standard EPC Class 1, V2, which allows some backward compatibility for those that aren't at version 2 yet, and have information about RFID tag vendors to help their suppliers get on the fast track. The Department of Defense is also requiring its top suppliers to be RFID compliant around the same time. It seems inevitable that the barcode is on its way out, to be replaced by the next big thing, RFID tags. And the potential to make even more money through supply chain efficiencies is driving it full speed ahead.

Privacy Concerns

You can see that being able to embed RFID tags in virtually anything is probably raising concerns about privacy. How can I be sure there aren't RFID tags in my clothing, notebooks, hair gel, and car? Can these be used to track my move anywhere I go? Is there anyway to search and destroy these RFID tags? Who is looking out for the consumer? Is the government doing anything to protect the privacy of consumers?

According to one privacy advocate, "…failing to impose conditions on the use of RFID technology could lead to a world not unlike the fictional society portrayed in Steven Spielberg's science-fiction thriller 'Minority Report'" (Gilbert, p.1). Imagine walking through the mall, with billboards shouting your name, and telling you to buy some snow chains to go with the tires that you purchased last week. Visualize getting home from a road trip finding a speeding ticket in the mail, and that your speed was tracked based on RFID tags embedded in the chrome wheels that you just had put on your car.

So far we've focused on retailers eavesdropping on customers that buy their products, but what about hackers? According to Scott Granneman of SecurityFocus, "Anything your companies' transceiver can detect, the bad guys' transceiver can detect. So don't be lulled into a false sense of security" (Granneman, p.1). The very nature of Passive RFID tags causes problems for security. With so little room for information, how can they be made secure? Where does the information go from the reader, and how is it stored? How can we protect our information from data pirates?

The insecurity of RFID Passive Systems stretches the privacy issue even further. Now do we not only have to worry about stores spying on us, but the potential of bad guys hacking in to our clothing and personal items. Now they can track me as I leave my house, and see that I'm headed across town. Then they can scan my house to see if there is anything worth taking and go burglarize my home. Maybe they can query a semi driving down the road to see if it is worth hijacking. Are these concerns legitimate or unfounded? The main concern is being able to associate multiple RFID tags to a certain person, based on known shopping patterns. If you query a tag for these three products, and you know that John Smith is one of a small percentage that uses those three products, then there is a good chance that it is John Smith.

As the potential is realized, however, businesses will try to push it closer and closer to the product level, and out into the public. If they can find out how long you have it in your home, when you throw it out, where you take it, they can Market to you better. They can see that a can of shaving cream lasts you two weeks, and have a coupon show up at your door, to get you to purchase their brand again. They could track consumption patterns throughout your household from the doll little Susie plays with, to the breakfast cereal that you eat. They could even make money selling this information to companies around the world. Law Enforcement could Subpoena businesses for information on who bought the pack of cigarettes that was found at the scene of a crime.

Recently, it was leaked, that Wal-Mart and Proctor and Gamble had been secretly testing RFID tags on individual lipstick packaging in one of their stores in Broken Arrow, Oklahoma, without consumer knowledge. Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), is one of many privacy groups speaking out on the use of RFID to track products into our homes. Founded, initially to speak out against the tracking of customer purchases through supermarket cards, they have now moved their primary focus to RFID tags in the retail arena. CASPIAN founder Katherine Albrecht was the first to voice her concern of the Wal-Mart incident. "'On the surface, the Broken Arrow trial may seem harmless. But the truth is that the businesses involved pushed forward with this technology in secret, knowing full well that consumers are overwhelmingly opposed to it. This is why we have called for mandatory labeling

of products containing RFID chips,'" (Vance, p.1). CASPIAN is currently pushing for government intervention through legislation.

The Electronic Privacy Information Center (EPIC) claims this is only the beginning of the privacy invasion. They say there is research going on right now, to develop microscopic chips hidden in ink, paint, or even explosives. Other groups such as Junkbusters, the Electronic Frontier Foundation, and Doxpara Research bring up similar concerns about our privacy. They already have the technology to embed them in fabric, and even money. With RFID tags on everything we own, will this allow the potential to track our every move, no matter where we are on the planet? Something must be done to protect our privacy, but what, and how?

Addressing Privacy Concerns

As you can see there are a number of privacy concerns that need to be addressed before the world-wide rollout of RFID. Work has already begun on addressing some of the privacy concerns. Boycotts, Government inquiries, education programs, and refocusing the RFID tag efforts farther away from the consumer, are a few current attempts. With the Wal-Mart deadline looming, a lot needs to happen in a very short time frame. Companies are already frantically moving to meet the deadline in January 2005. The concerns need to be addressed now before anything further is done. We can't pretend that this is going to go away.

CASPIAN, besides speaking out about privacy concerns regarding RFID tags, is organizing groups to fight it head to head in various ways. They have even managed to put a halt to an effort between Gillette and Wal-Mart involving tracking razors. After hearing of the plan to track razors through RFID tags, CASPIAN organized a world-wide boycott of Gillette. Shortly after, Gillette announced a 10 year delay in the plan. CASPIAN, however, isn't celebrating yet. "'We want to be sure their statements are not simply a convenient way to pacify the overwhelming number of consumers who have written and called Gillette to tell them they're outraged and switching brands'" (Albrecht, p.1).

They also had similar successful results in boycotting Benetton, when they started talking about embedding RFID tags in their clothing. After the world-wide advertising campaign announcing the boycott (see figure 1), Benetton quickly put on the brakes. By speaking out and organizing boycotts, CASPIAN is making it crystal clear to everyone, that if something isn't done to protect our privacy concerns, they will do something about it. Companies are not taking any chances on the privacy issue. They don't want to jeopardize the chance of having this great technology taken away from them. If they don't approach the implementation with kid gloves, the public could put a stop to it.

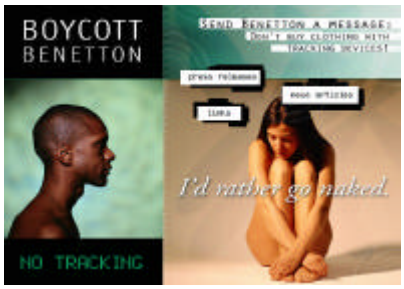

Figure 1 ("Group," p.1)

The Government needs to take an active roll on RFID privacy. We need privacy legislation now, before the widespread rollout. We need laws outlining how RFID tags can be used, and under what circumstances. We need to specify what information, if any, can be tracked. California, which seems to be the front-runner on privacy with its SB 1386 becoming law recently, had a Hearing on RFID and Privacy back in August. Kevin Ashton, Executive Director of MIT's Auto-ID Center which is the one of the main research groups behind the RFID EPC System, gave testimony to the California State Senate Subcommittee on New Technologies during the hearing. In his testimony, Mr. Ashton summed up his privacy recommendations into three key principles that consumers need to be empowered with:

> *-Notice. The right to know whether a product contains an EPC tag, and whether a public place is using RFID readers*
>
> *-Choice. The right to have the EPC tags in the purchased products deactivated without cost*
>
> *-Control. The right to have Personal Identity Information kept separate from Object Identity Information (Ashton, p.1).*

The most complete legislation proposal is the RFID Right to Know Act of 2003. Again CASPIAN is the front runner on RFID privacy, with this legislation. In it, they outline requirements on labeling to inform consumers, and direct businesses when and where RFID tags can be used. It also specifies what data can be collected, and how it can be shared. So far there doesn't seem to be much response from Government, but as more and more groups make their concerns known, it will be a matter of time before legislation such as this is passed and made into law.

A feature that is built in to the chips may help alleviate privacy concerns. The Auto-ID Center, in their research, has anticipated some of the privacy concerns that consumers would have. A feature that they designed into the RFID tags is a kill switch function that would allow the tags to be deactivated at the checkout, or by a device a consumer could use at home. Currently, many cash registers have similar disarming technology for deactivating RFID anti-theft tags. These anti-

theft tags are found on high dollar and high theft items such as CDs, clothing, and jewelry.

Of course with the anti-theft tags an alarm goes off if you leave the store without having them deactivated. With the product tracking tags you may never know if it was deactivated or not. Maybe this needs to be added into future revisions of the EPC standard. There are other ways to deactivate or prevent the functioning of the RFID tags. Some privacy groups such as the Electronic Privacy Information Center (EPIC) offer tips on thwarting privacy invasion through RFID tags. They spread the word on how to destroy the tags in various ways. Some of the methods include micro waving them, or using blocker tags to prevent the broadcast of information from certain tags.

Companies need to anticipate and actively listen to the public's privacy concerns. They need to start working together to come up with policies to deal with RFID tags and their use. They need to have a RFID privacy policy in place that is visible to the public, before they begin using them. The RFID privacy policy would state how RFID tags are used in the company, and what effect, if any, there is on the customer. They need to show the benefit to the customer, if any, of extending RFID tracking beyond the store. Maybe they need to give customers a chance to opt-in if they want to take part in the program. And finally, they could work with privacy groups such as CASPIAN in developing these policies. What better way to ease privacy concerns and build positive publicity, then to be approved, so to speak by a privacy group. Marks and Spencer, a British retailer, met with CASPIAN before launching its trial of RFID and was able to address their concerns before hand. This approach was highlighted by Forrester Research as "open, conservative and grounded in business purpose" (Thomas, p.1).

Since the CASPIAN boycott of Gillette, Wal-Mart is shifting its RFID efforts to the back room and the Distribution Center. Their initial implementation will involve truck, pallet, and case packs. No RFID tags will be used on individual products. This will still save the company millions of dollars, and avoid entering the anti-privacy melee. Rather than hand scan each item as it comes off the truck, they can get an instant reading of everything on the truck in real-time. They can still have real-time inventory at the distribution center level, since everything is stored at the pallet and case pack level. The million square foot warehouses can be inventoried instantly as opposed to the days or even weeks using the hand scan method. As large as Wal-Mart is, even a small per item savings, can lead to millions when spread company wide.

Education about the RFID technology is very important. People have to understand the technology a little better, before they start jumping out of windows. Currently, the range of Passive RFID tags is a maximum of three to five feet. The readers cost about a thousand dollars each. The tags are too expensive to put on the individual products. No one can agree on one standard.

I realize that all of this will change over time with economies of scale, but people have to realize the facts. They have to understand what is feasible with the current technology, and that they are not at this point even being used at the product level, and rarely at any point in the supply chain.

Passive RFID tags are not GPS systems. You can not put a Passive RFID tag on someone and know their exact coordinates, wherever they go around the world. The active RFID systems that the military uses have this capability, but these usually track large containers worth multi-million dollars. They also are much larger in size and cost then the passive tag system; not something you could hide in anything small. By knowing the facts, they can make an informed decision, and decide if they think it's a violation of privacy or not. Do I want to storm the Capitol, or maybe research it a little more thoroughly? There was a lot of outrage when barcodes first came on the scene, but now we don't pay any attention to them. We not only have a better understanding of them, but we have not heard any stories of people having their privacy violated. By keeping the public and most importantly the privacy groups informed, it will help to address the developing concerns of everyone involved.

There are ways to build more security into the RFID system to help protect our privacy from unauthorized sources. I mentioned the kill switch earlier as a way to overcome privacy concerns in the post retail setting. This is also a way to keep hackers from querying your RFID tags. If they are deactivated once they leave the store, they can not be read from authorized or unauthorized individuals. The Auto-ID Center also suggests, "…a simple RFID security scheme based on a one-way hash function….each hash-enabled tag contains a portion of memory reserved for a 'meta-ID' and operates in either an unlocked or locked state" (Sarma p.13). If a hacker attempts to query the tags they will awaken since they are passive tags, but without the matching meta-ID they will not unlock, and thus not be compromised. The trick will be not to add too much overhead to the system. There has to be a balance of low cost and security. If you focus too much on cost reduction, quite often security is compromised. Technologically, if we have a combination of the kill switch, along with the hash function for authentication, it will get us going in the right direction, and help reduce privacy concerns.

Conclusion

Radio Frequency Identification (RFID) is a technology that will add some great efficiencies to the product tracking supply chain. Not since the barcode have we seen something so big, with such an amazing potential. The technology will be embraced very quickly. There are many privacy concerns out there. Many of them are real, while some cry wolf. Some are currently being addressed, while others are still hanging. There are watch dog groups in place already, such as

CASPIAN, that are keeping an eye on what is going on, and taking steps to speak out for our privacy.

We need to focus on the facts, and provide education to the public. Both the Government and Big Business need to get to work on passing legislation and policies to deal with the privacy issue. We need to have mandatory labeling on packaging. There needs to be more done on the technology side to ensure that once the RFID tag technology is rolled out, the information is secure and private. The kill switch needs to be utilized, and more research needs to be done on implementing a hash function with meta-ID. Privacy groups will need to continue to boycott companies that proceed with RFID tag tracking until this issue is resolved. As with any new technology there are many questions, which will need to be answered sooner, rather than later. As it stands, the privacy concerns of product tracking through RFID tags have not been overcome.

Works Cited

Albrecht, Katherine. “Gillette Reverses Position on RFID Spy Chips at Mach 3 Speed.” C.A.S.P.I.A.N. 19 August 2003. http://www.nocards.org/press/pressrelease08-19-03.shtml. 11 November 2003.

Ashton, Kevin. “California State Senate Subcommittee on New Technologies, Hearing on RFID and Privacy, Testimony of Kevin Ashton.” 18 August 2003. http://www.sen.ca.gov/ftp/SEN/COMMITTEE/STANDING/ENERGY/_home/08-18-03auto-id.htm. 12 November 2003

Booth-Thomas, Cathy. “The See-It-All Chip.” Time.com. 22 September 2003. http://www.time.com/time/globalbusiness/printout/0,8816,485764,00.html. 31 October 2003.

Gilbert, Alorie. “Privacy advocates call for RFID regulation.” C|net NEWS.Com 18 August 2003. http://news.com.com/2100-1029_3-5065388.html?tag=st_rn. 30 October 2003.

Granneman, Scott. “RFID Chips Are Here.” SecurityFocus. 26 June 2003 http://www.securityfocus.com/columnists/169. 30 October 2003

“Group Proposes RFID Privacy Law.” RFID Journal. 18 June 2003. http://www.rfidjournal.com/article/articleprint/466/-1/1/. 19 November 2003

“Ports to Adopt RFID Security System.” RFID Journal. 17 July 2002. http://www.rfidjournal.com/article/view/26. 30 October 2003.

Sarma, Sanja E., Stephen A. Weis, and Daniel W. Engels. “RFID Systems and Security and Privacy Implications.” Auto-ID Center. 1 November 2002. http://www.autoidlabs.org/. Path:White Papers; Title “RFID Systems, Security & Privacy Implications.” 5 December 2003.

ZebraRFIDtransponders.jpg. Image. ScanPlanet.com. http://www.scanplanet.com/solutions/RFID.asp 05 December 2003.

Thomas, Daniel. “IT Management: Enterprise & Supply Chain.” ComputerWeekly.com. 4 November 2003. http://www.computerweekly.co.uk/Article126136.htm. 10 November 2003. (This is a very slow website, and takes time to come up.)

Vance, Ashlee. “Wal-Mart turns customers into RFID lab rats.” The Register. 13 November 2003. http://theregister.co.uk/content/5/33982.html. 18 November 2003.

"Wal-Mart Opts for EPC Class 1, V2." RFID Journal. 5 November 2003. http://www.rfidjournal.com/article/articleprint/641/-1/1/. 12 Nov 2003.