10 page(s) will be printed. Back

Record: 1

Title: RFID: A Key to Automating Everything.

Author(s): Want, Roy

Source: Scientific American; Jan2004, Vol. 290 Issue 1, p56, 10p, 3 diagrams, 3c

Document Type: Article

Subject(s): AUTOMATION
TECHNOLOGICAL innovations
ELECTRONICS
INTEGRATED circuits
AUTOMOBILE industry & trade
MOBILE communication systems
WEISER, Mark
ELECTRONIC digital computers
EMBEDDED computer systems
RADIO frequency identification systems

Abstract: Already common in security systems and tollbooths, radio-frequency identification tags and readers stand poised to take over many processes now accomplished by human toil. Thirteen years ago, in an article for Scientific American, the late Mark Weiser, then my colleague at Xerox PARC, outlined his bold vision of" ubiquitous computing": small computers would be embedded in everyday objects all around us and, using wireless connections, would respond to our presence, desires and needs without being actively manipulated. Weiser called such systems "calm technology," because they would make it easier for us to focus on our work and other activities, instead of demanding that we interact with and control them, as the typical PC does today. Today systems based on radio-frequency identification (RFID) technology are helping to move Weiser's vision closer to reality. The responsive RFID home--and conference room, office building and car--are still far away, but RFID technology is already in limited use. But the RFID revolution is not without a downside: the technology's growth raises important social issues, and as RFID systems proliferate, we will be forced to address new problems related to privacy, law and ethics. INSETS: Dealing with the Darker Side; Technical Challenges Ahead.

Full Text Word Count: 5670

ISSN: 0036-8733

Accession Number: ***11637793***

Database: Academic Search Elite

RFID: A Key to Automating Everything

Already common in security systems and tollbooths, radio-frequency identification tags and readers stand poised to take over many processes now accomplished by human toil

Thirteen years ago, in an article for SCIENTIFIC AMERICAN, the late Mark Weiser, then my colleague at Xerox PARC, outlined his bold vision of "ubiquitous computing": small computers would be embedded in everyday objects all around us and, using wireless connections, would respond to our presence, desires and needs without being actively manipulated. This network of mobile and fixed devices would do things for us automatically and so

invisibly that we would notice only their effects. Weiser called such systems "calm technology," because they would make it easier for us to focus on our work and other activities, instead of demanding that we interact with and control them, as the typical PC does today.

In a home equipped with this kind of technology, readers strategically placed in the bedroom, the bathroom door frame, the stairwell and the refrigerator would detect the identifying data in microchip tags sewn into your clothes and embedded in the packaging of foods and send the data to a home computer, which would take action based on that information.

The computer would notice as you got out of bed in the morning and would switch on the coffeemaker. As you entered the bathroom, the shower would come on, adjusted to your favorite temperature. When you started down the stairs, the preloaded toaster would heat up so that your breakfast would be done just the way you like it. When you opened the refrigerator, the appliance would remind you that you were out of milk and that the tub of coleslaw inside had passed its expiration date and should be thrown out.

Today systems based on radio-frequency identification (RFID) technology are helping to move Weiser's vision closer to reality. These systems consist of tags (small silicon chips that contain identifying data and sometimes other information) and of readers that automatically receive and decode that data.

The responsive RFID home--and conference room, office building and car--are still far away, but RFID technology is already in limited use. The tags, often as small as a grain of rice, now hide in ID cards and wristbands, windshield-mounted toll tags, gasoline quick-purchase tokens, and electronic ear tags for livestock, and they have begun to appear in auto key-chain antitheft devices, toys (Hasbro Star Wars figures) and other products. They have also timed runners in road races, and last year a company in Mexico began a service to implant tags under the skin of children as an antikidnapping measure.

In the near term, RFID tags will probably be found in airline luggage labels (British Airways has conducted extensive trials), and they may eventually be embedded in paper currency to inhibit counterfeiters and enable governments to track the movement of cash. (Hitachi in Japan recently announced that it has developed tags minute enough for this application.) Meanwhile the retail, security, transportation, manufacturing and shipping industries are all testing or starting to implement sophisticated RFID applications.

But the RFID revolution is not without a downside: the technology's growth raises important social issues, and as RFID systems proliferate, we will be forced to address new problems related to privacy, law and ethics. Controversy has already erupted: in mid-2003 two major retailers--Wal-Mart in the U.S. and the international clothing maker Benetton--canceled large-scale tests of in-store RFID-centered inventory control systems apparently partly as a response to public reactions that raised the specter of wholesale monitoring of citizens through tags embedded in consumer products.

The Inside Story

RFID technology is based on the simple idea that an electronic circuit in an unpowered, or "passive," tag--which requires no batteries or maintenance--can be intermittently powered from a distance by a reader device that broadcasts energy to it. So powered, the tag exchanges information with the reader. Tags essentially consist of a plain antenna bonded to a silicon chip and encapsulated inside a glass or plastic module.

Tags operate differently depending on several factors, especially the frequency at which they function. Initially RFID tags worked only at frequency bands of 13.56 megahertz or lower. Such tags, which are still the most widely used, typically need to be less than a meter away from a reader and offer poor discrimination (a reader cannot quickly interpret a multitude of individual tags grouped closely together).

More sophisticated, higher-frequency tags now enable a reader to quickly identify many individual tags grouped together, even haphazardly--although they are not yet able to distinguish perfectly among all the items in a loaded grocery cart. (The ability to swiftly and reliably scan a shopping cart full of jumbled, closely spaced RFID-tagged items is a major aim of this technology. Once perfected, such RFID scanning should streamline inventory and checkout procedures and save millions of dollars for retailers.)

The higher-frequency tags can potentially be read from much greater distances than their lower-frequency counterparts, although so far their range has been extended only to a few meters (largely because of tag electronics that operate at very low power derived from the reader's signal, improved antennas and inexpensive high-sensitivity receivers). The updated tags can also hold significantly, more information than earlier models, which allows manufacturers to incorporate useful data beyond a mere ID code. The tags can, for instance, use the energy they capture to power an onboard sensor. Tags with sensors that assess tire pressure and temperature while a vehicle is in motion are already in some cars, and Michelin, Philips Semiconductor and BMW are developing prototypes for the mass market.

RFID Now

RFID devices are beginning to replace magnetic-stripe security cards for unlocking doors and granting access to secured areas--especially at facilities with special security needs, such as military installations. The most visible use of RFID, though, is probably the automatic toll-payment systems that rely on readers at toll plazas to scan tags attached to the windshields of passing cars. The reader records the tag's ID and then deducts money from a prepaid account. These systems are designed to allow cars to zip through toll plazas ideally without stopping or even slowing down very much.

Known as E-ZPass in New York, New Jersey, Delaware and other states, as FasTrak in California, and by different names elsewhere, RFID-based automatic toll systems have been operating for several years. FasTrak, in place on the San Francisco Bay Bridge and on Interstate Highway 15 near San Diego, has been quite successful, but the East Coast E-ZPass system had some early teething problems related to administrative and political issues, not to the technology itself. The San Francisco Bay Bridge system requires drivers to slow to 25 miles per hour while passing the reader, but only for safety reasons, because the tollbooths are narrow. The FasTrak system on 1-15, however, operates at freeway speeds and, further, is being used to monitor traffic.

RFID systems are also in the early stages of replacing those familiar Universal Product Code (UPC) bar codes, which are read optically at very short distances to identify products, track inventory and semiautomatize the checkout process at stores. RFID tags, unlike bar codes, can be molded into a product's casing and can use encryption and other strategies to make them difficult to forge. In addition, some RFID tags permit readers to write new data to their onboard memories for later retrieval. For example, each transaction between reader and tag can record the time, date and identity of whoever accessed the tag. This capability should be useful for creating an audit trail in a tag attached to, say, a car, to indicate where it was manufactured and to record each time it was sold, its previous owners, its service history and its accidents.

Based on the growing number of business sectors that are beginning to test tag-and-reader systems, some experts in the field believe RFID will be widely used, especially in retail, by 2010. Others say such broad application will not happen until around 2015 or later, when the cost of RFID tags falls enough to make them economically viable for labeling inexpensive consumer products.

The, Near Future

RFID tracking technology is starting to be used to follow merchandise as it travels from factory to stores. It will probably be fully established for such applications before it makes deep inroads into stores proper, because warehouse systems are easier to develop and are less likely to fuel public concern that RFID tags in consumer goods could be used to monitor customers once they leave a store. Recently Wal-Mart announced that it will require its top 100 suppliers to place high-frequency tags on cartons and pallets shipped to its stores. And the U.S. Department of Defense has similarly called on its suppliers to adopt high-frequency RFID inventory labeling by 2005.

But the potential--and inevitable--uses for RFID in stores themselves remain tantalizing for retailers. The canceled Wal-Mart in-store test, planned in partnership with Gillette, would have evaluated the ability of RFID-based "smart shelves," equipped with built-in readers, to monitor the movement of millions of shavers and other Gillette products embedded with RFID tags. (In principle, the 96-bit code allotted for identification of each RFID tag would allow every person on earth to have about 50 quadrillion tags apiece.) The ability to keep tabs on individual products on store shelves is generally accepted as the most difficult task for RFID technology--but one that could pay off

royally for retailers.

Notably, RFID smart-shelf systems could save money on labor and help to increase sales by ensuring that shelves are always stocked. If the systems monitored stock levels, employees would not have to do it: when the computers sensed that stock was running low, they could automatically alert someone to order more or could place orders directly with the manufacturer. The systems could offer other benefits as well. Because inventory tags are programmable, their data can include information about where the item was manufactured and sold. And like pinned-on magnetic antishoplifting tags, the RFID inventory tags could be detected leaving the store to prevent theft (estimated to cost $50 billion a year).

Wal-Mart said it canceled its in-store test to free up resources for developing behind-the-scenes RFID capabilities in its warehouses, which will require fewer tags and less powerful computing. This is probably true; industry insiders, however, have suggested that consumer concerns over RFID systems invading individual privacy also played a significant role in the decision. That the backlash had an influence would not be surprising, given that it was at about the same time that Benetton aborted its own large-scale in-store test of an inventory system after its plans were criticized by consumers and the media. The Benetton trial would have examined RFID technology's ability to scan entire cases of tag-bearing clothes in many different colors, sizes and styles and to capture and upload the inventory data to its tracking system, obviating the need for workers to hand-check each garment.

Other tests of warehouse and in-store inventory systems continue, by Procter & Gamble, Canon, and International Paper. And last spring, Metro, a German retail chain, opened a "future store" equipped with an RFID inventory management system involving both smart shelves and scales equipped with RFID readers that can identify types of produce. In addition, tagged shopping carts are scanned to measure in-store customer traffic and to signal automatically for the opening or closing of checkout stations. The Metro pilot is the work of Intel, where I work today, and the German software developer SAP, along with more than 30 other companies, including Hewlett-Packard, Cisco Systems and Philips.

Over the Horizon

RFID inventory systems still fall far short of Weiser's vision: they do not help us perform everyday tasks. Indeed, computers and chips scattered throughout our homes--in toasters, games, entertainment systems and other devicess--demand more, not less, of our attention. We must configure and control dozens of devices, transfer data between them, and try to figure out what went wrong when a failure occurs. Simple tasks, such as setting a wristwatch or operating a television, require an instruction manual. It is clear that for computing to become invisible, we need not only ubiquitous computing but what David L. Tennenhouse of Intel calls "proactive computing"--systems that anticipate what we need and provide it without forcing us to do a lot of work first.

For proactive computing to function on a major scale, networks of RFID readers must be placed throughout the environment. Forward thinkers envision two main types of proactive RFID networks, both of which include a web of interacting readers that monitor many RFID tags and convey the information they collect to remote computers.

One type is made up of readers set permanently in place and connected together by cables. These devices would power and read tags--some with sensors--that are also permanently fixed in place. (If necessary, the tags could also be read by mobile readers passing by.)

This kind of network might be installed on a bridge: tags would be buried deep inside concrete structural members, welded into joints between steel beams and put in other places where their sensors could measure stress and change in various parts of the structure. They would collect and store such information as the discovery that a structural member had been flexed beyond its safe limits during a seismic tremor. The readers would be powered from ordinary AC electric lines or through the interreader network cables and would be hardwired to an Internet connection, so they could send their data to computers that would analyze the input and take action in response.

The second type of system--called an ad hoc wireless network--does not have all its readers and sensor tags permanently in place. Instead it is made up of RFID readers put wherever they are needed, in the same way you would choose a spot to plug in a lamp. They read tags that surround them: some of the tags are fixed and stationary; some have sensors and some do not; and some are mobile, attached to devices and people that pass through the network. Readers may be AC-powered if they are near power outlets or may be battery-powered. These

readers, also known as network nodes, can form short-range wireless connections to one another on the fly: information moves across the network by hopping wirelessly from node to node (which is why these are sometimes called multihop networks) and flows toward a gateway node with an Internet connection.

You might create an ad hoc network with many readers monitoring hundreds of tag sensors spread out across tens of square miles. Such a network could provide the data to make improved weather forecasts. If the sensors could simultaneously detect wind speeds at many locations across the whole area, the computer could even sense the formation of a tornado at an early stage and generate an earlier alert than is possible today.

An ad hoc RFID network in an office building could perform many tasks. Readers could monitor sensor tags that indicate the temperature in different rooms so that the central computer could maintain constant conditions throughout the building or on a single floor. Other readers would scan employees' security badges and recognize the tags in their laptops so that workers could access centrally stored data or link up with colleagues elsewhere in the building. The design of all kinds of sensor networks is being researched by Deborah Estrin's team at the Center for Embedded Networked Sensing at the University of California at Los Angeles, by David E. Culler's team at the University of California at Berkeley, by Gaetano Borriello's team at the University of Washington, at Intel Research's Network of Labs, and at several small companies, including Crossbow in Santa Clara, Calif., Dust Inc. in Berkeley, Calif., and Sensoria in San Diego.

The Responsive Environment

When RFID networks are finally in place everywhere and we are surrounded by tags and readers feeding responsive computer systems, we will have reached the point at which Weiser believed computing could be blended invisibly into everyday tasks. At this level of integration, RFID technology will support even our simplest activities. For example, RFID-enhanced computer products could "talk" to one another and independently configure their connections. My Intel colleague Trevor Pering has been exploring a way to automatically configure wireless network links between mobile computers and peripherals. If you purchased a printer with a wireless networking capability (such as Bluetooth) and an RFID tag, you might simply unpack the device and bring it near your computer: the computer would read the printer's RFID tag and connect to the printer automatically, eliminating messy configuration dialogues.

The scope of possible RFID applications is vast and could even include assisting people with Alzheimer's disease. Eric Dishman, also at Intel, is working on a system aimed at helping those with memory impairment maintain their independence. In one prototype system, all the objects needed for making a cup of tea are tagged. If the patient picks up at least two objects--say, a sugar jar and a tea bag--the system infers, by knowing the ID and location of the objects in relation to one another, that the patient needs help. The system also tracks the sequence in which the objects are used in order to infer whether the person is "stuck" and then delivers recorded voice assistance.

In a totally different realm, PSA Corporation, Hutchinson-Whampoa and P&O Ports--the three largest seaport operators in the world--have taken what could be the early steps toward developing an RFID-based antiterrorism security system that would outfit cargo containers with hidden sensor tags designed to detect radiation or chemical or biological agents in smuggled weapons. Right now the system can detect only whether a container has been opened by an unauthorized person during transit. It could be expanded so that at each stage of a container's journey, from its initial site to ground transportation, dockside storage and transport ships, readers would interrogate the tag to determine if it had detected dangerous materials. The tag's sensor would permanently register even very brief exposures to these substances and flag the incident at the next reading station.

Eventually PDAs (personal digital assistants) could be designed to operate as RFID tag readers so that we could receive proactive assistance from tags placed virtually everywhere in our environment. From a tagged sign on a train station, your PDA could retrieve a Web address linking you to an Internet-based timetable. Similarly, realtors could tag the signs on homes for sale: driving past, you could simply beam your PDA at the realtor's sign and then download photographs and information about the property from the Internet.

Important technical challenges remain, and so it will be years, perhaps decades, before we can reap the benefits of such fully realized RFID applications. As RFID reader-and-tag networks begin appearing in our environment, however, we will increasingly see how this technology can extend the ability of computers--in combination with the Internet--to sense and respond to the physical world.

In his 1991 article in this magazine, Weiser wrote: "There is more information available at our fingertips during a walk in the woods than in any computer system, yet people find a walk among trees relaxing and computers frustrating. Machines that fit the human environment, instead of forcing humans to enter theirs, will make using a computer as refreshing as taking a walk in the woods." Wielded sensibly, RFID has the power to make computing an unobtrusive, intuitive part of everyday life--indeed, as refreshing as a walk through nature.

HOW RFID WORKS

RFID systems operate in both low frequency (less than 100 megahertz) and high frequency (greater than 100 megahertz) modes. Unlike their low-frequency counterparts, high-frequency tags can have their data read at distances of greater than one meter, even while closely spaced together. New data can also be transmitted to the tags, a process not shown here.

LOW-FREQUENCY SYSTEM

1. An integrated circuit sends a signal to an oscillator, which creates an alternating current in the reader's coil.
2. That current, in turn, generates an alternating magnetic field that serves as a power source for the tag.
3. The field interacts with the coil in the tag, which induces a current that causes charge to flow into a capacitor, where it is trapped by the diode.
4. As charge accumulates in the capacitor, the voltage across it also increases and activates the tag's integrated circuit, which then transmits its identifier code.
5. High and low levels of a digital signal, corresponding to the ones and zeros encoding the identifier number, turn a transistor on and off.
6. Variations in the resistance of the circuit, a result of the transistor turning on and off, cause the tag to generate its own varying magnetic field, which interacts with the reader's magnetic field. In this technique, called load modulation, magnetic fluctuations cause changes in current flow from the reader to its coil in the same pattern as the ones and zeros transmitted by the tag.
7. The variations in current flow in the reader coil are sensed by a device that converts this pattern to a digital signal. The reader's integrated circuit then discerns the tag's identifier code.

HIGH-FREQUENCY SYSTEM

1. An integrated circuit sends a digital signal to a transceiver, which generates a radio-frequency signal that is transmitted by a dipole antenna.
2. The electric field of the propagating signal gives rise to a potential difference across the tag's dipole antenna, which causes current to flow into the capacitor; the resulting charge is trapped there by the diode.
3. The voltage across the capacitor turns on the tag's integrated circuit, which sends out its unique identifier code as a series of digital high- and low-voltage levels, corresponding to ones and zeros. The signal moves to the transistor.
4. The transistor gets turned on or off by the highs and lows of the digital signal, alternately causing the antenna to reflect back or absorb some of the incident radio-frequency energy from the reader.
5. The variations in the amplitude of the reflected signal, in what is called backscatter modulation, correspond to the pattern of the transistor turning on and off.
6. The reader's transceiver detects the reflected signals and converts them to a digital signal that is relayed. to the integrated circuit, where the tag's unique identifier is determined.

TRACKING THINGS HERE, THERE AND EVERYWHERE

RFID systems will let products, such as the hypothetical Mama's tomato sauce, be monitored and reordered automatically, once depleted. Even as individual item will be traced. Here is one scenario.

1. An RFID tag gets affixed to each can of Mama's tomato sauce as it passes by on a conveyor belt. A reader detects the tag's unique identifier code and stores it in a list ready to be sent to a central database.

2. A pallet containing boxes loaded with cans of Mama's sauce is prepared for transport.
3. When scanned by the reader at a factory, each box--and each jar in the box responds sequentially with its identifier code. The plant sends lists of codes, both from the conveyor belt and the packed boxes, to an Internet-based computer system (blue arrows), where they are stored in a database that ties each jar, box and pallet to the originating factory.
4. The jar of Mama's and the entire box are detected by a reader at the distribution center. After the manufacturer's computer system is queried about the jar's identity and shipping information, the lot is automatically routed to truck 47 without anyone having to open and inspect the box it is in.
5. The shipment of tomato sauce arrives at the supermarket, where it is automatically added to the store's inventory system. Once the stocks fall below some preset level, the inventory system can relay a message to the manufacturer's computer servers to send more. If a jar is defective or has been tampered with, the inventory system can query the manufacturer's server about which plant produced the product.
6. The customer doesn't have to wait in a checkout line. He or she can get the amount of a purchase totaled by a reader while pushing the cart along an aisle on the way out. A personal digital assistant or another device can list the goods and the total price, and the customer can then press a button that completes the transaction.
7. A reader in the refrigerator--or on a shelf--can tell when the supply of Mama's has been used up and then signal a home personal computer to print a shopping list that includes Mama's for the next trip to the supermarket.
8. Once ajar is discarded, the tag can help the recycling center sort it into the proper category.

TAG NUMBER IS 9908 GGH76.

JAR OF TO/VIA TO SAUCE SHIPPED FROM ELIZABETH, N.J.

FIRST DESTINATION: QUIK-EE

FINAL DESTINATION: QUIK MARTS

Overview/RFID Technology

. RFID systems consist of tags--chips that contain identifying and often other data--and reading devices that convey information from the tags to computers.

. Such systems are already in limited use and are being tested widely for applications involving the tracking of inventory from manufacturers to stores.

. As the technology improves and its costs fall, it could form the core of networks that will handle many activities, from monitoring the structural integrity of bridges to reminding you that the tub of coleslaw in the fridge is past its due date.

. Privacy advocates worry that RFID systems will give marketers and others access to more personal information than individuals would want them to have.

MORE TO EXPLORE

The Computer for the 21st Century. Mark Weiser in Scientific American, Vol. 265, No. 3, pages 94-104; September 1991.

Ubiquitous Electronic Tagging. Roy Want and Dan M. Russell in IEEE Distributed Systems Online, Vol. 1, No. 2; September 2000.

Connecting the Physical World with Pervasive Networks. Deborah Estrin, David Culler, Kris Pister and Gaurav Sukhatme in IEEE Pervasive Computing, Vol. 1, No. 1, pages 59-69; January-March 2002.

Comparing Autonomic and Proactive Computing. Roy Want, Trevor Pering and David Tennenhouse in IBM

Systems Journal, Vol. 42, No. 1, pages 129-135; January 2003.

The RFID Handbook. Klaus Finkenzeller. John Wiley & Sons, 2003.

PHOTO (COLOR): TALK TO ME: When interrogated by computer-controlled readers, widely dispersed RFID tags (highlighted) could indicate, for instance, that a bread bag has been thrown into the garbage and you need a new loaf.

DIAGRAM: LOW-FREQUENCY SYSTEM

DIAGRAM: HIGH-FREQUENCY SYSTEM

DIAGRAM

~~~~~~~~

By Roy Want

ROY WANT is a principal engineer at Intel Research/CTG in Santa Clara, Calif., where he leads a project that is setting a long-range research agenda for ubiquitous computing. Early in his career, at Olivetti Research, Want pursued an automated system for locating people inside buildings. At Xerox PARC's Ubiquitous Computing Program, he headed the development of one of the first context-aware computer systems, managed the Embedded Systems group, and worked on applications of electronic tagging and on the design of PDAs with manipulative user interfaces. Want holds more than 50 patents related to mobile and distributed computer systems and is associate editor in chief of IEEE Pervasive Computing.

Dealing with the Darker Side

What will be the social consequences of a world full of embedded RFID tags and readers? Will our privacy be further eroded as RFID technology makes it possible for our movements to be tracked and allows our personal information to be available in unprecedented detail? These and many other questions must be answered before RFID systems become commonplace.

One of the major worries for privacy advocates is that RFID tags identifying individual items purchased with credit or debit cards would link buyers to the specific items in the card's or the store's databases. Marketers could then use these data to keep track of exactly what particular people bought, down to the color, size, style and price--more information than UPC bar codes reveal. In an amplification of the way that phone and direct-mail solicitors use similar, less accurate data to target people for sales pitches, those equipped with RFID-derived data might home in on consumers with very specific sales pitches.

Another concern is that RFID equipment will produce automatic audit trails of commercial transactions: in a totally tagged world, it will be easier to detect when we lie about how we spent our time or what we did and where. This capability could have great consequences for the workplace, and the legal system might look to using logs kept by tag readers as courtroom evidence. We may need laws to specify who can access data logs and for what purpose. In Europe, the Data Protection Act already limits access to computer records of this kind, and the U.S. will probably enact similar legislation.

We will also have to grapple with the inevitable displacement of workers by RFID systems. Opposition to tagging could well come from the industrial labor force, which stands to lose significant numbers of jobs as industry adopts RFID tools able to perform tasks that now depend on human effort. A bitter strike by longshoremen on the West Coast in 2002, partial over new technology that threatened future jobs, may have been a preview of conflicts to come over RFID systems.
~~~~~~~~

Privacy Advocates Protest

The backlash against perceived invasions of consumer privacy by RFID applications began in March 2003, when Philips Semiconductor announced that it was shipping 15 million RFID tags to the clothing manufacturer and retailer Benetton to be incorporated into labels during production. The tags were to interact with a network of RFID readers in Benetton's store shelves and warehouses to track inventory throughout the company's 5,000 retail outlets worldwide.

Despite Philips's reassurances that tagged clothing could not be tracked outside Benetton stores, some industry experts said that criminals could increase the Benetton tags' tracking distance by creating more sensitive RFID readers. Privacy advocates worried that the tags could be scanned by RFID readers other than those in Benetton stores, which would allow people wearing the clothes to be monitored without their knowledge by, say, criminals or the government. Consumers Against Supermarket Privacy Invasion and Numbering, a U.S.-based privacy group, called for a worldwide boycott of Benetton until the company abandoned RFID tracking technology. Benetton quickly issued statements saying that although it had already tested RFID systems, it was not using RFID inventory tracking and had no firm plans to insert the millions of Philips tags into its products.

Similar concerns--that corporations might keep consumers' products under surveillance in purchasers' homes and on the streets--surfaced about a test of an in-store RFID inventory system that was planned by Wal-Mart and Gillette. To answer consumer concern, Gillette announced that it was embedding its RFID tags in packaging, not products, so purchasers would discard the tags with the packaging. But Declan McCullagh, a commentator who writes for computing publications and who favors RFID for its practical value, has written: "Future burglars could canvass alleys with RFID detectors, looking for RFID tags on discarded packaging that indicates expensive electronic gear is nearby.... [T]he ability to remain anonymous is eroded."

One way to avoid such possibilities is to put a kill switch into each RFID tag on a consumer item, which would allow the tag to be turned off after purchase. Indeed, the Auto-ID Center--a research consortium funded by information technology companies and headquartered at the Massachusetts Institute of Technology--has released guidelines saying that retailers must be able to disable RFID tags at checkout counters, and manufacturers, including Alien Technology, Matrics and Philips, are now producing tags with kill switches.

McCullagh has suggested four requirements for the use of RFID tags on consumer products: Consumers should be notified when RFID tags are present in what they are buying (this could be done with a printed notice on a checkout receipt). All tags should be readily visible and easily removable. The tags should be disabled by default at the checkout counter. And, when possible, RFID tags should be placed only on the product's packaging, not embedded in the product.

PHOTO (COLOR): PROTEST ENSUED when the British supermarket chain Tesco began testing RFID technology.

Technical Challenges Ahead

. RFID tags and readers are orientation-dependent. Tags must be positioned properly relative to readers so that the antenna coils can exchange signals. The solution to this problem will come with the development of multiple-reader systems that use an array of readers positioned to cover all the possible orientations for tagged items that might, for example, be found in a display bin in a store. Part of this solution will involve protocols to coordinate the operation of these reader arrays.

. RFID signals are easily blocked. Over short ranges, these signals can be attenuated by certain materials (the most common is packing made from metallic substances). Over longer ranges, the signals--which are much weaker than commercial radio broadcast signals--can be blocked by common objects, including the

human body. Researchers are working to solve this problem by using novel designs for tag antennas and more sensitive reader arrays.

. At an average cost of around 20 to 30 cents apiece, RFID tags are still too costly, especially for retail applications and certainly for use on inexpensive and low-margin products, such as a 50-cent candy bar or a $1 bar of soap. This is a key reason why mass-market consumer retail businesses--which operate on very thin profit margins--have been slow to adopt RFID-based smart shelf and smart checkout technology. RFID tag developers are working to lower the cost of tags to 10 cents, or even five cents, over the next few years. Some experts in the tag-manufacturing field believe that at these costs, RFID may not be widely adopted until at least 2010--if ever. Others say the cost must shrink to a fraction of a cent before we will see a tag on every item in the grocery store, which may take until 2015 or later.

. Competing technical standards for RFID readers and tags prevent their universal adoption. Different manufacturers are developing tag protocols operating at different frequencies with a variety of packet formats--the way in which a tag's digital data are packaged and transmitted to a reader. Ideally, a single standard should be adopted to make all tags compatible with all readers.

. Both the cost and standardization challenges are being addressed by individual companies and by the Auto-ID Center and the International Organization for Standardization (ISO), industry consortia working to set standards for RFID tags.

PHOTO (COLOR): DIVERSITY of RFID tags reflects the lack of standards for the technology.

Source: Scientific American, Jan2004, Vol. 290 Issue 1, p56, 10p
Item: 11637793