washingtonpost.com

Microchips Everywhere: a Future Vision

By TODD LEWAN
The Associated Press
Saturday, January 26, 2008; 12:16 PM

-- Here's a vision of the not-so-distant future:

_Microchips with antennas will be embedded in virtually

everything you buy, wear, drive and read, allowing retailers and law enforcement to track consumer items _ and, by extension, consumers _ wherever they go, from a distance.

_A seamless, global network of electronic "sniffers" will scan radio tags in myriad public settings, identifying people and their tastes instantly so that customized ads, "live spam," may be beamed at them.

_In "Smart Homes," sensors built into walls, floors and appliances will inventory possessions, record eating habits, monitor medicine cabinets _ all the while, silently reporting data to marketers eager for a peek into the occupants' private lives.

Science fiction?

In truth, much of the radio frequency identification technology that enables objects and people to be tagged and tracked wirelessly already exists _ and new and potentially intrusive uses of it are being patented, perfected and deployed.

Some of the world's largest corporations are vested in the success of RFID technology, which couples highly miniaturized computers with radio antennas to broadcast information about sales and buyers to company databases.

Already, microchips are turning up in some computer printers, car keys and tires, on shampoo bottles and department store clothing tags. They're also in library books and "contactless" payment cards (such as American Express' "Blue" and ExxonMobil's "Speedpass.")

Companies say the RFID tags improve supply-chain efficiency, cut theft, and guarantee that brand-name products are authentic, not counterfeit. At a store, RFID doorways could scan your purchases automatically as you leave, eliminating tedious checkouts.

At home, convenience is a selling point: RFID-enabled refrigerators could warn about expired milk, generate weekly shopping lists, even send signals to your interactive TV, so that you see "personalized" commercials for foods you have a history of buying. Sniffers in your microwave might read a chip-equipped TV dinner and cook it without instruction.

"We've seen so many different uses of the technology," says Dan Mullen, president of AIM Global, a national association of data collection businesses, including RFID, "and we're probably still just scratching the surface in terms of places RFID can be used."

The problem, critics say, is that microchipped products might very well do a whole lot more.

With tags in so many objects, relaying information to databases that can be linked to credit and bank cards, almost no aspect of life may soon be safe from the prying eyes of corporations and governments, says Mark Rasch, former head of the computer-crime unit of the U.S. Justice Department.

By placing sniffers in strategic areas, companies can invisibly "rifle through people's pockets, purses, suitcases, briefcases, luggage _ and possibly their kitchens and bedrooms _ anytime of the day or night," says Rasch, now managing director of technology at FTI Consulting Inc., a Baltimore-based company.

In an RFID world, "You've got the possibility of unauthorized people learning stuff about who you are, what you've bought, how and where you've bought it ... It's like saying, 'Well, who wants to look through my medicine cabinet?'"

He imagines a time when anyone from police to identity thieves to stalkers might scan locked car trunks, garages or home offices from a distance. "Think of it as a high-tech form of Dumpster diving," says Rasch, who's also concerned about data gathered by "spy" appliances in the home.

"It's going to be used in unintended ways by third parties _ not just the government, but private investigators, marketers, lawyers building a case against you ..."

___

Presently, the radio tag most commercialized in America is the so-called "passive" emitter, meaning it has no internal power supply. Only when a reader powers these tags with a squirt of electrons do they broadcast their signal, indiscriminately, within a range of a few inches to 20 feet.

Not as common, but increasing in use, are "active" tags, which have internal batteries and can transmit signals, continuously, as far as low-orbiting satellites. Active tags pay tolls as motorists to zip through tollgates; they also track wildlife, such as sea lions.

Retailers and manufacturers want to use passive tags to replace the bar code, for tracking inventory. These radio tags transmit Electronic Product Codes, number strings that allow trillons of objects to be uniquely identified. Some transmit specifics about the item, such as price, though not the name of the buyer.

However, "once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile," the U.S. Government Accountability Office concluded in a 2005 report on RFID.

Federal agencies and law enforcement already buy information about individuals from commercial data brokers, companies that compile computer dossiers on millions of individuals from public records, credit applications and many other sources, then offer summaries for sale. These brokers, unlike credit bureaus, aren't subject to provisions of the Fair Credit Reporting Act of 1970, which gives consumers the right to correct errors and block access to their personal records.

That, and the ever-increasing volume of data collected on consumers, is worrisome, says Mike Hrabik, chief technology officer at Solutionary, a computer-security firm in Bethesda, Md. "Are companies using that information incorrectly, and are they giving it out inappropriately? I'm sure that's happening. Should we be concerned? Yes."

Even some industry proponents recognize risks. Elliott Maxwell, a research fellow at Pennsylvania State University who serves as a policy adviser to EPCglobal, the industry's standard-setting group, says data broadcast by microchips can easily be intercepted, and misused, by high-tech thieves.

As RFID goes mainstream and the range of readers increases, it will be "difficult to know who is gathering what data, who has access to it, what is being done with it, and who should be held responsible for it," Maxwell wrote in RFID Journal, an industry publication.

The recent growth of the RFID industry has been staggering: From 1955 to 2005, cumulative sales of radio tags totaled 2.4 billion; last year alone, 2.24 billion tags were sold worldwide, and analysts project that by 2017 cumulative sales will top 1 trillion _ generating more than $25 billion in annual revenues for the industry.

Heady forecasts like these energize chip proponents, who insist that RFID will result in enormous savings for businesses. Each year, retailers lose $57 billion from administrative failures, supplier fraud and employee theft, according to a recent survey of 820 retailers by Checkpoint Systems, an RFID manufacturer that specializes in store security devices.

Privacy concerns, some RFID supporters say, are overblown. One, Mark Roberti, editor of RFID Journal, says the notion

that businesses would conspire to create high-resolution portraits of people is "simply silly."

Corporations know Americans are sensitive about their privacy, he says, and are careful not to alienate consumers by violating it. Besides, "All companies keep their customer data close to the vest ... There's absolutely no value in sharing it. Zero."

Industry officials, too, insist that addressing privacy concerns is paramount. As American Express spokeswoman Judy Tenzer says, "Security and privacy are a top priority for American Express in everything we do."

But industry documents suggest a different line of thinking, privacy experts say.

A 2005 patent application by American Express itself describes how RFID-embedded objects carried by shoppers could emit "identification signals" when queried by electronic "consumer trackers." The system could identify people, record their movements, and send them video ads that might offer "incentives" or "even the emission of a scent."

RFID readers could be placed in public venues, including "a common area of a school, shopping center, bus station or other place of public accommodation," according to the application, which is still pending _ and which is not alone.

In 2006, IBM
received patent approval for an invention it called, "Identification and tracking of persons using RFID-tagged items." One stated purpose: To collect information about people that could be "used to monitor the movement of the person through the store or other areas."

Once somebody enters a store, a sniffer "scans all identifiable RFID tags carried on the person," and correlates the tag information with sales records to determine the individual's "exact identity." A device known as a "person tracking unit" then assigns a tracking number to the shopper "to monitor the movement of the person through the store or other areas."

But as the patent makes clear, IBM's invention could work in other public places, "such as shopping malls, airports, train stations, bus stations, elevators, trains, airplanes, restrooms, sports arenas, libraries, theaters, museums, etc." (RFID could even help "follow a particular crime suspect through public areas.")

Another patent, obtained in 2003 by NCR Corp., details how camouflaged sensors and cameras would record customers' wanderings through a store, film their facial expressions at displays, and time _ to the second _ how long shoppers hold and study items.

Why? Such monitoring "allows one to draw valuable inferences about the behavior of large numbers of shoppers," the patent states.

Then there's a 2001 patent application by Procter & Gamble, "Systems and methods for tracking consumers in a store environment." This one lays out an idea to use heat sensors to track and record "where a consumer is looking, i.e., which way she is facing, whether she is bending over or crouching down to look at a lower shelf."

The system could space sensors 8 feet apart, in ceilings, floors, shelving and displays, so they could capture signals transmitted every 1.5 seconds by microchipped shopping carts.

The documents "raise the hair on the back of your neck," says Liz McIntyre, co-author of "Spychips," a book that is critical of the industry. "The industry has long promised it would never use this technology to track people. But these patent records clearly suggest otherwise."

Corporations take issue with that, saying that patent filings shouldn't be used to predict a company's actions.

"We file thousands of patents every year, which are designed to protect concepts or ideas," Paul Fox, a spokesman for Procter & Gamble, says. "The reality is that many of those ideas and concepts never see the light of day."

And what of his company's 2001 patent application? "I'm not aware of any plans to use that," Fox says.

Sandy Hughes, P&G's global privacy executive, adds that Procter & Gamble has no intention of using any technologies _ RFID or otherwise _ to track individuals. The idea of the 2001 filing, she says, is to monitor how groups of people react to store displays, "not individual consumers."

NCR and American Express echoed those statements. IBM declined to comment for this story.

"Not every element in a patent filing is necessarily something we would pursue....," says Tenzer, the American Express spokeswoman. "Under no circumstances would we use this technology without a customer's permission."

McIntyre has her doubts.

In the marketing world of today, she says, "data on individual consumers is gold, and the only thing preventing these companies from abusing technologies like RFID to get at that gold is public scrutiny."

___

RFID dates to World War II, when Britain put transponders in Allied aircraft to help radar crews distinguish them from German fighters. In the 1970s, the U.S. government tagged trucks entering and leaving secure facilities such as the Los Alamos National Laboratory, and a decade later, they were used to track livestock and railroad cars.

In 2003, the U.S. Department of Defense and Wal-Mart gave RFID a mammoth push, mandating that suppliers radio tag all crates and cartons. To that point, the cost of tags had simply been too high to make tagging pallets _ let alone individual items _ viable. In 1999, passive tags cost nearly $2 apiece.

Since then, rising demand and production of microchips _ along with technological advances _ have driven tag prices down to a range of 7 to 15 cents. At that price, the technology is "well-suited at a case and pallet level," says Mullen, of the industry group AIM Global.

John Simley, a spokesman for Wal-Mart, says tracking products in real-time helps ensure product freshness and lowers the chances that items will be out of stock. By reducing loss and waste in the supply chain, RFID "allows us to keep our prices that much lower."

Katherine Albrecht, founder of CASPIAN, an anti-RFID group, says, "Nobody cares about radio tags on crates and pallets. But if we don't keep RFID off of individual consumer items, our stores will one day turn into retail 'zoos' where the customer is always on exhibit."

So, how long will it be before you find an RFID tag in your underwear? The industry isn't saying, but some analysts speculate that within a decade tag costs may dip below a penny, the threshold at which nearly everything could be chipped.

To businesses slammed by counterfeiters _ pharmaceuticals, for one _ that's not a bad thing. Sales of fake drugs cost drug makers an estimated $46 billion a year. In 2004, the U.S. Food and Drug Administration recommended that RFID be incorporated throughout the supply chain as a way of making sure consumers get authentic drugs.

In the United States, Pfizer has already begun chipping all 30- and 100-count bottles of Viagra, one of the most counterfeited drugs.

Chips could be embedded in other controlled or potentially dangerous items such as firearms and explosives, to make them easier to track. This was mentioned in IBM's patent documents.

Still, the idea that tiny radio chips might be in their socks and shoes doesn't sit well with Americans. At least, that's what Fleishman-Hillard Inc., a public-relations firm in St. Louis, found in 2001 when it surveyed 317 consumers for the industry.

Seventy-eight percent of those queried reacted negatively to RFID when privacy was raised. "More than half claimed to be extremely or very concerned," the report said, noting that the term "Big Brother" was "used in 15 separate cases to describe the technology."

It also found that people bridled at the idea of having "Smart Tags" in their homes. One surveyed person remarked: "Where money is to be made the privacy of the individual will be compromised."

In 2002, Fleishman-Hillard produced another report for the industry that counseled RFID makers to "convey (the) inevitability of technology," and to develop a plan to "neutralize the opposition," by adopting friendlier names for radio

tags such as "Bar Code II" and "Green Tag."

And in a 2003 report, Helen Duce, the industry's trade group director in Europe, wrote that "the lack of clear benefits to consumers could present a problem in the 'real world,'" particularly if privacy issues were stirred by "negative press coverage."

(Though the reports were marked "Confidential," they were later found archived on an industry trade group's Web site.)

The Duce report's recommendations: Tell consumers that RFID is regulated, that RFID is just a new and improved bar code, and that retailers will announce when an item is radio tagged, and deactivate the tags at check-out upon a customer's request.

Actually, in the United States, RFID is not federally regulated. And while bar codes identify product categories, radio tags carry unique serial numbers that _ when purchased with a credit card, frequent shopper card or contactless card _ can be linked to specific shoppers.

And, unlike bar codes, RFID tags can be read through almost anything except metal and water, without the holder's knowledge.

EPCglobal, the industry's standard-setting body, has issued public policy guidelines that call for retailers to put a thumbnail-sized logo _ "EPC," for Electronic Product Code _ on all radio tagged packaging. The group also suggests that merchants notify shoppers that RFID tags can be removed, discarded or disabled.

Critics say the guidelines are voluntary, vague and don't penalize violators. They want federal and state oversight _ something the industry has vigorously opposed _ particularly after two RFID manufacturers, Checkpoint Systems and Sensormatic, announced last year that they are marketing tags designed to be embedded in such items as shoes.

Marc Rotenberg, executive director of the Electronic Privacy Information Center, says, "I don't think there's any basis ... for consumers to have to think that their clothing is tracking them."

___

On the Web:

http://www.epcglobalinc.org

http://www.spychips.com

http://epic.org/

http://www.idtechex.com/

© 2008 The Associated Press