SIMSON GARFINKEL

THE NET EFFECT

AN RFID BILL OF RIGHTS

Think of it as a bar code for your bra.

Tiny wireless identification tags are soon going to start showing up throughout your daily life. If you have an E-ZPass transponder in your car or one of several Swatch watches on your wrist, you're already carrying a wireless tag. Your house, your food and even your clothes might someday be permeated with such tags, which can be read without your permission or knowledge.

Think I'm crazy? Last November, Texas Instruments and the Gap announced that they had completed a three-month test in which every piece of denim in a store in Atlanta received a wireless ID tag. This technology, boasts TI, allows each item of clothing to be tracked from the warehouse to the shelf to the checkout counter. Some of the largest retailers and consumer products firms, including Coca-Cola, Home Depot, Procter and Gamble and Wal-Mart, have joined to create standards to make sure that future tags and readers will all be compatible. That work is being done at the MIT-based Auto-ID Center.

By themselves, these tags seem harmless enough. Hit one with a radio beam at the right frequency, and it spurts out its unique serial number; that's why they're known as radio frequency identification (RFID) tags. E-ZPass uses the serial number to debit a driver's account when he or she passes through a tollbooth; companies like the Gap and Coca-Cola will use it to track inventory. Many animal shelters now have devices to look for tags implanted in lost household pets, speeding their return to their owners. Ranchers track cattle by implanting tags in the animals' ears. Futurists say that one day we might have houses filled with RFID readers and use them to find lost glasses, key chains and other tagged items.

The first mass application for these radio-read tags, however, will be inventory management and control. Playtex might put a tag in each bra to make sure that shipments destined for Asia aren't diverted to New York, where consumers are likely to pay more. Pass a reader over a box of bras and every undergarment will sing back its serial number. This allows for more accurate inventory control than tracking boxes does; individually serialized garments also make it dramatically harder for corrupt employees at a warehouse or trucking company to make a few bras "disappear," since automated readers will continually log the whereabouts of every item.

To increase public acceptance, the companies backing wireless ID systems are touting potential consumer benefits. A reader built into your washing machine, for instance, might automatically warn you that the dyes in your red shorts aren't colorfast and will ruin your yellow blouse. Microwave ovens might read the tags in frozen-dinner packages and automatically calibrate to cook your food properly. Already under development is tag-embedded meat packaging, which could help trace the spread of *E. coli* and other food-borne contaminants.

But it's easy to see how this technology could be misused. A woman I met at a privacy conference told me she didn't want a man standing next to her to be able to learn the make and size of her bra using a handheld reader hidden in his pocket. (Such readers already exist.) Others fear that implanted chips might one day be required for people, the way some cities now require them for pets. Some nursing homes are already giving their patients RFID bracelets; in Florida this past May, a family and, separately, an 82-year-old man voluntarily had the chips implanted to help identify them in case of emergency.

The likely proliferation of these devices has spurred me to come up with this RFID Bill of Rights. Consumers should have

- The right to know whether products contain RFID tags.
- The right to have RFID tags removed or deactivated when they purchase products.
- The right to use RFID-enabled services without RFID tags.

Your house, your food and even your clothes might someday be permeated with wireless ID tags, which can be read without your permission. It's easy to see how this technology could be misused.

- The right to access an RFID tag's stored data.
- The right to know when, where and why the tags are being read.

I see these not necessarily as the basis for new law, but as a framework for voluntary guidelines that companies wishing to deploy this technology can publicly adopt. Consumers could then boycott companies that violate these principles.

Of course, some of these "rights" could easily be curbed or otherwise limited by federal regulation. For example, the U.S. Department of Transportation could require certain safety-critical parts inside a car to have radio tags to aid in recalls. But for the overwhelming majority of applications, these rights make sense. Manufacturers have no business playing hide-and-seek with radio tags when consumer privacy is at issue. Likewise, they shouldn't be able to require that consumers choose between participating in tomorrow's economy and preserving their privacy. For example, this spring the Massachusetts Turnpike Authority started giving discounts to state residents who pay tolls with electronic transponders—a policy that is both discriminatory and coercive.

RFID is moving slowly enough that we citizens can still influence the way it will be deployed. But we will lose this chance if we do not make our voices heard soon.

Editor's note: Simson Garfinkel, now a graduate student at MIT, plans to work with the Auto-ID center on privacy issues.