

www.futurebrief.com

Tag, You're It.

Jeffrey R. Harrow
Principal Technologist, The Harrow Group

[\(download PDF version\)](#)
[\(read his bio\)](#)

I'm beginning to feel like a broken record (uh, I guess I'd better change that to 'scratched audio CD') as we continue to recognize the growing number of technological innovations that certainly confer benefits, but also raise the very real specter of making "privacy" a thing of the past.

The (sometimes) unfortunate reality is that technology is continuing the double-exponential growth that we tend to think of as a generalized "Moore's Law" (Intel's Gordon Moore's 35+ year old, and still going strong, prediction that the number of transistors will double in the same space, and at the same cost, every 18 months). While this has driven the technology that now pervades our society, it also presents opportunities for using a growing number of innovations in ways that, often unintentionally, drive another chink into the walls of privacy. Let's explore several related recent events.

Talking Trash.

First, according to the Feb. 11, 2005 [The Guardian](#), the London town of Croydon is marrying the plebian trash pickup bin with what appears to be a variant of RFID chips; each remotely readable tag uniquely associates each bin with its owner's address. This will, initially, allow garbage trucks to wirelessly and automatically keep track of which bins have been left out with trash, and by extension it will identify which homes have been skipped over on a given day.

This would seem to be a benign way to keep good records that will help plan for future trash system expansion, but it also makes it easy for the local government to track just how much trash each household is generating. While many might pooh-pooh this as ancillary information that would never be of value or a privacy concern, it seems that this system *is indeed intended* to notice the top trash producers, and send officials to their homes to advise them on how to "...*manage their rubbish more effectively.*"

Another concern, brought up by London Assemblyman Andrew Pelling, is that:

"If, for example, computer hackers broke in to the system, they could see sudden reductions in waste in specific households, suggesting the owners were on holiday and the house vacant."

Given the generally poor protection of online data, I see this as one very real risk. Other risks include similar exposure from Internet-accessible electricity meters, water meters, and more...

The 'ID' That Keeps On Giving...

Another interesting development in this area of "marking" things is a technology from [SmartWater](#). They have developed a method of encoding synthetic DNA into liquids and other materials by using "tiny metal fragments" that uniquely identify each item. While this may not sound particularly

www.futurebrief.com

interesting at first, a range of products containing SmartWater marks are already helping to identify most anything that we can image.

For example, "SmartWater 'Tracer'" is designed as a liquid that *"is practically impossible to remove entirely."* It can be brushed or sprayed onto anything, such as home stereo equipment, jewelry, currency, and the like, and if the items are stolen a reader can positively identify their owner.

In a similar vein, "SmartWater SuperLabel" embeds the identifying codes into the adhesive that sticks those maddeningly difficult to remove price tags to store merchandise. Now, even if someone does manage to completely remove the sticker and replace it with another one (displaying a lower price), the slightest remainder of the original encoded adhesive will tell the tale of who did what to whom.

We can surely think of many beneficial uses for such a product in preventing or dealing with criminal activity. Imagine, if you will, a "burglar alarm" (or bank teller window or bank money bag, etc.) that along with sounding an alarm, also mists the air with some of this tagged water. If and when the police catch up with a suspect, the presence of the uniquely addressed chemical tags could provide compelling evidence that the suspect was indeed (or was not) at the scene of the crime. But it's also easy to envision how the benign and legal actions of ordinary people might also be traced...

For another example, this described in the Feb. 15, 2005 [Wired](#), imagine how a new kind of Valentine's Day card might transfer especially long-lived markers to someone's fingers as they read the card; their fingers would then mark anything they touched for months come!

While this sounds improbable, it's not science fiction at all. Vicki Marr, Chief Superintendent of the London police force has *already* sent just such cards to many of Croydon's most notorious criminals:

"Marr sent her valentine -- reading "roses are red, violets are blue, when SmartWater's activated, it's over for you" -- to known criminals in Croydon, reinforcing the message in what [SmartWater CEO Phil] Cleary said amounts to "psychological warfare" against burglars."

While clearly useful in this and many other regards, such marking would certainly also be open to abuse.

New-Age Passports, And...

New U.S. passports, and those of countries whose citizens do not require visas to enter the U.S., are due to get their very own RFID chips. By 2006 the U.S. plans to embed these chips in all new passports, which will wirelessly transmit typical personal passport information PLUS some biometric information such as a ["digital face recognition template."](#)

A major problem with this, as I see it, is that much of this wirelessly readable information will NOT be encrypted! This means that anyone who can read the passport's chip (which is, after all, a "radio" device) will easily be able to access this very personal information. Although RFID tags are intended to be read from only a few inches or feet away, this does not impose the protections that most people expect (see below.)

www.futurebrief.com

Another variation, the "liquid RFID chipless chip," comes from [CrossID](#) whose Micha Shafir sent me a video demonstrating how, if their technique was used by a country to tag each piece of its paper currency, law enforcement agencies would easily be able to enforce regulations on the amount of money that can be taken out of or brought into their country. Consider that if the ubiquitous airport metal detectors were also equipped with RFID readers attuned to the liquid RFID tags in each bill (which could identify its denomination and perhaps its serial number), then if anyone carried more than \$10,000 in cash (the U.S. "undeclared limit") through the gateway an alarm would sound leading to a through search.

Such ideas certainly have their positive uses in enforcing laws (it's getting harder for an honest criminal to make his or her living... J), but one downside is that any RF ("radio") accessible information *IS* susceptible to unauthorized access. Imagine someone sitting in an airport parking lot and electronically watching (and recording) all of the passport information from travelers. Or imagine someone on a busy street monitoring the amount of cash that people are carrying so that they can choose the best victim for pickpocketing or mugging...

I know - this all sounds very improbable. But we're about to find out realistic these concerns *already are!*

From A Distance?

One of the "safeguards" touted for items with embedded RFID and other wirelessly accessible information devices is that they are designed to work only within a very limited distance, thereby preserving privacy by only giving up their bounty near a reader. But do you remember the days of the "yagi" VHF/UHF TV antennas that adorned almost every building?



These highly directional antennas (often mounted on a "rotor" that could be controlled from inside) would point towards distant TV transmitters and "focus" on that signal to the exclusion of others, thereby delivering a stronger signal, from farther away, than a more omnidirectional "simple" antenna.

Fortunately or unfortunately, as we choose to look at it, this principal applies to almost any radio signal, including those used by popular wireless computer networks such as WiFi (802.11 and its variations). It's not hard for someone to construct (such as this one made from, yes, a Pringles can),



or to purchase an antenna (such as this one from RadioLabs CNC)



that will allow them to access, or listen-in on our WiFi networks from quite a distance away.

Nor is the relatively new Bluetooth radio technology immune even as it's increasingly being used to connect wireless headsets to cell phones and PDAs and perhaps to music players. Bluetooth is also connecting keyboards to computers, and printers to many of those items as well as to cameras (such as the Nikon D2Hs). While extremely useful (I've always hated the cord between my "handsfree" headset and my cell phone), Bluetooth's intended ten to thirty foot range can also be dramatically extended to "*hundreds of meters*" by commercial and homebrew Bluetooth antennas, such as this one demonstrated at the recent RSA Conference 2005.



According to John Hering, one of the "gun's" inventors,

"We can remotely log keystrokes from the keyboards and we can record a WAV file from a phone conversation."

Yes, From A Distance!

It now seems clear that long range access to any of our wireless signals is fairly trivial. So if the wireless devices we use do not incorporate reasonably good encryption on their radio links (many WiFi systems don't use any by default, and encryption is not part of most Bluetooth implementations), then everything we type, and all the data we send and receive including account

www.futurebrief.com

numbers and passwords, and everything we say over our cell phones, could show up on a wireless voyeur's system with potentially nasty results.

Needless to say, unencrypted RFID chips, wherever they may be, are also targets of opportunity to similar "long distance" browsing regardless of their advertised "short distance" limitations.

Privacy Sneaks.

Some elements of giving up privacy happen in the open, such as from legislation passed after Sept. 11 and the knowledge that our cell phone, even if not in use, leave movement tracks within the cell company's computers. But other dilutions of privacy, such as unencrypted (or insufficiently encrypted) wireless data communications, RFID chips and identifying liquids, and more, can benignly sneak in under another (legitimate and beneficial) guise. And each one will have an impact on the society that we're crafting for ourselves and our kids.

As an *informed* society, we may decide that the benefits of some of these technologies outweigh their privacy and other downsides, and if open chosen, that would be OK (from a majority societal standpoint.) But if we're *not* 'informed;' if we allow our privacy to be eroded beneath the threshold of our awareness, then we may wake up one day and find that we, and our communications and data and actions, 'are not alone.'

Do stay informed. And inform others.

In other words --

Don't Blink!

This essay is original and was specifically prepared for publication at Future Brief. A brief biography of Jeff Harrow can be found at our main [Commentary](#) page. Other essays written by Jeff Harrow can be found at his [web site](#). Jeff receives e-mail at jeff@theharrowgroup.com. Other websites are welcome to link to this essay, with proper credit given to Future Brief and Mr. Harrow. This page will remain posted on the Internet indefinitely at this web address to provide a stable page for those linking to it.