

www.futurebrief.com

Private Paper

Jeffrey R. Harrow
Principal Technologist, The Harrow Group

It doesn't surprise most of us that sophisticated "tags" or "codes" can now be embedded in digital information - consider the copyright information within some digital movie files, or "digital watermarks" (steganography) that can be invisibly embedded within a digital picture, or on a more simplistic basis, the mostly-transparent network logos that are increasingly appearing during TV shows.

But in a piece of paper?

Generally, we consider a piece of paper without our names or code numbers or bar codes to be anonymous, such as "survey forms" that we receive in the mail, fill out, and return. But even today this isn't always the case; "invisible inks" can be used to identify such paper in a way we won't notice. Now, a recent announcement from CrossID (www.crossid.com or www.ponsholdings.com/CrossID/#FAQ) promises to take the idea of identifying individual sheets of paper a giant leap forward.

As described in the February 11th [RFID Journal](#), the CrossID concept actually prints tiny, wireless, passive, "chipless" RFID (Radio Frequency IDentification) tags, costing less than one-tenth-of-a-cent each, onto any desired sheet of paper (such as government and corporate documents, currency, stock certificates, or any other documents that the issuer wishes to be tracked

How It Works

Specifically,

"The system uses "nanometric" materials—tiny particles of chemicals with varying degrees of magnetism—that resonate when bombarded with electromagnetic waves from a reader. Each chemical emits its own distinct radio frequency, or "note," that is picked up by the reader, and all the notes emitted by a specific mix of different chemicals are then interpreted as a binary number. Since the system uses up to 70 different chemicals, each chemical is assigned its own position in a 70-digit binary number.

"For example, if the chemicals A, B, C and D were assigned to the first, second, third and fourth positions in the 70-digit number, then a mixture consisting of A and C would represent the binary number 1010 followed by 66 zeros. CrossID is testing readers that operate at three to 10 GHz, which is higher than the frequencies commonly used by wireless LANs and handheld computers, although the company has not made a final determination on what frequency the readers will use."

www.futurebrief.com

Don't Write Your Shopping List On THIS Paper!

These chemical "bar codes" can be read at a distance of up to ten feet, without line-of-sight. So, for example, an office that dealt with sensitive information could replace all notepaper and paper used by copiers and printers with blank sheets that had been pre-printed with unique identification codes. They would then install CrossID readers at all building exits, and the system would signal if someone attempted to leave with a concealed piece of paper that had been generated within those walls. It could even identify the specific piece of paper, since each is serial-numbered! (Note that I have no association with CrossID.)

Another possibility for a "mixed" sensitivity environment (where the most important documents should be tracked but most need not be), would be to have the computer systems force all sensitive documents to only be printed on printers that contain CrossIDed paper. Or, to have special printers actually print CrossID codes and serial numbers (or other information) onto every sensitive document as it is printed. Insecure information could still be printed on un-tagged paper as usual.

But if this were implemented, why couldn't nefarious people simply copy secure documents onto un-tagged paper on a copy machine? One answer would be to embed CrossID readers within every copy machine so that they can detect a secure document on the glass -- and then refuse to copy it. With a bit more sophistication, the system could simultaneously alert Security that, at this time and place, this specific person (whose image was captured by the security camera near that copier) attempted to copy a secured document with this specific ID.

[By the way, the concept of automatically preventing the copying of certain documents is already a reality -- a growing number of color copiers have "currency detection" algorithms built-in, and refuse to copy designated currency(s), even for legal uses (as discussed at [Security Focus](#)). Even PCs are being affected, as new versions of Adobe's Photoshop contain a similar currency filter (described at [its site](#)) -- Slashdot has an extensive discussion on this issue at [its site](#).]

The Bottom Line

By 2006, CrossID anticipates that their paper-tagging solution will be ready to go, costing less than one-cent per page (or product label, or garment...) And they're not alone -- other companies, such as Inkode ([see RFID Journal article](#)) have their own technological solutions to the issue of marking paper. (Inkode's solution has already been on the market for some time; they embed tiny metal fibers in paper, plastic packaging, "chipless RFID tags," etc., that provide a unique signature (rather than specific information) when queried by its reader.)

So it seems that the once-anonymous sheet of paper will not be, for long.

There's Also a Dark Side

There are many valuable uses for such technology. But many of the concerns I've explored in the past regarding RFID technology in general here at Future Brief certainly apply to "tagged paper" as well. Imagine, for example, if a merchant paid you change with a tagged banknote, which was matched to "You" via your "loyalty card" (even though you paid cash). Subsequently, as you walk down the street, every reader in every storefront (or on every utility pole) that you pass could also note the bill's ID and uploaded it to a database that consolidated the information. Not only could this database track your movements, but it might also know exactly what you later purchased with that banknote, and *where*...

It's Up to Us

But through careful, informed choices, it may be possible to implement the societally-valuable aspects of these technologies without treading on the dark side. It remains up to us -- to each of us through our elected representatives, to assure that technology is only implemented in ways that we are, quite literally, willing to live with.

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.

To hear about future **Commentary** essays, take a few seconds to read about [Daily Brief](#), one of the "briefest" Internet updates offered anywhere.