that only tagged items are secure, and industry proclaims the convenience and savings made possible through mobile RFID readers. It is not surprising that two main supporters of RFID are the U.S. Department of Defense and Wal-Mart and are likely to be joined by the mobile technology sector and others once new revenue streams are more apparent.

Benefits to major corporations and governments will not in and of themselves generate public acceptance of tagged cash. That acceptance is essential if the technology is to overcome privacy objections. Hence the issue of mobile RFID and tagged bank notes, while contributing to decreased anonymity, is being marketed to individuals as a self-evident personal advantage. Once people are proffered a bank note, their mobile phones read the tag, establish a connection to the authority's database, and receive confirmation of the note's authenticity and validity and of the legitimacy of the bearer. Fraud will decrease dramatically. As a byproduct of the process, the government will obtain yet more information for its database of cash transfers from private citizens, as well as from the banking, retail, and service sectors. As tagged product purchases find their way into our homes, we will be only a step away from installing indoor receivers into our shelves, floors, and doorways [1]. The net on anonymity will continue to tighten. The criticism of Katherine Albrecht, founder and director of an advocacy group called Consumers Against Supermarket Privacy Invasion and Numbering (www.spychips.com), and others have convinced Auto-ID Labs around the world to address the growing concern and work on ways to deal with the privacy issue.

This is just as well, because the databases of tags and their bearers maintained by various governments don't stop with money. In the name of homeland security, new U.S. passports will contain standard passport data in an embedded tag that can trigger the respective name, address, and digital picture. Although not encrypted, security will be warranted through digital signatures [11]. The world's national borders will be equipped with readers, thereby increasing control of the transnational flow of people. By extension, immigration officials will be able to identify individual travelers through the tagged cash and goods they carry. There will be no more slipping through customs without paying duty or carrying suitcases full of money to Switzerland.

However, because RFID technology doesn't require a physical connection between tag and reader, officials will be able to validate a person's identity not only at the port or airport but also in any public or private space within the limited range of the RFID tag/readers, all without the express permission or even awareness of the person. As the range at which tags may be read increases and the technology improves, will unreasonable search and seizure become imperceptible search and seizure?

BY COLLECTING TAG DATA ON THE PERSON BEING RF-INTERROGATED, THE "DATA VOYEUR" MIGHT CREATE A COMPLETE COMMERCIAL, AND, WORSE, PERSONAL PROFILE.

But it's not only the government watching from the shadows. Privacy advocates argue that mobile RFID readers can lead to increased identity theft, high-tech stalking, and commercial data collection [11], perhaps with the intent of hijacking the seemingly good intentions of RFID-tagged goods and cash. Indeed, retailers are concerned that thieves equipped with mobile RFID devices will create new and sophisticated ways of shoplifting. Anarchists have long dreamed of the destruction of the state by destroying its power to issue and control money. In "chaos attacks," they hope to damage tags embedded in cash to render it practically invalid until exchanged at banks for good money with valid tags, causing major inconvenience and disruption. Global retail chains (such as McDonald's), for years targets of environmental activists, would find collecting and then validating large amounts of cash a constant headache.

When only fully functioning tagged money will be good money, what happens when a tag is destroyed, whether by accident or on purpose? General access to the government's provenance database of money (needed to replace genuinely damaged bank notes) will introduce unimagined levels of complexity into the system, along with the likelihood of database failure. How do we ensure that thieves do not screen the tagged content of our wallets to find out if we are worth robbing? Innocents will need to engage in countermeasures: wallets will contain RFID shielding