By IAN ANGELL and JAN KIETZMANN

RFID AND THE END OF CASH?

RFID-embedded money is likely to mean the end of anonymous transactions and with it one of the last bastions of personal anonymity.

Thinking about buying a new car with cash? How about paying school fees? Don't bother. Such money is not welcome. Western banks today treat all large cash deposits as "suspicious transactions," covering their backs by immediately reporting cash-loaded customers to the authorities for carrying sums far less than the minimum amounts required by regulations. Governments say "Only the guilty deal in cash." Consequently, sensible businesses avoid large cash deals. Depositing cash into the banking system means everything is electronically recorded. New anti-money-laundering regulations, especially since the terror attacks of September 11, 2001, identify these deposits as the entry point of an audit trail of suspicious transactions. What is going on?

Illustration by ROLAND SARKANY

Legislators in the West have decided that the deregulation of the past decades, particularly concerning money (such as the loosening of exchange controls), has gone too far. Despite profiting substantially from seigniorage, including the profit resulting from the difference in the cost of printing money and the money's face value, governments grudgingly issue exchangeable money; or else other private groups would. Harking back to Plato and his moneyless utopian *Republic,* governments today prefer a perfect society with a nonconvertible currency that (they claim) safeguards their economies from external meddling and from losing the wealth of those dissidents who choose to escape what they see as state oppression. New technology raises the spectre of the state gaining total control over money, achieving this nominal collectivist heaven by destroying the essence of cash—the cornerstone of individual freedom.

This scenario seems paradoxical given that global telecommunications is bringing about the death of distance. Businesses, along with some individuals, have become truly international. Today's convergence of the Internet, mobile technology, and electronic payment schemes makes everyone a trader, a global business elite that is of one mind: arbitrage the new opportunities to minimize their tax liability.

THE MORE DETAILED THE RECORDING OF RFID TRANSFERS, THE TIGHTER THE NET BECOMES, AND THE MORE LIMITATIONS THAT ARE PLACED ON THE INDIVIDUAL'S ABILITY TO REMAIN ANONYMOUS.

However, most governments are addicted to taxation. Democracies are no exception; how else could they afford to subsidize the benefits they deliver to preferred voters and contributors? Increased regulation makes the state even more costly to run, so the tax take must increase. The state is a Faustian pact, where the individual submits to its "legitimate violence" in return for protection and security [12]. The government, from its side of this bargain, demands ownership of its citizens and the monopolistic right to tax them at whatever level whenever it wishes, calling it "balancing the budget." However, taxing cash is complicated due to its three interrelated properties: anonymity, fungibility, and ability to store value.

Although credit and debit cards do away with the need for cash, the amount of cash in circulation is increasing in almost all countries. As of July 2004, U.S.$730 billion in coins and notes was in circulation in the U.S., much of the increase due to the use of ATMs and demand from abroad [5]. Governments don't easily give up on their tax take, developing tactics for eroding anonymity, fungibility, and the ability to store value that make cash so attractive to tax evaders.

Cash has no provenance. Unlike with checks and credit cards, it is very difficult in cash transactions to associate a purchaser with a purchase or a particular purchase with other purchases. Audit trails have to be separately and expensively imposed. Roman Emperor Vespasian 2,000 years ago may have believed *pecunia non olet* (money doesn't stink), but modern governments sense the possibility of cash giving off the unmistakable odor of each identifiable bearer, making it a de facto identity card and negating the personal freedom encapsulated in anonymous money.

Although individual bank notes have unique identification numbers, they are not tracked from the moment of issue. Indeed, until recently it was too costly to track the cash transactions of individuals (even their checks and credit card transactions), except in special high-priority cases. Now there is computerized profiling, data mining, and radio-frequency identification (RFID). The government's long-term aim may be to turn society into a Panopticon, using it as an analogy for a prison in which an unseen guard observes all prisoners without them knowing they are being observed. By constructing a complete record of the personal debits and credits of all its citizens, thereby spinning a web connecting all buyers and sellers, the Internal Revenue Service and its equivalents outside the U.S. not only calculate every tax bill but are able to seize payment from those operating in both the official economy and the underground "shadow economy."

In a democratic regime, this assault on individual freedom must appear benign so as to avoid popular discontent. Democracies are obliged to profess superior morality and/or utility in order to convince citizens of the rightness of their legitimate violence [12]. The enforcers of state power—the police, national

security services, and tax collectors—may be given the right, nay the obligation, to invade the privacy of citizens with impunity.

How do democratic governments get their citizens to accept a wholesale loss of privacy? The trick is to convince them that such intrusion is in their own self-interest and may even deliver personal benefits. Some politicians seize the moral high ground by stirring up a smokescreen of public outrage against drug trafficking, terrorism, corporate greed, pedophilia, and counterfeiting. They also make the highly suspect claim that the pairing of regulation and technology will cure these social ills, protecting the individual from fraud and theft. Unfortunately, this duo comes at a cost. For example, of the £250 billion estimated to have been laundered through the U.K., the government has recovered a mere £46 million, at a cost of £400 million [2].

The USA PATRIOT Act of 2001 and in the U.K. the Regulation of Investigatory Powers Act of 2000 and the Proceeds of Crime Act of 2002 were all approved with atypical haste. Legislators have learned the lesson of the 1931 conviction of Al Capone by the U.S. Department of the Treasury. If you can't catch a criminal in the act, "follow the money" instead. Invert the burden of proof. The accused (in fact everyone) is guilty until proven innocent, where proof of innocence is nothing less than the unconditional surrender of all personal and financial information. No surprise that anti-money-laundering regulations, especially the "know your customer" rules, demand that every bank official act as a secret policeman for the government.

Should the privacy dissident operate in electronic cash? No. E-cash is hopelessly compromised, with issuers intimidated into insinuating an audit trail in the encrypted data; it is just a glorified debit card. Perhaps the dissident should stay well away from the government-regulated banking system, using only high-denomination bank notes. Unfortunately, this well-used tactic no longer provides the desired level of anonymity, owing to its convergence with another technology.

RFID's ability to perform as an auto-identification technology was first utilized by the Royal Air Force in World War II to differentiate between friendly and enemy aircraft. Friendly planes were equipped with bulky "active" RFID transponders (tags) energized by an attached power supply and interrogated by an RFID transceiver (reader). Applications today rely on similar communication between RFID tag and reader, although the tags (miniscule microchips attached to antennae) are generally "passive," powered by an electromagnetic field emitted by the reader. Radio signals inform nearby readers of a serial number stored on the tag that uniquely identifies any item bearing the tag. So-called "smart tags" are used to track or trace objects. Worldwide in 2003, they helped keep track of about 100 million pets and 20 million livestock [3].

The Auto-ID Center, established in 1999 as an academic research project at the Massachusetts Institute of Technology, developed the architecture for creating a seamless global network of all physical objects (www.autoidlabs.org/aboutthelabs.html). The technology has since been transferred to EPCglobal (www.epcglobalinc.org), which oversees development of standards for electronic product code (EPC) tags. These tags are used for every imaginable item—from clothes to medicine, electronics, food, motor vehicles, books, door locks, and airplanes—revolutionizing logistics and supply-chain and inventory management worldwide. For example, Legoland in Denmark uses RFID and 802.11 WLAN technology to find lost children [4], and U.S. forces employ Texas Instruments wristbands to help track wounded U.S. soldiers and prisoners of war in Iraq.

The turn of the century saw substantial gains in the efficiency of power conversion in circuits, providing power for cryptographic operations. The least expensive and least powerful tags (such as basic EPC tags) provide no layers of security. More advanced and costly tags require additional power for cryptography (such as for static key operations in PINs and passwords, symmetric key encryption, and cryptographic co-processors). These extra levels of security enable novel opportunities, not only for commercial transactions but for money itself.

An RF-emitting tag can be small enough to fit into bank notes so as to uniquely identify each one as it passes within range of a sensor. The authorities claim its purpose is to combat counterfeiting and identify money transfers between suspicious parties. RFID readers interrogate multiple tags simultaneously. Every time notes are passed to or from a bank, RFID readers identify and record them, linking this data with the person who presented or received them. The government has the potential to know not only exactly how much cash is being carried out/in the door but who is carrying it and who carried it previously. By comparing the respective identification numbers to entries in their database (for authentication purposes, of course), the authorities can draw a link between the last recorded holder of the note and the current one.

This web of contact information is also incomplete. It misses out on the numerous cash transac-

tions not captured by banks, including those that occurred as the note was passed hand to hand, starting with the party who issued it and ending with whoever returned it to the bank. To increase the accuracy of their records, authorities will indeed expect intermediate retail and service outlets to identify customers, then read and report their tags. Cash registers can record all transactions, good and bad, legal and illegal, honest and dishonest, and identify notes that enter their system, flagging those that are either counterfeit or no longer accepted as legal tender. The new RFID-based technology gives the authorities the power to cancel a particular note. The more detailed the recording of RFID transfers, the tighter the net becomes, and the more limitations that are placed on the individual's ability to remain anonymous.

A 2004 Internet hoax involved $20 bills with an RFID tag in Andrew Jackson's eye [10]. So it's all a ruse? Not at all. The 10,000-yen bills (~$100) of 2004 were to be implanted with Hitachi's 0.4mm^2, 60-micron-thick "μ-chip" [8], each costing around 50 yen [9]. Plausibly, as the price of tags decreases further, they will be embedded into smaller-denomination bank notes to increase the recording and monitoring of yet more cash transactions. The European Union considered implanting tags in its notes by the end of 2005, though this is on hold, and the Swedish National Bank has announced a similar idea. Is the U.K. or U.S. next?

No more anonymous cash. But worse, two other properties of cash—fungibility and stored value—are also under attack. Each bank note, whatever its denomination, should be as good as any other, but not if it's rejected, discounted, or terminated. By insisting that only bank notes with operational tags are legal tender, governments may cancel the cash of targeted individuals.

What a great method for instantly taxing citizens. Governments calculate the tax owed and take the correct sum straight out of each taxpayer's pocket by canceling bank notes, then reprinting and reissuing new ones bearing different RFID tags. The possibilities are limitless. By giving each note an expiration date, governments may force bearers of cash to spend their money. The government can also hold out the threat of instant devaluation, with the value of a bank note being not the numbers printed on the note itself but the amount coded into the tag, drastically transforming the notion of stored value.

Why doesn't everyone object loudly and publicly? It's not just ignorance of the technology. A very real opportunity presents itself, as RFID technology finds its way into the home at a price all can afford. The viral message is going out that the benefits far outweigh the hazards through a marketing blitz aimed at gaining widespread public acceptance.

It's not only that passive RFID tag technology is rapidly maturing among a passive (some might say apathetic) public. Innovators predict huge public demand for the products of the convergence of personal RFID readers and mobile telephones. The mobile telephony industry senses a killer application. Who wouldn't pay to locate misplaced keys, spectacles, gloves, or socks (conveniently tagged by their manufacturers)? By marrying an asynchronous reader with a synchronous mobile phone, the emergent device would be able to read and transfer tag data anywhere in near real time. Connecting phones and/or tags would make it possible to send and receive electronic funds. Accessing a tag might also trigger a connection to the manufacturer or retailer's Internet presence through a mobile phone. Applications for mobile phones equipped with RFID readers are endless, promising to introduce huge new revenue streams to handset manufacturers, application developers, and service providers.

The security infrastructure surrounding this technology, balancing privacy against commercial applications, is a major concern. RFID does not require line-of-sight for reading tags, operating instead on radio frequency. Hence, private data about people and their belongings and shopping behavior can be received simply by waving a reader near their clothes, handbags, and other personal items. The size of their shirts is no longer their personal secret, nor is the amount of cash they are carrying. By collecting tag data on the person being RF-interrogated, the "data voyeur" might create a complete commercial, and, worse, personal profile.

One may argue that this problem would be solved by disabling each tag when it leaves a shop, but this is neither in the interest of the retailer nor, in fact, of the customer. Tags will store warranty information (paper receipts will no longer be accepted) and, more important, the rights of ownership (a stolen item is easily identified). It is thus in the interest of the purchaser to keep tags alive. Furthermore, using RFID-enabled phones in the exchange of goods and money is both a guarantee and a proof of the transfer of ownership. Only a troublemaker would want to destroy or disable such useful data.

So there are very real general benefits in RFID technology. However, this does not mean that the mixing of cash and mobile RFID will receive strong support. As with many new technologies, innovators promise utopia; meanwhile, governments may declare

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

material for personal security reasons, and people will carry RFID blockers or tag jammers to disrupt transmission of information to scanning devices.

We will soon be living in a world of tags, with different ones serving different purposes. EPC tags will store Global Trade Identification Numbers to give each item a unique identification number. RFID-tagged items will be as ubiquitous as barcoded products are today but be even more pervasive. However, unlike barcodes, multiple RFID tags can be read simultaneously, each distinctively identifying the bearer at once without the need for line-of-sight or direct contact between reader and tag. Each of us will be a walking mountain of tags, and it will be impossible to isolate them all from being read. Moreover, due the convergence of the pervasive mobile telephone and RFID readers, everyone will be able to obtain all manner of information about everyone else—from passports, clothes, personal data, and, in particular, cash.

HOW DO WE ENSURE THAT THIEVES DO NOT SCREEN THE TAGGED CONTENT OF OUR WALLETS TO FIND OUT IF WE ARE WORTH ROBBING?

Will the convergence of money, mobile telephony, and RFID inexorably lead to the end of cash as we know it? Is this "the complete delivery of the individual to the tyranny of the state, the final suppression of all means of escape, not merely for the rich, but for everybody" [7]? Possibly. The technology will ensure that personal credit devices no longer come in the shape of cards but as tags in keychain fobs, stickers, and implants. Cash as we know it will be an anachronism. RFID developments in the name of supply-chain management and national security will complement the worldwide flood of tags. The public will be ready—enthusiastically armed with RFID-reading mobile phones to scan items in shops and the money they handle, as well as information about one another.

Can the stampede of privacy-invading mobile technology along Friedrich Hayek's *Road to Serfdom* [7] be stopped? After all, money does not have to be created legal tender by governments. Due to low transaction costs, organizations can issue money, possibly as a percentage of their equity. To a certain extent this is already happening with large-denomination bonds, but new technology introduces the potential for use in small denominations—real cash money. Maybe Hayek's vision of the "denationalisation of money" [6] will become a reality. As a substitute for government-issued bank notes, we may instead just deal in yet another, untagged currency to maintain our anonymity. C

References

1. Albrecht, K. Supermarket cards: The tip of the retail surveillance iceberg. *Denver University Law Review 79,* 4 (Summer 2002), 534–539 and 558–565.
2. Bawden, T. U.K.'s bid to trace dirty money is 'pathetic.' *Times Online* (Mar. 15, 2005); business.timesonline.co.uk/article/0,,8209-1525951,00.html.
3. Booth-Thomas, C. The see-it-all chip. *Time Online Edition* (Sept. 14, 2003); www.time.com/time/globalbusiness/article/0,9171,1101030922-485764,00.html.
4. Collins, J. Lost and found in Legoland. *RFID Journal* (Apr. 28, 2004); www.rfidjournal.com/article/articlview/921/1/1/.
5. Federal Reserve Bank of New York. *How Currency Gets into Circulation.* Aug. 2004; newyorkfed.org/aboutthefed/fedpoint/fed01.html.
6. Hayek, F. *The Denationalisation of Money.* Institute of Economic Affairs, London, 1976.
7. Hayek, F. *The Road to Serfdom.* University of Chicago Press, Chicago, 1972.
8. Hitachi. *The World's Smallest RFID IC.* Hitachi, Ltd., Tokyo, 2004; www.hitachi.co.jp/Prod/mu-chip/.
9. Leyden, J. Japan yens for RFID chips. *The Register* (July 30, 2003); www.theregister.co.uk/2003/07/30/japan_yens_for_rfid_chips/.
10. McCullagh, D. *RFID Industry Tries to Debunk 'Exploding $20 Bill' Myth.* Association for Automatic Identification and Mobility, Inc., Warrendale, PA, Mar. 18, 2004; www.prisonplanet.com/031804_RFID_industry_tries_to_debunk_exploding_$20_bill_myth.html.
11. Singel, R. American passports to get chipped. Wired.com news (Oct. 21, 2004); www.wired.com/news/privacy/0,1848,65412,00.html.
12. Weber, M. *Politics As a Vocation.* Hackett Publishing Co., Indianapolis, IN, 2004.

Ian Angell (i.angell@lse.ac.uk) is a professor of information systems in the Department of Management in the London School of Economics.

Jan Kietzmann (j.h.kietzmann@lse.ac.uk) is a researcher in the Department of Management in the London School of Economics.