RFID and the End of Cash?

Ian Angell and Jan Kietzmann
London School of Economics
{i.angell; j.h.kietzmann}@lse.ac.uk

Thinking of buying a new car with cash, or paying school fees? Don't bother! Nowadays such money isn't welcome. Banks treat all large cash deposits as 'suspicious transactions,' and cover their backs by immediately reporting cash-loaded customers to the authorities for carrying sums far less than the amounts required by regulations. For the state insists that "only the guilty deal in cash." Consequently, sensible businesses avoid large cash deals like the plague, because by entering cash into the banking system, where everything is electronically recorded, new anti-money laundering regulations identify such firms as the entry point of an audit trail of suspicious transactions. What is going on?

Legislators 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, states begrudgingly issue exchangeable money, for otherwise other private groups will. Harping back to Plato and his moneyless utopian *Republic*, governments would prefer a perfect society with a non-convertible currency that (they claim) safeguards their economy from external meddling, and from losing the wealth of those dissidents who choose to escape state oppression. New technology raises the spectre of them gaining total control over money, achieving this hell of a collectivist heaven by destroying the essence of cash, the very corner stone of individual freedom.

This seems paradoxical given that global telecommunications is bringing about the "death of distance." Businesses and some individuals have become truly international. The convergence of the Internet, mobile technology and electronic payment schemes now makes everyone a trader, and this global business elite is of one mind: arbitraging the new opportunities to minimize their taxes.

However, most states have become addicted to taxation. Democracies are no different, for how else can they afford to subsidize the benefits to preferred voters? Paradoxically, 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 (Weber 2004). The state, from its side of this unholy bargain, demands ownership of its citizens, body and soul, and the monopolistic right to tax them at whatever level whenever it wishes – they call it balancing the budget. Taxing cash, however, isn't easy because of three interrelated properties of cash - its 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 in the world. As of July 2004 there was US$730 billion in coins and notes in circulation in the U.S., much of the increase due to both the use of ATMs, and demand from abroad (NYFED, 2004). States won't give up on their tax-take that easily, and are developing a very effective tactic to erode the anonymity, fungibility, and ability to store value that make cash so attractive to tax evaders.

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

Previous unpublished version that later was revised and published as:
Angell, I. & J. Kietzmann (2006): RFID and the End of Cash?
Communications of the ACM, vol. 49, no. 12, pp. 91-96.

Although individual banknotes have unique identifying numbers, they are not tracked from the moment of issue. Indeed, until recently it was too expensive to track the cash-transactions of individuals (or even their checks and credit cards), except in special high priority cases. Now there is computerized profiling and data mining – and, as we shall see, RFID! The state's long-term aim is to turn society into a Panopticon, constructing a complete record of the personal debits and credits on all its citizens, thereby spinning a web that connects all buyers and sellers, with the IRS not only calculating every tax bill, but also seizing payment from those operating in both the official economy and the underground 'shadow economy.'

In a democratic regime, this assault on individual freedoms must appear benign to avoid a popular revolt. Therefore, democracies are obliged to profess a superior morality and/or utility in order to delude citizens of the rightness of this legitimate brutality (Weber 2004). Then policemen and tax collectors, the enforcers of state power, preening themselves in this sanctimonious morality, can be given the right, nay the obligation, to invade the privacy of its citizens with impunity.

How do democratic governments get their citizens to accept a wholesale loss of privacy? The trick is to convince voters that such intrusion is in their own self-interest, and may even have personal benefits. How? Politicians seize the moral high ground by stirring up a smokescreen of public outrage against drug trafficking, terrorism, corporate greed, pedophilia, counterfeiting. To cap it all they also make the highly suspect claim that the pairing of regulation and technology will cure all these social ills and protect the individual from fraud and theft. Unfortunately, this dynamic duo doesn't even protect the state: of the £250 billion estimated to have been laundered through the U.K., the government has recovered a mere £46 million. The cost of this compliance was £400 million (Bawden, 2005)!

The U.S. Patriot Act, and in the U.K., the RIP Act and the Proceeds of Crime Act have all been cleverly rushed through. Legislators have learned the lesson of the successful 1931 conviction of Al Capone by the U.S. Treasury. If you can't catch a criminal in the act, then "follow the money" instead. Invert the burden of proof! The accused (in fact everybody) is guilty until proven innocent, where proof of innocence is nothing less than the unconditional surrender of all personal and financial information. No surprise then that anti-money laundering regulations, especially the 'know-your-customer' rules, demand that every bank official acts as a secret policeman for the state.

Should the privacy dissident operate in electronic cash? No! E-cash has been hopelessly compromised with the issuers intimidated into insinuating an audit trail amongst the encrypted data – it's just a glorified debit card. Perhaps the dissident should stay well away from the banking system, and use only high denominational banknotes? Unfortunately, that well-used tactic no longer provides the desired level of anonymity either, thanks to the convergence with another technology. Radio-frequency identification (RFID) has reared its ugly head.

RFID's capability as an auto-identification technology was first utilized by the Royal Air Force (RAF) in World War II to differentiate between friendly and enemy aircraft. Friendly planes were equipped with bulky RFID 'active' transponders (tags) that were 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 now the tags (a miniscule microchip attached to an antenna) 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 that bears that tag. So-called 'Smart Tags' are used to track or trace objects.

Worldwide, they already help keep track of about 100 million pets and 20 million livestock (Booth-Thomas 2003). The Auto-ID Center, initially established as an academic research project headquartered at the Massachusetts Institute of Technology, developed the architecture for creating a seamless global network of all physical objects (Auto-ID Labs 2005). The technology has since been transferred to EPCGlobal, which now oversees the development of standards for Electronic Product Codes (EPC). Such EPC tags for every imaginable item are revolutionizing logistics, supply chain and inventory management around the world. Legoland employs RFID and 802.11 WLAN technology to find lost children (Collins 2004); Texas Instruments wristbands help U.S. Forces track wounded U.S. soldiers and Prisoners of War in Iraq (Scheeres 2003).

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 powerful tags, for example basic EPC tags, provide no layers of security. More advanced tags require additional power for cryptography, e.g. for static key operations (PINs and passwords), symmetric key encryption and cryptographic co-processors. These extra levels of security enable novel opportunities, not only for commercial transactions, but also for money itself.

An RF-emitting tag can be small enough to be fitted into banknotes so as to identify each note uniquely as it passes within range of a sensor. The authorities claim its purpose is to combat counterfeiting, and to identify money transfers between suspicious parties. RFID readers can interrogate numerous tags simultaneously. Every time notes are passed to or from a bank, RFID readers will identify and record them, and link this data with the person who presents or receives them. The state has the potential of knowing not only exactly how much cash is being carried out/in the door, but also who is carrying it, and who has 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 – they will know who is doing business in cash (not just as now in other forms of money), and with whom.

Naturally such a web of contact information would be incomplete. It would miss out on the numerous cash transactions not captured by the banks: those that occur as the note is passed hand-to-hand, starting with the party issued with the note, and ending with whoever returned it to the bank. To increase the accuracy of their records, authorities will expect intermediate retail and service outlets to identify customers, and then read and report their tags. Cash registers can record all transactions, good and bad, and identify notes that enter their system, flagging those that are either counterfeit or no longer accepted as legal tender. More sinisterly, the new technology hands 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 placed on the private individual's ability to remain anonymous.

Science fiction, you may think. A recent Internet hoax told of twenty dollar bills having an RFID tag placed in Andrew Jackson's eye (McCullagh 2004). So it's all a ruse? No! The new 10,000 Yen bills (~$100) currently entering production are to be implanted with Hitachi's 0.4mm^2, 60-micron thick 'μ-chip' (Hitachi 2004). Each chip costs around a mere 50 Yen (Leyden 2003)! Plausibly, as the price of tags decreases further, they will be embedded into smaller denomination banknotes to increase the recording and monitoring of yet more cash transactions. The European Union is considering implanting tags in its notes by the end of 2005 (Ingdahl 2004). Is the U.K. or the 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, or discounted, or terminated! By insisting that only banknotes with operational tags are legal tender, governments may cancel the cash of any targeted individual. What a great method for instantly taxing citizens: governments calculate the tax owed and take the correct sum of money straight out of each taxpayer's pockets by canceling banknotes, and then reprinting new ones bearing differently identifiable RFID tags! The possibilities are limitless. By giving each note an expiry date, governments may force bearers of cash to spend their money. There can be the threat of an instant devaluation, with value of the banknote being not that printed on the note itself, but the amount indicated on the tag – so much for stored value!

So why no voices raised in objection? It's not just ignorance of the technology. No, a very real opportunity is presenting itself as RFID technology is finding its way into the home, and at a price that will fit everyone's pocket. The message is going out that the benefits far outweigh the hazards, in 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 would say apathetic) public. Innovators are predicting a huge public demand for the products of the convergence of personal RFID readers and mobile telephones. The mobile telephony industry is sensing the next killer application – who wouldn't pay to locate those irritatingly misplaced keys, spectacles, or gloves, soon to be conveniently tagged by the 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. Electronic funds can be sent and received by connecting phones and/or tags. Accessing a tag might also trigger a connection to the manufacturer or retailer's Internet presence through a mobile phone. Benetton is already testing the technology by tagging 15 million garments (RFID Journal 2003). Applications for a mobile phone equipped with an RFID-reader are endless, and promise 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, will be of major concern, because there is a downside. RFID does not require line-of-sight for reading tags; it operates on radio frequency. Hence private data about another person, his or her belongings, and shopping behavior can be received simply by waving a reader near their clothes, handbags etc. The size of their shirt no longer remains their little secret, nor does the make and style of underwear, nor the amount of cash they are carrying. By collecting tag-data on the person being RF-interrogated, the 'data voyeur' can create a complete commercial, and, worse, a personal profile.

One may argue that this problem would be solved by disabling each tag once 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 importantly the rights of ownership (a stolen item can easily be identified). It is 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, that doesn't mean that the mixing of cash and mobile RFID is likely to receive strong support. As with many new technologies, the planners promise utopias: the state declares that only tagged items are secure, and industry proclaims the immense convenience and savings made possible through mobile RFID

readers. It is not surprising that the two main supporters of RFID are the Department of Defense and Wal-Mart – they will be joined by the mobile technology sector once the benefits of the new revenue stream become more apparent. However, benefits to the major corporations and governments will not in themselves generate public acceptance of tagged cash – and that acceptance is essential if the technology is to overcome privacy objections. Hence the issue of mobile RFID and tagged banknotes, although contributing to decreased anonymity, is being marketed to individuals as a self-evident personal advantage. Once a person is proffered a banknote, her mobile phone will read the tag, establish a connection to the authority's database, and receive confirmation both of the note's authenticity and validity, and of the legitimacy of the bearer – fraud will dramatically decrease. As a by-product of the process, the state will obtain yet more information for its database of cash-transfers, from the private citizen as well as the banking, retail and service sectors. As tagged product purchases will find their way into every home, we will be only a step away from installing indoor receivers into people's shelves, floors and doorways (Albrecht 2002) and the net on anonymity will continue to tighten. The criticisms of Katherine Albrecht and others have convinced Auto-ID Labs around the world to address the growing concern, and to work on ways of dealing with the privacy issue.

This is just as well, because the government database of tags and their bearers doesn't stop with money. In the name of homeland security, U.S. passports will soon contain standard passport data in an embedded tag that can trigger the respective name, address and digital picture. Although not encrypted, authorities say that security will be warranted through digital signatures (Singel 2004). 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 each traveler with the tagged cash they are carrying, and goods they have bought – no more slipping through Customs without paying duty, or carrying suitcases of money to Switzerland.

However RFID technology doesn't require a physical connection between tag and reader, and so 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, and all without the expressed permission or even the awareness of that person. As the range at which tags may be read increases, as the technology improves, will unreasonable search and seizure become imperceptible search and seizure?

But it's not only government watching from the shadows. Privacy advocates argue that mobile RFID readers can lead to an increase in identity theft, high-tech stalking, and commercial data collection (ibid.) Other parties are intent on 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 will damage tags embedded in cash so as to render the money practically invalid until exchanged at banks for good money with valid tags, causing major inconvenience and disruption. Retail chains and food outlets like McDonalds, for years targets for environmental activists, will find collecting and then validating large amounts of cash a constant headache.

In a time when only fully-functioning tagged money will be good money, what happens when a tag is destroyed, by accident or on purpose? The general access to the government's provenance database of money, needed to re-issue genuinely damaged banknotes, will introduce unimagined levels of complexity into the system, and the likelihood of database failure. How do we ensure that thieves do not screen the tagged content of our wallet to find out if we are worth robbing? Innocents

will need to engage in counter-measures: wallets will contain RFID shielding material for personal security reasons; people will carry RFID blockers or tag jammers to disrupt the transmission of information to scanning devices, and thereby thwart unwarranted collection of data.

We will soon be living in this wonderful world of tags. Different tags will serve different purposes. Electronic Product Code tags will store Global Trade Identification Numbers (GTIN) to give each item a unique identification number. Without a doubt, RFID tagged items will become as ubiquitous as barcoded products, but even more pervasive. However, unlike barcodes, RFID tags can be read multiply and each distinctively identifies the bearer at once without the need for line of sight or direct contact between reader and tag. We will each be a walking mountain of tags – it will be impossible for the individual carrier to isolate them all from being read. Through the convergence of the already all-pervasive mobile telephone with RFID readers, everyone will be able to obtain all manner of information about everybody else: from their passports, clothes, personal data, and in particular cash.

Does the convergence of money, mobile telephony and RFID 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" (Hayek 1972)? Possibly! The technology will ensure that personal credit devices will no longer come as cards, but as tags in the shape of keychain fobs, stickers or implants. Cash as we know it today will become an anachronism. RFID developments in the name of supply-chain management and national security will complement the spreading of tags throughout the world. The public will be ready, enthusiastically armed with RFID-reader mobile phones, to scan items in shops, the money they handle, and of course information about each other. And all for the best possible reasons!

Can the stampede of privacy-invading mobile technology along Hayek's "Road to Serfdom" (Hayek 1972) be stopped? After all money does not have to be created legal tender by governments. Because of the low transaction costs and ease of guaranteeing the legitimacy of each note, companies can issue money, possibly as a percentage of their equity. To a certain extent this is already happening with large denominational bonds, but new technology introduces the potential of small denominations – and real cash money. Maybe Hayek's vision of *the Denationalisation of Money* (Hayek 1976) will now become a reality. Paradoxically, perhaps the convergence of money, mobile telephony and RFID will lead us closer to trading in private money, where the real issue is not 'dollar bills, but Bill's [Gates] Dollars.' As a substitute for government-issued banknotes, we may instead just deal in another, untagged currency to maintain our anonymity.

References

Albrecht, K. "Supermarket Cards: The Tip of the Retail Surveillance Iceberg," Denver University Law Review (79:4), Summer 2002, pp. 534-539 and 558-565.

Auto-ID Labs "About the Labs, " 2005; http://www.autoidlabs.org/aboutthelabs.html.

Bawden, T. "UK's bid to trace dirty money is 'pathetic'," Times Online, March 15, 2005; http://business.timesonline.co.uk/article/0,,8209-1525951,00.html.

Booth-Thomas, C. "The See-It-All Chip," Time Online Edition, 2003; http://www.time.com/time/globalbusiness/article/0,9171,1101030922-485764,00.html.

Collins, J. "Lost and Found in Legoland," RFID Journal, 2004; http://www.rfidjournal.com/article/articleview/921/1/1/.

Federal Reserve Bank of New York "How Currency Gets into Circulation," August 2004 http://newyorkfed.org/aboutthefed/fedpoint/fed01.html.

Hayek, F.A. *The Road to Serfdom* University of Chicago Press, Chicago, 1972.

Hayek, F.A. *The Denationalisation of Money* Institute of Economic Affairs, London, 1976.

Hitachi "The World's Smallest RFID IC," 2004; http://www.hitachi.co.jp/Prod/mu-chip/.

Ingdahl, W. "RFID in the euro notes?" The Sprout, 2004; http://www.eudoxa.se/content/archives/2004/06/rfid_in_the_eur.html.

Leyden, J. "Japan yens for RFID chips," The Register, 2003; http://www.theregister.co.uk/2003/07/30/japan_yens_for_rfid_chips/.

McCullagh, D. "RFID industry tries to debunk 'exploding $20 bill' myth," AIM Inc., 18 Mar 2004 2004; http://www.prisonplanet.com/031804_RFID_industry_tries_to_debunk_exploding_$20_bill_myth.html.

RFID Journal "Benetton Explains RFID Privacy Flap," 2003; http://www.rfidjournal.com/article/articleview/471/1/1/.

Scheeres, J. "Three R's: reading, writing, RFID," Wired.com, 2003; http://www.wired.com/news/technology/0,1282,60898,00.html.

Singel, R. "American Passports to Get Chipped," 2004; http://www.wired.com/news/privacy/0,1848,65412,00.html.

Weber, M. *Politics as a Vocation* Hackett Publishing Company, Indianapolis, 2004.