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-