# Biometrics gets down to business

**Biometrics: Body-scanning security technology is finally taking off—and not just because governments are adopting it**

FOR many people, "biometrics" conjures up images of a Big Brotherish surveillance society. But tell them they could save a few precious seconds at the supermarket checkout just by waving their fingers over a scanner, and they will sign up in their millions.

After more than a decade of hype, biometrics—the use of body measurements such as eye scans or fingerprints to determine or verify identity—is finally taking off. And all it took to convince the public of its merits, it seems, was the promise of shorter queues or a few extra loyalty points. In the past year there has been an explosion in the commercial use of biometrics, utterly eclipsing the uphill efforts of various governments to introduce identity cards and passports that store electronic signatures derived from facial images, fingerprints or eye scans.

In America more than 3m customers now regularly pay for goods at the supermarket, chemist or convenience store just by scanning their fingers and punching in a personal-identification number (PIN) rather than using credit or debit cards. Similarly, in Japan more than 2m people now use contactless palm-scanners when they want to withdraw cash from a cashpoint. And in the next few months ABN AMRO, a Dutch bank, will be rolling out a new telephone-banking system to its 4m customers that can verify each user's identity using voice analysis.

And this appears to be just the beginning. Many laptops, and even a few mobile phones, now ship with built-in finger scanners. Domestic applications, such as biometric front-door locks, garage doors and safes, are also available. There are online services that can be accessed only if the rhythm and other characteristics of your typing match a stored template of your "keystroke dynamics". There are even memory sticks or flash drives secured with built-in thumbprint scanners.

For a long time it was assumed that biometrics would be a government-led technology, says Sapna Capoor, an analyst at Frost and Sullivan, a consultancy. But in the past couple of years this has quietly started to change. "There has been a group of biometrics vendors who have shifted away from working with governments and focused instead on commercial products," she says.

One reason for this shift is that the technology has matured, says Michael Thieme of the International Biometric Group, an industry body based in New York. In the past many biometric technologies would not work on a broad section of the population. Some types of biometric scanners worked well in the laboratory, but ran into problems in real-world environments when scanning children, old people, people with small or sweaty hands, bricklayers or subjects with eye conditions. But the technology has since improved and is considerably more inclusive, says Mr Thieme. As a result it is finally reliable enough to be used in supermarkets and laptops.

New regulations in the financial sector have also boosted adoption, says Mark Upson, the boss of BioPassword in Issaquah, Washington, whose company has more than 400,000 online-banking users enrolled in its keystroke-dynamics security scheme. In a bid to tighten security and reduce online fraud and identity theft in online banking, America's Federal Financial Institutions Examination Council is pressing banks to adopt "two factor" authentication, says Mr Upson. Previously, account holders had to provide only a single means of identity verification, such as an account number and password. Two-factor systems rely not just on something you know, however, but also on something you have, such as an electronic token, or something you are, in the form of a biometric.

Electronic tokens can be expensive, and must be carried by users at all times to ensure access. "You can also give them to someone else," says Charles Palmer, chief technology officer for security and privacy at IBM Research in Yorktown Heights, New York. That is not the case with biometrics, so the technology's appeal is obvious, he says. Telephone banking has been going through a similar trend, turning to biometrics to improve security, says Vance Harris of Voice Vault, a division of Biometrics Security, a firm based in Chertsey, England. It developed the voice-verification system soon to be rolled out to ABN AMRO customers. Since banks receive tens of millions of calls each year, it was important to find a way to authenticate people quickly and reliably, says Mr Harris.

But although adding an extra identity check to such financial transactions improves security, doesn't it also add complexity and inconvenience? After all, users still have to remember account numbers and passwords as before, but must now provide a biometric too. Fujitsu's palm-scanning system, which is being used in cashpoints by four big Japanese banks, is widely considered to ▸▸

Credit, debit, or finger-scan?

be the most successful deployment of biometrics to date—yet it does not liberate customers from having to carry bank cards and remember PINs. A two-factor authentication system has been replaced by a three-factor system which is more secure but less convenient.

In contrast, the fingerprint-recognition system being used in some American shops, called Pay By Touch, appears to be more convenient but less secure, since shoppers are no longer required to present a bank card or cheque to buy things. Instead, they present a finger to be scanned and then enter a seven-digit "search code", usually the same as their phone number. The combination of the finger-scan and the search code are then looked up in a central database, to ensure that they tally, before the transaction is approved. Since the last seven digits of a phone number are not unique and are in the public domain, the security of the system would be undermined if two users' fingerprints were similar enough to generate a false acceptance.

For banking, such lax security measures would be laughable. But for shops it is more than adequate, says Mr Thieme. In a shop, where the scanner sits by the till and is supervised by a clerk, a thief could not make repeated payment attempts without raising suspicion, so false positives are unlikely. In addition, the mere incorporation of biometrics into the payment system is likely to deter criminals, says Mike Bond, an expert in banking security at Cambridge University. And even if the system can be beaten occasionally, it may not matter. "If companies can make more money by getting people through checkout more quickly, then it's possible they could offset any losses incurred through fraud," he says.

The point is that just because biometrics can be used to make systems extremely secure does not mean that the technology always has to be deployed in that way. In some applications a lower level of security is tolerable, says Mr Thieme. And in some cases biometrics can enhance both security and convenience, says Mr Harris. If you are using a phone-banking system, having to provide a passphrase is no less convenient than speaking a password to a human operator, and is more convenient than typing in a PIN. And because Voice Vault lets you set your own security question, the answer to which is used as the passphrase, it is easier than remembering a PIN.

Those in the industry believe the banking and retail approaches to biometrics—one of which puts security above convenience, the other convenience above security—will eventually converge, opening up new applications in the process. Mr Harris predicts that as confidence in biometric technologies increases, banks will start to peel away other security layers.

### Setting the standard

Once standards become established, the use of biometrics could spread so that it is used to secure retail transactions made via the internet and mobile phones, not just in shops. At the moment the technology tends to be proprietary and application-specific. But as the industry matures and interoperable standards emerge, it is likely that the biometrics hardware and software used for one application could equally well be used for others.

For example, fingerprint sensors on laptops often come with software that lets the user run a "password safe". Multiple user names and passwords for different websites are stored by the computer, which fills them in automatically once the user's identity has been verified with a finger-scan. The next logical step, suggests Alan Kramer of UPEK, a firm based in Emeryville, California, that makes finger-scanning systems, is to cut out the intermediate step and log into websites directly using the biometric itself. But this will mean devising new standards.

Using biometrics to secure transactions made using mobile phones, also known as m-commerce, looks promising too. "The killer app really is m-commerce," says Scott Moody, the boss of AuthenTec, a firm based in Melbourne, Florida that makes fingerprint sensors. M-commerce is starting to gain traction in Japan and South Korea, where phones are used both to buy things online and as a wireless-payment system in some shops and railway stations. But once you can buy things with a wave of your handset, the need to secure it becomes apparent, and the first phones with built-in fingerprint readers have already appeared.

As governments grapple with schemes to introduce biometric passports and identity cards, companies are pushing ahead with biometrics on their own. And what is perhaps even more surprising than the commercial adoption of the technology is the speed and willingness with which the public is embracing it. This is unlikely to be because people trust big companies more than they trust governments. Instead, it is because the commercial applications of biometrics tend to place a greater emphasis on the benefits to the customer, so providing incentives for adoption. As governments start to foist biometrics on their citizens, they would do well to bear this in mind.

A recent survey found that air passengers would welcome biometric check-in procedures at airports if it meant less queuing, for example. People will embrace biometrics, it seems, provided there's something in it for them. ■

**Fingers in the till**

Worldwide fingerprint biometric revenues*, $bn