Biometrics roadmap for police applications

J Elliott

It is already clear that the future of digital identity is closely linked to the future of biometrics, because biometrics can provide a degree of authentication well beyond any other technologies. But there are a lot of biometric technologies from which to choose and they are evolving largely independently. How can an organisation develop a long-term strategy for the use of the technology? One useful technique is technology roadmapping, and this paper looks at biometrics in the context of organisational strategies for their deployment.

1. Introduction — planning for biometrics

Consult Hyperion has found technology roadmapping to be useful in overcoming problems arising from distribution of expertise across different departments within an organisation or even across different continents. Once knowledge and information are located, it needs to be analysed and distilled in order to understand and communicate the complex interactions that are commonplace in today's business world. Technology roadmap charts are particularly useful aids in this respect.

These issues are especially pertinent to the application of biometric technologies within identification systems for several reasons. Each biometric technology has its own set of characteristics as does the environment within which each identification application operates. Therefore, it is impossible to choose any particular biometric as 'best' overall. Instead, it is important to consider the characteristics of any given application and choose the most appropriate biometric technologies. To complicate matters further, the pace of advancement varies radically between biometric technologies and is easily influenced by injecting research funding or political events across the globe.

2. Technology roadmapping

There are as many different flavours of technology roadmap charts as there are reasons for building them, but generally they are time-based, comprising a number of layers that include both commercial and technological perspectives. They enable the evolution of markets, products and technologies to be explored, together with the linkages between the various perspectives.

Technology roadmaps can be used to communicate visions, attract resources, stimulate investigations and monitor progress. In short, they capture the 'inventory of possibilities' for a particular field.

Figure 1 shows a generic roadmap chart view. It consists of a timeline that can include past as well as future ('know-when'). There are layers in the chart to show the interactions between purpose ('know-why'), delivery ('know-what') and resources ('know-how') as indicated down the right-hand side [1].

As well as technology, the technology roadmap document can consider softer issues such as privacy, data protection and ethics. The business processes put in place while creating the technology roadmap often build better communications between the organisations involved.

While technology roadmaps are an invaluable planning tool, one problem with predicting complex interactions in the long-term future is that you will certainly be wrong. It is all too common for unforeseen events to stimulate new directions. For example, prior to 9/11, there was staunch resistance in the UK to the idea of a national ID card. Since 9/11 and subsequent terrorist attacks, the picture has been considerably changed by the imminent introduction across the globe of national ID cards and passports supporting biometrics. Technology roadmaps are a snapshot of how the future seems now and need to be kept alive by being revisited and refreshed on a regular basis.

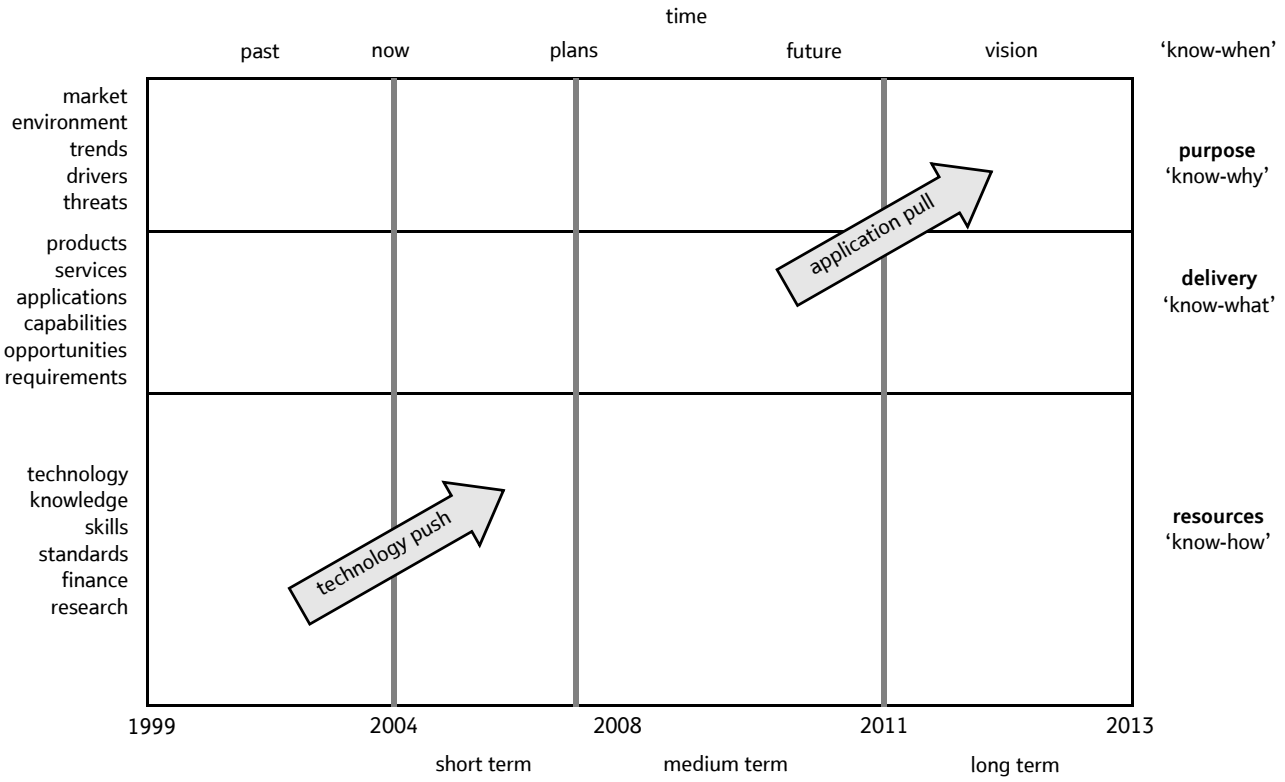


Fig 1 Generic roadmap chart.

Experience in the construction of technology roadmaps shows that the following critical success factors need to be considered in order to maximise the benefits [2]:

- include the right people:

  — the lead stakeholders need to provide effective leadership in taking ownership of the technology roadmap and defining its scope and purpose,

  — the appointed experts need to be competent and objective and have a breadth of experience beyond the client domain,

- there must be commitment from the client to ensure continued funding to maintain the technology roadmap,

- the technology roadmap conclusions must be implemented, and regular updates of the technology roadmap planned, to reflect changing needs and maturing technologies,

- there should be a dissemination plan to capitalise on the technology roadmap and ensure increased participation,

- as well as the technical barriers, the technology roadmap should paint a realistic picture of the non-technical barriers (e.g. legislation),

- the technology roadmap should provide broad recognition of competing technologies.

These roadmap charts allow the full picture to be seen for the first time. They provide clarification of the barriers to progress and highlight opportunities for reducing critical time-scales (see Fig 3 in the next section).

3. A real example — person identification for policing

Effective person identification is becoming increasingly central to law enforcement. The police are interested in whether they have already met a suspect before and what they know about them, such as whether they have a criminal record, whether they are armed and violent, etc.

Working with the UK Police Information Technology Organisation (PITO) in 2003, Consult Hyperion built the biometric technology roadmap for person identification within policing. The work was inspired by the EU Biovision project [3] that was under way at the time, and the aim was to provide the police with a focused long-term view of biometrics and highlight areas where specific action is necessary in order to ensure the technology can be harnessed in time to meet their needs.

The original PITO roadmap was completed within three months by a small team focused on specific requirements. By contrast, Biovision was a multi-national project considering a wide range of needs across sectors and did not include any roadmap charts in its final form. In April 2005, Consult Hyperion was asked to perform the first update of the roadmap [4]. The Consult Hyperion approach to the original PITO biometrics roadmap is shown in Fig 2.

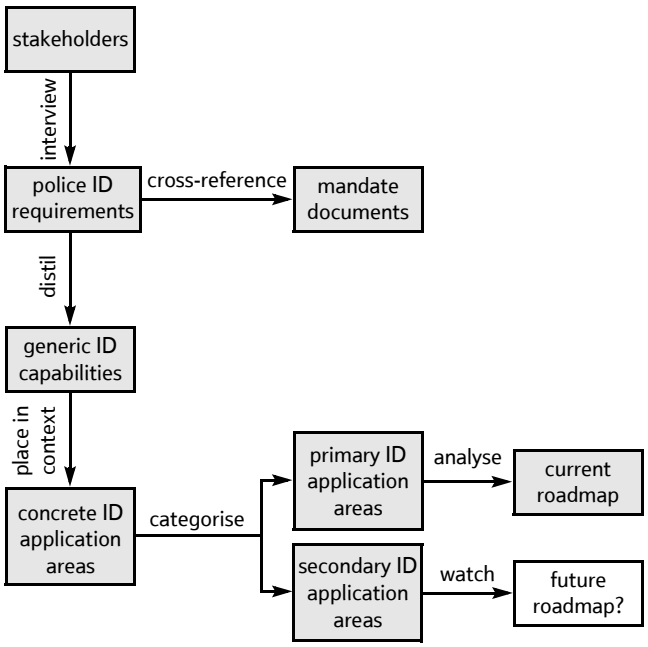


Fig 2 Approach to building the PITO roadmap.

Application of the technology roadmapping approach presents considerable challenges, as the roadmap itself, while fairly simple in structure and concept, represents the final distilled outputs from a strategy and planning process. The development of an effective roadmapping process within a business is reliant on significant vision and commitment for what is an iterative, and initially exploratory, process.

Extensive interviews were carried out in order to collect the widely distributed requirements across the Police Service of England and Wales. From this, Consult Hyperion drew up the business requirements for person identification which were distilled down into generic (more abstract) identification capability areas in order to prevent any duplication of requirements hidden by the different wording used during the interviews.

As a concrete example, let us look at an actual application area — identification of individuals at the point of contact. For police out in the field this effectively means having mobile devices capable of assisting them in identifying individuals.

The timeline used for the roadmap charts stretches from the present to 2020 (see Fig 3). Separate layers were included in the diagrams for the following:

- police applications using biometrics to perform a specific operational function,
- drivers, such as Home Office strategic documents, that give impetus to a particular application,
- inhibitors that could delay the introduction date of applications if a particular external activity does not coincide with technical development (e.g. passing of new legislation),
- central police products and programmes designed to meet identification needs, such as the existing national fingerprint system,
- technology necessary to enable products (often developed by suppliers),
- research necessary to enable the technology.

This roadmap chart shows that the Criminal Justice Act changed police powers in 2003/4 to enable fingerprints to be taken from all arrestees at custody centres. Subsequently, existing mobile fingerprint readers are being used to identify the occupants of vehicles stopped as part of intelligence-led operations. In the near future, it is likely that this service will be rolled out using the robust and secure mobile carrier, Airwave, which is now installed in all police forces. Once the national police mugshot service (FIND) is live, it can be foreseen that additionally returning a mugshot of persons matched by fingerprint would be a valuable confirmation of identification of the person in front of the police officer.

In the longer term, it might be possible to perform facial recognition or match DNA samples on mobile devices in real time, and perhaps fingerprinting could then be dispensed with.

4. Any time, any place, anywhere

Thus it can be seen that technology roadmapping provides a solid foundation paving the way towards a desired vision. Another project Consult Hyperion conducted at PITO was to determine the best deployment option for a national facial image database (FIND), allowing UK police forces to co-operate in the exchange of ‘mugshots’ and, ultimately, video images. The study considered mobile access (using various devices), allowing the policeman on the beat to verify identity without needing to return to the local police station, saving considerable amounts of resource.

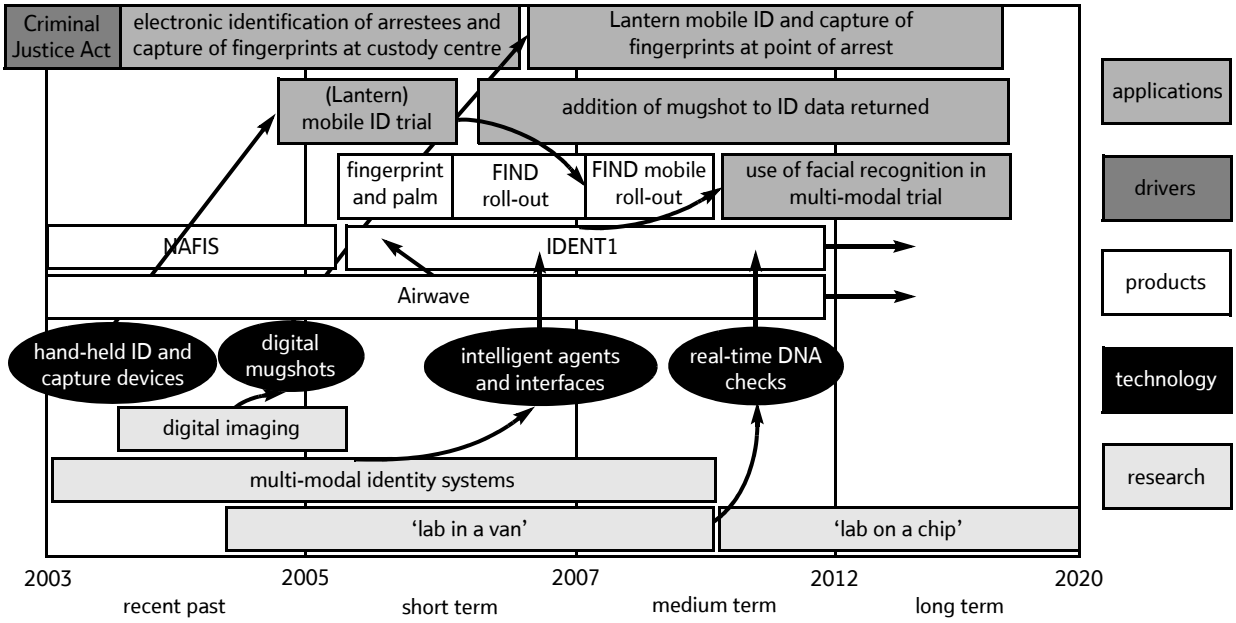


Fig 3 Sample roadmap for identification at the point of arrest [4].

One possible vision for law enforcement is that officers might wear a visor and infra-red camera that can transmit pictures of what is currently in view via a Bluetooth interface to a radio for sending to others. Relevant intelligence information might be automatically downloaded to their notebook computer, using a wireless local area network (WLAN) connection (see Fig 4). Some of this is happening already. For example, the police are undertaking trials on the use of mobile data terminals in cars to take fingerprints from suspects and have them matched against the central police database in real time (project Lantern trial shown in Fig 3).

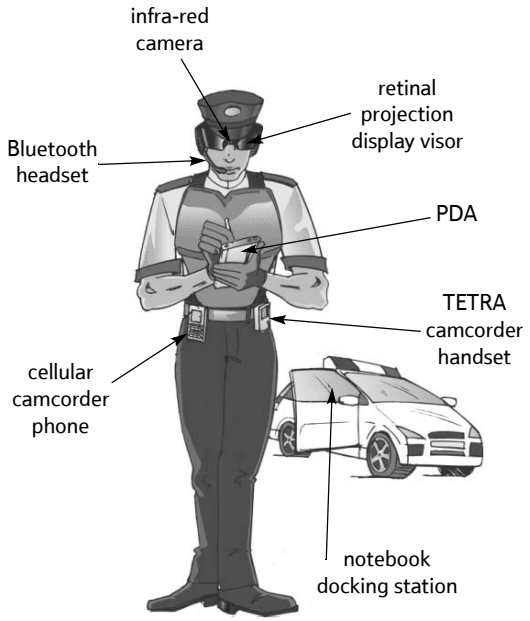


Fig 4 Vision of joined up networks in policing (source: Consult Hyperion).

5. Status check

As mentioned above, technology roadmaps should provide broad recognition of competing technologies. In terms of biometrics, the various technologies are intrinsically very different (consider fingerprints versus body odour). Each is appropriate for its own set of application and maturing at a different rate.

As well as biometric technologies, supporting technologies such as smartcards, cryptography and intelligent agents were examined. It is important to remember that, without these, biometrics technologies would be impractical and therefore it is equally important to track their evolution. For example, when contactless smartcards and readers begin to interoperate in the next year or so, it will make sense to commence international deployment of biometric e-passports based on these technologies and standards. This was not the case in 2003 when the International Civil Aviation Organisation (ICAO) began its specification of e-passports using these immature technologies. The delays ICAO has experienced were anticipated by us back in 2003 [5], and the embarrassment suffered by the US Visa Waiver Program could have been avoided. The deadlines for e-passports slipped by 12 months, and further delays are expected to be encountered.

Each technology was scored against the current identification requirements gathered from the police service. This resulted in the snapshot assessment of the technologies considered for PITO (Fig 5). Note that additional identity management technologies were considered beyond the field of biometrics such as intelligent agents (for presenting the right information

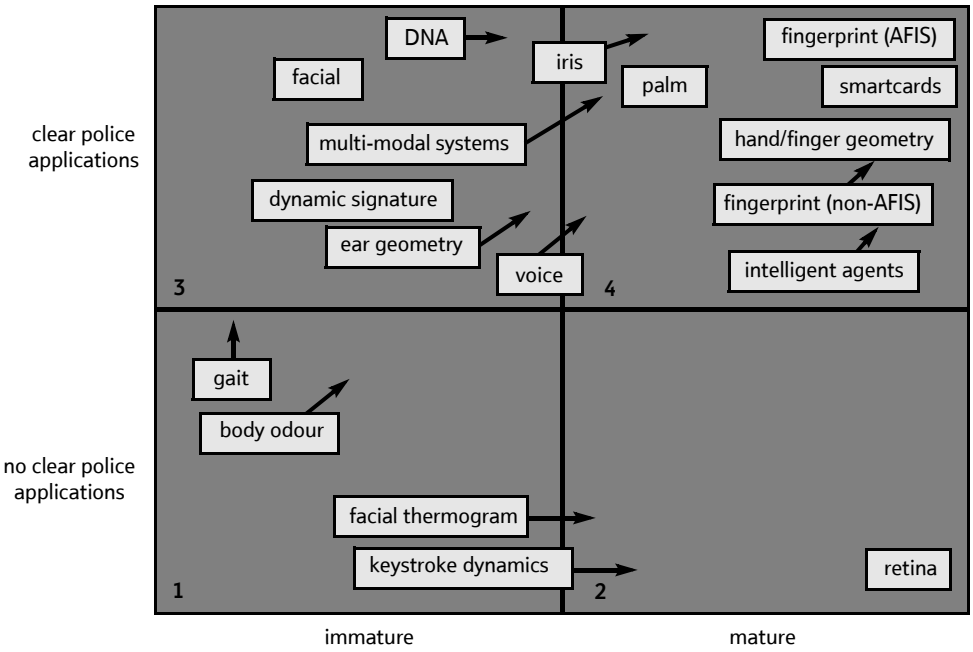


Fig 5 Technology assessment.

to each specific user) and smartcards (for providing portable tamper-resistant cryptographic security tokens).

Some of the more well-known identification technologies and some of the important aspects of their evolution for use in policing applications are considered below.

5.1 Fingerprint

Fingerprint details are believed to be unique to each person (and each finger). Fingerprints are one of the most mature biometric technologies used in forensics and thus have a stigma of criminality associated with them. However, this stigma is decreasing as more and more 'civil' biometric systems come into the public domain such as the US-VISIT immigration control at USA borders.

Automatic fingerprint identification technology is mature and has been used in law-enforcement domains for several years. Therefore, most recent activity in this area has focused on improving ease, accuracy and security of fingerprint capture. Developments in sensing technology have resulted in several ink-less (often referred to as livescan) fingerprint scanners. Compared to the ink and paper-based methods traditionally practiced in law-enforcement environments, this technology is easy to use. The introduction of integrated circuits and other technologies has made it possible to shrink the sensor size to the area of a postage stamp so that the sensors fit in laptops, mobile telephones and personal digital assistants.

However, compared to rolled prints and ten-print cards, these 'flat-print' sensors produce less information about a finger. Automatic identification of images of such small fingerprint portions requires complex algorithms similar to the algorithms used for conventional latent fingerprint identification used for marks found at the crime scenes.

Novel fingerprint capture techniques have been gaining attention to overcome the ease with which traditional 'capacitance fingerprint-capture' systems have been spoofed. Such systems include non-contact 3-D imaging of all ten fingerprints in a single reading and are claiming to be able to collect prints of quality equivalent to traditional 'rolled' fingerprints used in policing. Fingerprint systems using ultra-sound claim to accurately image a fingerprint and overcome problems with contaminates (i.e. dirt and grease transferred from finger in the normal course of fingerprint capture).

Mobile units that provide fingerprint capture capabilities at a remote site are seen to be the area of strongest growth. PITO is already working on mobile fingerprinting demonstrators that look set to save considerable amounts of police time wasted in deciding whether to arrest a subject in order to take them in for formal identification (see Fig 3).

5.2 Iris

Person identification techniques based on mapping images of the pits and furrows that make up the iris which surrounds the pupil in the human eye have become increasingly popular in the last few years. The pattern of the human iris is determined by the chaotic

morphogenetic processes during embryonic development and is believed to be unique for each person and each eye. Once stable, the pattern does not change with age, and rarely suffers damage.

The technology can now be installed as software into commonplace computer and digital camera infrastructure without the need for specialist hardware. Iris-matching systems claim some of the highest accuracy rates and, unlike most biometric systems, are capable of operating in a one-to-many (identification rather than verification) mode at all times. This is possible because of its ability to search accurately and extremely quickly across large databases. Potentially a biometric of such speed and accuracy could move human-to-human identification into a position where human operators are made unnecessary.

New technology developments enable both eyes to be captured automatically from distances, not requiring the user to step up close and peer into a camera — usability and technology trials are currently under way.

The large scale deployment of iris technology is currently hampered for two reasons.

- Lack of evidence

  Unlike fingerprint, there are no large-scale implementations in the world today that can be pointed to as a proof of the theoretical performance against large number of enrolled persons. The largest is in the United Arab Emirates (UAE) where approximately 550 000 individuals are enrolled as expellees not allowed back. More than 22 000 matches have so far been found between persons on the watch list and persons seeking re-entry. According to the UAE Ministry of Interior, all of these matches have ultimately been confirmed by other records.

- Lack of base data

  Most countries do not have existing iris databases of their population, meaning that any such venture would have to build such a database from scratch without the benefit of cross-checks against databases of known persons.

Iridian has relinquished its concept patent(s) on the use of iris as a biometric a year early. This is largely in response to ICAO's insistence that it would not include proprietary technology in its international passport specification recommendations. While Iridian retain its patents on the algorithms used to extract and match the iris feature space used in their biometric systems, the field of iris technology is now open to all vendors and advances in the field are more likely.

5.3 Face

Biometric systems based on face recognition have an intuitive appeal because people most commonly use facial inspection to identify others. These systems work in a variety of ways, most commonly they measure the relative positioning of key features to each other (eyes, nose, mouth, etc), or assess the differences between a captured facial image and a 'standard' (eigen) facial image.

Similar to the way fingerprint matching works for one-to-many checks, facial recognition systems often return a range of possible matches that then require human intervention in order to select the 'best' match. However, a big advantage of a facial biometric is that the ability to recognise and compare face recognition is innate to humans, unlike say interpretation and matching of an iris, or fingerprint pattern that takes training and experience.

These systems are not highly effective in uncontrolled environments. Even the vendors of such systems admit that a good frontal image of the faces of persons to be identified needs to be captured by the system's cameras in order for the matching process to work. On the other hand, face recognition used in controlled settings based on one-to-one matching can be more effective.

In the USA, NIST has launched an effort called the Face Recognition Grand Challenge. Given the relatively poor performance of face recognition, the challenge set is to improve the performance of still and 3-D facial images by an order of magnitude. With a false accept rate of 0.1%, the current error rate is 20% and they seek to lower this to 2%. This implies that out of 50 000 match scores there are 1000 errors.

The next logical step foreseen for facial recognition is to migrate from a 2-D model to a 3-D model. 3-D facial recognition is being championed as a means of overcoming the problems experienced by computer analysis of faces. Where 3-D technology is likely to improve facial recognition is the creation of systems that can synthesise full-face images from oblique angle facial capture.

The major milestone that is coming in the facial market is that of full and operational 3-D facial systems. Work has been ongoing in universities and laboratories for some time in this regard and it is expected that commercial systems will be stable by around 2008.

5.4 DNA

There is debate as to whether DNA[1] is a true biometric. The International Biometric Group states that DNA differs from standard biometrics in several ways:

[1] Deoxyribonucleic acid, the molecule that encodes genetic information.

- DNA requires a tangible physical sample as opposed to an impression, image, or recording.

- DNA matching is not done in real time, and currently not all stages of comparison are automated.

- DNA matching does not employ templates or feature extraction, but rather represents the comparison of actual samples.

DNA is very similar to biometric technologies inasmuch as it is the use of a physiological characteristic to verify or determine identity. It cannot yet be used to provide timely and automated person identification, but it is important that it be considered since it is expected to be a major component of future systems within the criminal justice system.

DNA identification relies on matching repetitive sequences known as markers. In the UK, forensic scientists tend to use 10 of these markers, or loci, to link a person to a crime scene sample reliably. The technique can also be used to identify victims of disasters such as the Asian tsunami by using the DNA of relatives or DNA from a missing person's toothbrush, for example.

Currently technology exists for DNA matching, but it is a time-consuming task and has a large portion of manual processing. The UK National DNA Database, established in 1995, is an important tool in the fight against crime and fear of crime. There are now 3 million DNA profiles, developed from samples of people on the database. There is a 40% chance that a crime scene sample will be matched immediately with an individual's profile on the database. In a typical month, matches are found linking suspects to 15 murders, 31 rapes and 770 motor vehicle crimes. It is clear that DNA evidence is a powerful aid to crime investigation and detection.

In 2004, there were around 21 000 detections in crimes where DNA evidence was available, a 132% increase since 2000. In crimes where a DNA profile has been obtained, the rate of crimes solved increases to 37% from the overall average of 24%.

It is also expected within the next few years DNA sampling equipment will become cost effective and small enough in size to be located at distributed locations within the police force. Mobile DNA labs are likely to appear as a significant step towards real-time processing of DNA samples — 'Lab-in-a-van' (see Fig 3).

5.5 Summary comparison

Table 1 summarises at a high level the characteristics and differences between the four biometric technologies considered above. This is intended to help the reader compare the technologies, but it must be remembered that performance is dictated largely by the particular application environment, making comparison difficult.

6. Conclusions

This paper has given a flavour of the issues arising from the diversity of biometric technologies, their status and speed of evolution. Technology roadmaps are powerful strategic tools that allow gaps to be identified as well as barriers. Armed with a view of this information for the first time, organisations can plan to remove or work around the barriers and plug the gaps so as to ensure that they can fulfil their ambitions within desired timescales.

The PITO identification roadmap, given as an example, sets out a vision for how identification technology can best be used to provide the police service with real operational benefit over the next 15 years to 2020. PITO does not have the power to achieve this vision alone. The potential future applications and the operational benefits they provide will only become reality if enthusiastically supported by the police service, the wider criminal justice system and central government. The identification roadmap is a tool to help encourage that enthusiasm through the communication of the 'bigger picture'. Similarly, having a technology roadmap does not mean an organisation's vision is going to be achieved, but it does ensure that the vision is consistent and achievable, and it does provide a valuable tool for communicating, and achieving buy-in for, the vision, giving it the best chance of future success.

Another key benefit of technology roadmaps is the flexibility they give to a corporate strategy. If the roadmap is properly maintained, it is far easier to evolve the strategic direction of the organisation in a way that is consistent with long-term goals, while maintaining a realistic and up-to-date view of what is happening in the wider world.

For example, when asked to review the PITO identification roadmap in 2005, the review of the primary police application areas showed that these findings are still valid, but additionally highlighted new areas where PITO had an opportunity to positively influence the development of identification services for policing. Working within an existing technology roadmapping framework enabled PITO to evolve their long-term identification strategy rapidly and with clear purpose.

Table 1 A summary of the characteristics of and differences between four biometric technologies.

Technology / Factor	Fingerprint	Iris	Facial recognition	DNA
General characteristics	Primary identity used for many criminal justice and immigration procedures for the last 10 years.	Relatively new technology but now being rolled out in some national border control applications. Systems designed to return automated absolute match/no match responses rather than lists of possible matches.	The biometric used by humans to naturally identify each other enabling enforcement officer crosscheck with minimal expertise. No specialist hardware required to capture facial images.	DNA is powerful because it can provide more information than identification, such as blood relationships to others. This can be useful in identification applications such as large disasters killing the general public who are not on existing databases.
Maturity	Well established technology. Accepted for many years in court of law (experts can corroborate).	Recently started being rolled out — still learning about integration into different application environments. Extent and nature of exception cases needs to be addressed.	Least effective of the technologies compared here for automatic recognition, though performance can be good in the right conditions. Therefore, facial biometrics are not used in many rolled out systems to date.	UK national DNA database established in 1995. Used in policing applications, but not yet mature enough to provide portable automatic solutions.
Identification/enrolment performance	Multiple fingerprints required to maintain accuracy over large databases. Used for largest biometric databases to date.	Highly effective matching on database sizes to several hundred thousand. No examples of 'population-scale' databases to date.	Least effective technology for 1:*n* matching. However, starting to be used to spot multiple enrolments, e.g. driving licence, passport, where no other biometric is available. Work on 3-D facial recognition likely to improve performance.	Highly accurate in large populations.
Degree of automation	Operator assistance required for rolled prints capture. For larger databases, often returns a list of possible matches requiring expert human follow-up inspection.	No 'man handling' necessary at enrolment. No contact with machine necessary — relatively easy to use. Facial images can be captured at same time providing multiple biometrics with no additional inconvenience.	Performance not good enough to be used without human verification. However, human verification is relatively easy compared with the other technologies.	Not automatic — DNA comparison currently required to be done by experts in a lab. Expecting to see mobile lab-in-a-van approach in next few years.
Some issues	Fingerprints of under-5s change (stretch) too frequently for this to provide an accurate historical record. Contact required with reader apparatus — perceived hygiene concerns in some people groups. New contact-free readers are emerging to address this issue.	Experts cannot corroborate an iris image pattern matching (e.g. in court of law).	Covert capture of facial image is possible (e.g. CCTV). However, image needs to be captured in correct lighting and aspect for good performance.	Not yet automatic and therefore not yet considered to be a biometric technology. Social implications since DNA matching can be used to determine family relationships and some health issues as well as to identify an individual.

References

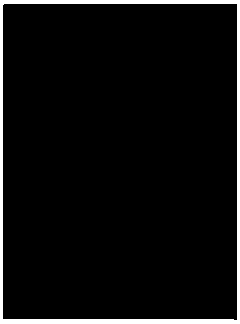
1 Phaal R et al: 'Technology roadmapping — a planning framework for evolution and revolution', Technology Forecasting and Social Change, North Holland (May 2003) — http://www.sciencedirect.com/

2 'Technology planning for business competitiveness: a guide to developing roadmaps', Emerging Industries Occasional Paper 13, Emerging Industries Section, Department of Industry, Science and Resources, Australia (August 2001) — http://www.ist.gov.aus/industry/emerging/

3 'BIOVISION, Roadmap to successful Deployments from the User and System Integrator Perspective', prj number IST-2001-38236, EC roadmap in preparation for Sixth Framework of support for R&D.

4 PITO: 'Part 1: Identification Roadmap 2005-2020', (April 2005).

5 'Crunch Time', Card Technology, 9, No 2, p 52 (March 2004).



John Elliott