IDNewswire®
Trends in Personal Identification and Biometrics

www.cardtechnology.com

Vol. 3 No. 3 February 4, 2004

NASA Smart Card ID Blasts Off Pg. 4
NASA announced this week it has awarded a contract for a smart card ID project that will control employee and contractor access to secure facilities and information systems.

Japanese Condo Using Biometrics Instead Of Keys Pg. 4
Bionics is offering blood cell recognition for physical access.

Mexico Chooses Bioscrypt Pg. 4

A New Dimension For Facial Recognition

Facial recognition biometrics will see widespread deployment in the coming years as countries around the world equip their passports with digital photos to verify the identity of the document holder.

The problem, up until this point, has been the less than stellar accuracy rates of facial recognition systems. The Facial Recognition Vendor Test 2002, released last year, showed the best systems correctly performed a one-to-one match 90% of the time under controlled conditions. With potentially hundreds of thousands of individuals being processed daily, and lighting and other conditions not necessarily ideal, there are real questions about whether facial recognition will be accurate enough.

That provides an opening for an emerging type of facial recognition biometric, three-dimensional. Instead of just looking at the height and width of a face, 3D measures depth, which vendors claim leads to greater accuracy. 3D faces several obstacles, however, including the fact that existing photos could not necessarily be used with a 3D system, the cost of the cameras and the lack of extensive testing of the technology. Meanwhile, two-dimensional facial recognition vendors are working on various ways to improve the accuracy of current systems.

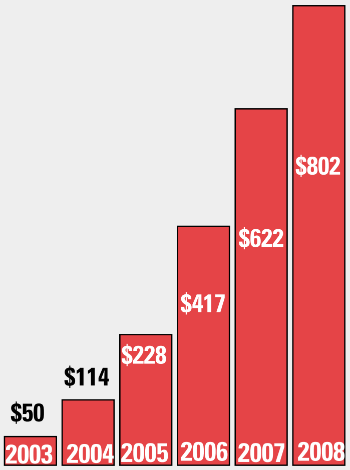
The facial recognition market is expected to explode in the coming years as countries across the globe start using the technology extensively at border crossings. The New York-based International Biometric Group predicts facial recognition will grow from a $50 million market in 2003 to $802 million by 2008.

Travel documents are the primary driver for this growth. Last

> 3D, Page 2

Facial Recognition Revenue 2003-2008

(In millions of dollars)
Source: International Biometric Group



Fraudsters Phishing For Consumer Info, Banks Step Up Education

It begins with an e-mail. You look at your inbox and see a message from Citibank, Bank One or eBay.

After opening the e-mail a link appears. The e-mail instructs you to click on the link and enter the appropriate information — either a PIN, user ID/password, or Social Security number — in order to verify an account, use an ATM or for a variety of other reasons.

If you're a savvy consumer you might realize something is amiss. Perhaps you don't have an account with the bank that sent the message, or words are misspelled or the sender's e-mail address doesn't look right. But enough consumers fall for this ploy — called phishing — to make this one of the newest ways to lure customers into giving up information about themselves.

Consumers who click on the link and provide the information requested might find themselves a victim of identity theft or another type of fraud. With "phishing" apparently on the rise, financial institutions are working on ways to protect customers from these scams and security software vendors are trying to figure out how to combat the problem.

The term phishing (pronounced fishing) is a hacker

> Phishing, Page 3

Biometric Passports Deadline Likely To Be Missed By Many

Only a couple of the 27 Visa Waiver countries will be ready to issue biometrically-enabled passports by this October, raising the possibility that the U.S. government will extend its deadline for new border control security or face the prospect of having to issue many more visas.

A hearing last week in front of the House Select Committee on Homeland Security's Subcommittee on Infrastructure and Border Security discussed some of the problems with the proposed new passports that are to carry biometric data.

Under the Enhanced Border Security and Visa Entry Reform Act, passed by Congress in 2002, Visa waiver countries—those major U.S. allies whose citizens can enter the United States with just a valid passport—must have programs in place to issue machine-readable travel documents with biometrics by October 26. The International Civil Aviation Organization, the group that sets standards for travel documents, decided last May that facial recognition will be the primary biometric used and that a digital photo would be stored on a contactless microchip in the new passports.

Maura Harty, assistant secretary of state for consular affairs, testified that the department

> Passports, Page 4

IBG Forecasts The Biometric Market 2003-2008

The New York-based International Biometric Group looks at specific biometric technologies and how they will fare in the coming years.

> IBG, Page 5

A Bad Phishing Example

IDNewswire staffers are not exempt from receiving e-mails attempting to pry information from them. Check out one of the latest attempts.

> Phishing, Page 3

> 3D, Page 1

May, the Montreal-based International Civil Aviation Organization selected facial recognition as the biometric of choice for passports. Digital photographs will be stored on chips that will communicate with readers via radio frequency. ICAO also allows countries to use fingerprint and iris biometrics in addition to facial recognition.

With facial biometrics likely to be widely adopted, traditional vendors are working to make their systems as accurate as possible, and 3D vendors have entered the fray. There are at least ten 3D vendors working on systems. How close they are to offering a commercial product is up for debate. When interviewing vendors six months ago, Tony Moore, a senior consultant with IBG, says none of them had a commercially available product.

Moore, who has been following the development of 3D facial systems for IBG, says there are two different approaches to 3D facial biometrics. The first is active illumination and structured lighting, in which a pattern is projected on the face and a 3D image is mathematically derived. This is the more common approach to the technology.

The other type is passive stereo, using two cameras to capture an image, Moore says. "This approach is computationally very intensive," he says. "It might take three or four years before computer power can increase to go this way."

Moore says 3D technology looks to address the shortcomings of traditional facial systems. "The two biggest problems with 2D is dealing with different poses and variable lighting conditions," he says. "3D has a real opportunity to address both these issues."

‘The two biggest problems with 2D is dealing with different poses and variable lighting conditions. 3D has a real opportunity to address both these issues.’

— Tony Moore, International Biometric Group

The main drawback for 3D facial biometrics is the camera cost. While traditional digital cameras cost hundreds of dollars, it’s expected that 3D camera may cost thousands of dollars.

Cupertino, Calif.-based 3D facial recognition vendor A4Vision Inc. is selling its cameras for $1,400, but hopes to get the price down to the $400 to $500 range by the third quarter, according to Grant Evans, the company’s CEO.

The company is focusing on the physical access and identification markets, Evans says. He claims the company’s system can verify an individual’s identity in a dark room.

A4Vision’s technology uses near-infrared light which projects a grid that is distorted by the topography of the face. This allows A4Vision’s camera to capture 60 degrees of an individual’s face, or all the way back to the ears, whereas most cameras only capture 50 degrees, Evans says. Enrollment in the system takes about eight to ten seconds.

Evans says its facial recognition systems have been tested by undisclosed independent third-party institutions and, in some cases, A4Vision’s system is almost 15% more accurate than the top 2D systems.

But what might be the best type of facial system, in terms of performance, is a combination of 3D with 2D, Evans says. Using both types of systems allows for the best algorithms from each to be used. A4Vision has teamed up with a 2D facial recognition vendor to integrate both the systems, but he would not name the 2D vendor.

A4Vision also is working with Philadelphia-based Unisys Corp. to test its 3D system. Last year Unisys received a U.S. Department of Defense contract to research biometric systems for physical access control, border security, and authentication for computer and network log-on.

Separately, Unisys also worked with Minnetonka, Minn.-based Identix Corp. to explore whether three-dimensional facial geometry algorithms improve accuracy compared with two-dimensional approaches. The team also studied how conventional photographs can be converted into three-dimensional models that incorporate information on texture, facial expression and aging.

Joseph Atick, CEO of Identix, doesn’t see 3D face being a commercially viable solution yet. He says the system is good for solving the posing problem — 2D systems have trouble recognizing individuals if they are posed differently than in the enrollment image — but otherwise has not shown significant improvement over current 2D technology. Littleton, Mass.-based Viisage Technology Inc., a 2D facial recognition vendor, is doing some research and development with 3D face but doesn’t have a product ready, says John Dorr, vice president of marketing at the firm.

A 3D facial recognition access control scanner from A4Vision

He says 3D face has the best chance for success in access control. But that market is quite cost-sensitive and customers might be unwilling to pay the high price for 3D scanners, he says.

The technology is less likely to succeed as a surveillance tool, Dorr says. "There is no portfolio of 3D images to compare against," he says.

Before 3D facial recognition catches on there will have to be independent testing to confirm vendors’ accuracy claims. The U.S. National Institute of Standards and Technology, a division of the U.S. Department of Commerce, is just starting to collect data for testing 3D systems, says Charlie Wilson, manager of the Imaging Group in the NIST IT Lab. "We haven’t measured it well enough, but are just starting to collect data," he says.

NIST is making some headway in improving accuracy using 2D facial biometrics with multiple photos, Wilson says. A report scheduled to be released this week shows that using multiple photos in a controlled environment can achieve 99% accuracy with a one-to-one match. The multiple photos are used to show the different angles of an individual’s face, Wilson says.

NIST is performing further research into this area to find out how many photos provide the best accuracy. "We know that two is better than one and three is better than two, but we don’t know how many is ideal." This could lead to more than one photo being stored on the new biometrically-enable passports. <

> Phishing, Page 1

term for luring "fish," that is, gullible consumers, into providing account information or financial data, according to the anti-phishing.org Web site of the Anti-Phishing Working Group. Hackers commonly use "ph" instead of "f," the Web site states.

This scam has been around since the mid-1990's, but has become more prevalent in the past year. Over the past holiday season phishing attacks jumped 400%, according to the Anti-Phishing Working Group. The organization, comprised of various software vendors, Internet service providers and financial institutions, estimates that more than 60 million phishing e-mails were sent out during the holiday season in an attempt to take advantage of consumers' confusion during the busy time of year.

Protecting consumers from these attacks is not that easy, says Dave Jevans, co-chairman of the Anti-Phishing Working Group. Jevans is also a senior vice president at Redwood City, Calif.-based Tumbleweed Communications Corp., a provider of online communications software.

Stronger authentication would prove one antidote to prevent phishing, Jevans says. "The only sure-fire, 100% way to stop it is strong authentication and give people a smart card or secure token to log-in with," he says. "The problem with that is it's infeasible; you're looking at $100 to $150 a person."

Jevans says that properly educating consumers is the best place to begin. "Everything is based on education," he says. "Consumers need to know what to look for in an e-mail from a financial institution.

Chicago-based Bank One Corp. has been a target of these attacks in the past and is taking steps to protect its consumers, says Chris Conrad, senior vice president of the fraud management division at Bank One Card Services.

The home page of BankOne.com carries information on the latest phishing scams and gives consumers tips on how to protect themselves, Conrad says. "The Bank One Web site has greatly expanded information on e-mail related to fraud and abuse," he says. "It's constantly updated with examples of fraudulent e-mails and notification to our customers on what to look out for and how to notify us should the need arise."

Bank One also uses various technologies to try to stop the attacks before they happen, Conrad says. "On a basic level we monitor the Internet for domain names set up with the intent of attracting Bank One customers," he says. Some examples of spoofed names include citibankonline.com or visa-security.com. "We monitor that and we look for any information on Internet sites and message boards that may indicate a potential scam against our customers."

Since the phishing attacks have increased in the past six months many companies have begun offering services to help institutions prevent these raids. For example, systems from San Francisco-based Brightmail Inc. and the UK-based Netcraft scan the Internet for potential scammed domain names. Another solution is offered by Tumbleweed Communications. That firm offers a service that digitally signs e-mails so consumers know the messages are coming from the legitimate financial institution.

New York-based Cyota, a security software provider, rolled out FraudAction last week, which is designed to help institutions fight phishing attacks, says Naftali Bennett, CEO of Cyota. "The banks are in the dark during the attacks," he says. "They don't know until it's too late, and then they don't know who's been hit."

Cyota's FraudAction has multiple parts. The first service is a real-time alert of when an attack is taking place, Bennett says. Following an attack notification, Cyota can tell a bank when the attack occurred, how long it went on, where it happened, the estimated size of the fraud, and whether it was a high- or low-quality attack.

Cyota will also recommend a response to the attack. The company may recommend disregarding an unsuccessful attack, or it may tell the bank to shut down its site and notify customers of any potential risk, Bennett says. The recommendation depends on how large the attacks are and how many consumers responded to the phishing expedition. "We've seen response rates from 5% to 20%," he says.

Bennett would not name any institutions that are using FraudAction, but he says that Cyota was asked to look into the phishing problems by its customers. Bank of America, Bank One, and US Bank are among the institutions using Cyota's products. Bennett would also not discuss the cost of FraudAction. <

A Bad Example of Phishing

Sent from: norum@netsiam.com

_Dear Citi_Bank _Member_,

This message was _sent_ by-the Citicard _server to
veerify _your_ Email address_.
You mmust celmtpoe this poescrs by clicking on the_ link
below and enntering in the smmall _window your Citi-bank
ATM full card number and Pin that you use_ in the Atm_Machine.
That_is _done_ for_your pectortion -i- becouse some_of_our
memmbers no loengr have acecss to their email adedessrs
and we must verify it.

http://www.citibankcards.com:%69%6d0%42%78%68%6b4%58%4c%775@
%69%6c5%6d%66%64%6a4%62%2e%64%61%2e%52%55/%3f%4e%61%78
%6f%7a4

To veerify your_ E_MAIL adress and access your_ Online-Citibank
account, click on the link beelow.

cCvZTaJ48zEgTY

Source: IDNewswire Staff

> Passports, Page 1

has a program underway that should produce the first biometric passports by October. But other countries are not as far along as the United States.

"Visa Waiver Program governments have indicated that they will be unable to meet the legislatively mandated deadline to issue to their nationals only machine-readable passports incorporating this enhanced biometric identifier that complies with the standards established by the ICAO," she said during the hearing. "None of the larger countries (Japan, the U.K., France, Germany, Ireland, Italy or Spain, for example) will begin issuing passports with the ICAO biometric by October 26, 2004. Japan and the United Kingdom say they will begin in late 2005; others may not come on-line until a year after that."

State Department officials are working on the criteria for what constitutes a biometric-passport program, officials say. The agency is waiting for final specifications from ICAO before informing the Visa Waiver countries what will be required.

Harty did not directly say the deadline for Visa Waiver countries needs to be extended, but industry officials in attendance say there were allusions to a possible extension. The State Department cannot change the deadline; that would take an act of Congress.

A State Department spokesperson could not comment on whether the agency is seeking an extension, but the department is providing information on the situation to legislators. Sources close to the situation say the office wants the deadline to be extended and is working toward that goal.

Some officials say the deadline should be extended or there could be political fallout. "The longer this is put off the more of an issue it becomes in a political season," says one insider, who asked not to be named.

If the deadline is not extended, travelers from all countries not complying with the mandate will have to apply for visas, Harty says. "Since travelers from (Visa Waiver Program) countries with non-biometric passports issued on or after October 26, 2004 will need visas to travel to the U.S., we estimate that the demand for nonimmigrant visas will increase significantly over FY2005 to over five million applications, nearly double last year's workload," she testified.

Visa applications should return to normal levels after the countries are able to issue passports with biometrics, she said. <

NASA Smart Card ID Blasts Off

NASA announced it has awarded a contract for a smart card ID project that will control employee and contractor access to secure facilities and information systems. The agency will begin a trial of the new "One NASA" card at its Marshall Space Flight Center in Huntsville, Ala. in May, followed by expanded trials elsewhere. "If the field trials are successful, and we receive the approval of the Office of Management and Budget, we plan to deploy over 100,000 smart cards before the end of the 2005 fiscal year," said David Saleeba, assistant administrator for security management and safeguards at NASA, in a news release. A spokesperson for the U.S. General Services Administration, which awarded the $93 million contract to Reston, Va.-based Maximus Inc., says the One NASA card will serve as a pilot for other government programs. NASA has been working with the National Institute of Standards and Technology and other federal agencies for two years to plan the ID initiative. The One NASA card will have both contact and contactless chips and be used to gain physical access to restricted areas and logical access to computer networks. Biometrics will not be used with the card. <

New Biometric Technology May End Search For Door Keys

Future condominium owners of a building under construction in Osaka, Japan, will not have to search frantically for their door keys thanks to an alliance between a biometrics company and JCB Co. Ltd., Japan's largest credit card issuer. Tokyo-based JCB is working with Bionics Co. Ltd., an Osaka-based biometrics vendor, to deploy blood-vessel pattern authentication to residents of a 156-unit condominium that will open March 2005. The biometric system works by using an infrared light to capture individuals' unique blood-vessel pattern, Bionics said in a statement. After enrolling in the system, the building's owners will be able to unlock their condo doors without a key, according to a JCB release. Residents also will be able to make purchases in the building's service center using the biometric system. The store will charge the purchases to residents' JCB credit cards. Bionics' Web site says individuals can be verified by the system in one second. <

Mexican Government Selects Bioscrypt For Physical Access

Toronto-based Bioscrypt Inc., a fingerprint access control system vendor, deployed its scanners at the Mexican Ministry of Agriculture for physical access control and time and attendance applications, the company announced late last month. The deployment is designed to provide increased security to restricted areas of government buildings while also verifying attendance of the over 1,500 individuals working for the department. <

IDNewswire®
Trends in Personal Identification and Biometrics

Editor
Zack Martin
zachary.martin@thomsonmedia.com

Group Editor
Donald Davis
don.davis@thomsonmedia.com

Contributing Editor
Michael Fenner
michael.fenner@thomsonmedia.com

Advertising Sales
Jim Baker
james.baker@thomsonmedia.com

Publisher
Andrew Rowe
andrew.rowe@thomsonmedia.com

Group Publisher
Timothy Murphy
timothy.murphy@thomsonmedia.com

Thomson Media: *Pres. & CEO: James M. Malkin; Pres./CEO Publishing & Conference Group: Bruce Morris; CFO: William Johnston; SVP, Operations: Celie Baussan; CTO: Raymond Ouellette;VP, Business Development and Strategy: Greg Mazzanobile; VP, Human Resources: Robert DeNoia.*

IDNewswire® is published biweekly by Thomson Media. Visit our Web site at http://www.cardtechnology.com. The contents of IDNewswire are, and remain, the property of Thomson Media. Reproduction or forwarding of this publication is strictly prohibited. Individuals who infringe on these rights will be prosecuted to the full extent of the law. IDNewswire is a registered service mark used herein under license.

Subscribers who want multiple copies of IDNewswire should contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com for information. The annual subscription rate is $695. For subscription, renewal or licensing information, please contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com.

For advertising information, contact Jim Baker at 312-983-6179 or james.baker@thomsonmedia.com. Editorial offices are located at 300 S. Wacker Drive, 18th Floor, Chicago, IL 60606. Telephone: 312-983-6168. FAX: 312-913-1365.

THOMSON ™

IBG's Forecasts The Biometric Market 2003 To 2008

International Biometric Group

The following is the second part of an edited transcript from the Jan. 8 International Biometric Group teleconference with Michael Thieme, director of special projects at IBG, talking about the soon-to-be-released "Biometrics Market and Industry Report 2004-2008."

We have one more set of things to walk through: what are vendors doing well and what sort of technologies are we seeing that allow products to be adopted and adopted successfully. It's one thing to have demand, but you also need the second half of the equation, which are products that are capable of addressing that demand effectively.

Some of the major factors that we've seen – and these are not all new but they are important trends in the industry – are reduced price and increased functionality for things like access control and logical access systems. We're getting to the point now that we as an industry can secure a door biometrically for only a modest few hundred dollars, as opposed to a few thousand dollars. And those devices that are more expensive – let's say the $1,500 devices – are much more functional and more robust then they had been before.

And the corollary to that is the development of some logical, well-rounded product lines. For example, AuthenTec offers a large number of fingerprint sensors tailor-made for a specific type of application: access control, logical access, and device access. A few of their competitors have taken a similar approach. But certainly, that is a better approach than attempting to convince everyone to use a specific form factor or specific sensor when certainly it's not a one-size-fits-all solution.

A second trend that we are seeing in the industry – which is happening a little bit slower than we want, but it is a growth enabler for those looking for long-term solutions – is the development and the adoption of interoperability standards. These standards take a few different forms, and I alluded earlier to things like CBEFF and BioAPI. These are basically data formatting and application programming interfacing standards, which are of primary interest to developers.

We are starting to see the emergence of standards in more controversial areas as well. Standards for image and template formats mean that the interoperability problem–once viewed as a major problem – isn't solved, but at least there's a roadmap. These maps allow a deployer to use standards – in terms of how fingerprints are imaged, minutia stored, and facial images included – to be adopted, and they allow for migration from different technologies. And that's important.

With regard to fingerprint specifically–one of the central technologies of interest in the industry–continued reduction in power requirements and also in sensor size has been important. Sensor size reduction is controversial because the intuitive response is that small sensors might make it difficult to acquire sufficient data to provide accuracy.

But for the sorts of applications that are being targeted, often times it's as much as a convenience issue as it is a pure security issue. It's much easier for cell phone providers and PDA manufactures to incorporate their biometric technology without worrying about battery drain and that type of thing.

One last point I want to make here in terms of enabling growth from a vendor perspective. I think that there has been a fairly strong increase in the amount of credible and rational approaches within the industry. Biometrics are still young, but what we were seeing in the late 90's – what you might call outlandish claims of accuracy and functionality – have been replaced by more sober projections as far as what a technology can and can't do.

'Biometrics are still young, but what we were seeing in the late 90's–what you might call outlandish claims of accuracy and functionality–have been replaced by more sober projections as far as what a technology can and can't do.'

And really taking an intelligent approach to how biometrics fit within a company's overall infrastructure – be it a deployer or somebody who wants to implement the technology as part of a product line – much of the credit goes to the vendors. Many vendors in the industry have taken the time to become a bit more serious about how they address their potential deployer's business issues. These are some of the primary factors we've seen in the industry and, like I said, they ought to be further broken down by technology and application, but those are topics for another day.

We'll take a little bit of time right now to talk about some of the specific breakdowns, the numbers I alluded to earlier. We'll look at it from a couple different perspectives: one is biometric applications, and the other is biometric technologies. Those are the primary means by which we divide up the industry. Certainly it's valuable to look also at vertical or market-driven areas, such as health care. But often times what we find is that it is really the applications of the technologies that provide us with the best insight into the market space.

When we look at applications, our report tracks according to divisions. These divisions are the source of a lot of contention and it takes a lot of time to come up with them. Our first category–and this is the first time that we covered it–is called "Device Access." By "Device Access," we mean the use of biometrics for access to the use of a standalone piece of equipment such as a PDA or a cell phone. The category used to fit under things like PC/network access, but it's becoming a viable industry in itself, where people are securing devices, which usually will allow access to information.

In addition to "Device Access," we have the standard areas that we track, which are in order: criminal identification, e-commerce/telephony, retail/ATM/point-of-sale, PC/network access, access control, civil identification, and surveillance.

It certainly could be argued that surveillance perhaps belongs as part of criminal identification, or that civil and criminal identification are hard to split, but these divisions are meant to capture the fundamental elements of what makes a purchaser decide to go with biometrics, as well as the constraints on how biometrics can be implemented.

If we look at 2004 and how different applications break down, still the largest in terms of biometric revenue is criminal identification. It's not unreasonable to take the entirety of criminal identification and to bundle it as a separate area, because that industry is so much more established and proven, and it has much more regular sales tracks and is much more stable than the emerging areas like e-commerce and PC network access. But we do track criminal identification because it is important to quite a large number of vendors in the space, and to discount it would be to understate a lot of their revenues and a lot of their future potential.

The two applications that we project will account for the largest percentages of revenue

> IBG, Page 6

> IBG, Page 5

in 2004 are access control and civil identification. The projections are close enough to each other that it's really difficult to determine, within an acceptable margin of error, which one will be the largest. We project each one to account for approximately $260 million in global revenue, attributable mainly to four or five biometric vendors.

If you look at applications that are near that in size – and one that's been disappointing in the last couple years – we project that 2004 will finally be a year where there's some decent growth in PC/network access. Our prior analysis has often pointed to this being an area where revenues will get a lot of traction, but that's been superceded a bit by the Sept. 11, 2001, terrorist attacks and by a lot of emphasis on physical as opposed to logical security. Nevertheless, I do think things bode well in 2004 for the use of biometrics in PC/network access, which includes both enterprise and a lot of different types of remote access.

Other applications, which are still emerging, would include e-commerce and telephony, retail/point-of-sale, and surveillance. We should mention that each of those is tracked for pretty dynamic growth between today and 2008. Some of these figures will be available only in the report, others we'll put up on the Web site once we release them.

Technologies, like applications, are a pretty fundamental way of viewing the industry and oftentimes there are certain technologies that lend themselves very strongly to certain applications. For example, for any type of telephony-based solutions, voice biometrics works very well. Voice isn't often deployed in non-telephony based applications, but it is sometimes. The technologies that we cover include: fingerprinting, facial recognition, hand geometry, iris, voice and signature and there are a few other categories that are not quite as intuitive.

One is AFIS (automated fingerprint identification systems). AFIS is a market that we cover separately which includes any implementation of multiple fingerprint searching on a large database, and that encompasses quite a lot of hardware and software, a lot of professional services, and a lot of infrastructure.

Another space that we cover that is not completely intuitive is middleware. Middleware includes any software that's meant to tie more than one biometric to more than one application. Oftentimes folks who provide middleware prefer that it be called something else – identity management software, this or that type of infrastructure – but when push comes to shove, by our categorization it's all middleware. It's a very important space in the industry that is often overlooked or perhaps not covered at all.

One last area that we've just started covering this year as a "separate" area is multi-modal biometrics – the use of, let's say, fingerprint and face in a given system. Because multi-modal revenues are fairly small (we had them at only 11 million dollars for 2003) we actually don't count them at a separate category. Essentially multi-modal is tracked as an interesting component of the rest of the industry, but really multi-modal today is just comprised of let's say fingerprint, face and middleware. It is interesting nevertheless to know what percentage of those technologies are being implemented in a multi-modal fashion.

Our projections for 2004 for the fingerprint space are pretty aggressive. We have total global revenues – including things like civil ID, access control, logical access, sensors and enabling software – of more than $350 million, which is clearly a lot of money. That money is divided across dozens and dozens of companies from several different sub-segments that don't necessarily compete with each other so, while it is a large number, it's being shared by a lot of companies.

'As we look at the way technology grows out through 2008, one of the interesting things that we see is that facial recognition does emerge very strongly as the technology ranking second in terms of revenues to fingerprints.'

As we look at the way technology grows out through 2008, one of the interesting things that we see is facial recognition emerging very strongly as the technology ranking second in terms of revenues to fingerprints, approaching or exceeding slightly more than $800 million dollars annually by 2008. One of the very essential drivers of this growth is the use of facial recognition in passports and travel documents as is manifest in the ICAO decision to make facial recognition the baseline for interoperability in those documents.

Clearly there are going to be a lot of areas where facial recognition can be used in travel documents, despite it's current drawbacks, and that infrastructure is going to be one of the primary contributors to its growth.

We have fairly aggressive, we think, and realistic revenue projections for technologies such as iris recognition and voice verification. Iris recognition exceeds $350 million in our estimates by 2008, and voice exceeds $200 million. By 2008, it's hard to say whether the current composition of the market in terms of vendors and providers will remain or whether we'll have new providers – different, larger manufacturers – involved in this phase, but we do anticipate they'll be fighting over a piece of a much bigger pie.

One last area that we'll touch on very briefly is a new area that we cover in the market report: professional services or consulting and integration services. Of course the vast majority of that is in integration, as opposed to consulting, but it is interesting to cover and start getting a perspective on the industries that have propped up in and around biometrics.

You might have an amount of revenue change hands or amount of money generated where there's only a few thousand dollars in products from, let's say, government to private sector or private sector to government. But you also have several kinds of that being executed in testing, professional services, integration, evaluation, design and the whole engineering life cycle thing – which doesn't always get taken care of by the vendors.

A couple of the interesting things that we've seen is that when we start to boil down professional services revenue, we actually see that it is a somewhat more substantial part of the industry than just the core technologies.

A great way to illustrate this is if you think of an enterprise deployment. An enterprise deployment may involve, let's say, 1,000 sensors and a server component, and the sensors may cost $100 apiece. So you're looking at perhaps $120,000 in core revenue, but the integration of that solution – which often times wouldn't be executed by the biometric vendor but by a systems integrator or professional services firm – might be three, four or five times higher than that.

One of the interesting things we've tried to work out in the new report is to try to determine – for each application, like criminal ID, e-commerce, retail, etc. – what is the percentage of professional services revenue to core technology revenue? It is very interesting to see that, in some spaces, it really is the core technologies driving revenue growth, and in other spaces, it's the services in and around those technologies. <

For more information contact Mike Thieme at mthieme@biometricgroup.com or 212-809-9491.