

The identity crisis - what comes after the post 9/11 anti-terrorism hype

Beyond the nebulous concept of "enhancing security": the key to transforming biometrics from high-tech wizardry into practical ROI-based applications



The biometrics industry is in the midst of a post 9/11 identity crisis. While many vendors and industry pundits remain fixated on performance issues and high security requirements, progress is being made, albeit slowly, in shifting the emphasis from technology development to real world solutions deployment. This transformation has been particularly difficult for industry stalwarts who have learned to survive on research grants and laboratory test results. But it is business process improvement and consumer convenience that are the keys to biometrics adoption. They will provide the impetus and lay the foundation for substantial and sustainable market growth. A review of current biometrics market dynamics exposes those areas where "legacy thinking" continues to hamper market progress and points to places where market evolution has taken hold and begun its seemingly inevitable march towards mainstream ubiquity.

An industry lacking vision...

Biometrics is a market void of clear vision or leadership. No individual or identifying or branding force has emerged to drive the industry towards a well defined vision of the future. This is partially due to limited vendor resources spread across a highly fragmented industry and a valuation mentality that emphasizes positioning companies for the investment community rather than positioning them in the marketplace. Individual companies and the industry as a whole tend to realign hastily around the opportunity de jour rather than formulating comprehensive vertical market driven strategies.

This approach may address a short-term goal of the most basic sort - to stay funded long enough to stake a position in the market. But it is ultimately self-defeating. The real value of biometrics companies will be determined by end users, not financial analysts. Without a strong vision of how biometrics can enable commercial enterprises to address pressing business issues, to

achieve new levels of efficiency, effectiveness and customer service, there will be no compelling justification for broad based adoption. Post 9/11 anti-terrorist hype has actually exacerbated this situation by drawing energy and resources away from solving problems integral to the core competencies of commercial end-user prospects and towards the more nebulous concept of "enhancing security".

...and market leadership

In spite of the exaggerated claims of some prominent vendors, there are no "market leaders" in the biometrics industry. There simply has not been enough penetration in any single vertical market to claim leadership status. Press releases and marketing material do not make a leader.

There is however, one highly specialized company that can claim dominance in a narrowly defined niche market - Biometrica. This boutique firm, a Viisage spin-off, has focused exclusively and quietly on providing facial recognition solutions to US based casinos and claims to have achieved an 80% market share in this select niche. Biometrica was re-acquired by Viisage last year and now faces an increasingly uncertain future. With Viisage's focus on government sector opportunities and renewed interest in casinos by established and up-start facial recognition companies, Biometrica's market position is tenuous at best.

Government projects are for the patient and well funded

Development of large scale government projects is moving forward but at a pace

more likely to choke financially constrained biometrics vendors than to provide the critical mass of opportunities required to keep a significant number of these 200+ players in business. Post 9/11 US legislative initiatives are the center piece, and in many cases the driving force, behind much work in this area. Three of the most prominent programs launched in the wake of this regulatory onslaught - Trusted Traveler, TWIC and US Visit - continue to face operational, political and financial stumbling blocks. More than two years after 9/11 the US government has made no substantial progress on air, border or port security.

There is no doubt that civil ID, immigration and border control projects will materialize over time and offer significant opportunities for the privileged few. But even the recent Department of Homeland Security announcement that a five year Blanket Purchase Agreement has been issued to Identix for approximately \$27 million over 60 months carries no commitment or minimums. This appears to be the largest single "order" for biometrics on record. However, the order is for livescan AFIS systems (which many would argue do not belong in the same market category as other more interactive biometrics) and at \$5.4 million a year this is not a windfall for an organization whose gross revenues are in the \$80 to \$100 million range.

Many biometrics hopefuls are recruiting executive rainmakers with extensive government experience in the hope of cashing in on potential large scale programs. While this in itself is not a bad idea, exclusive focus on government opportunities will retard market growth in several ways. As noted, these contracts are materializing slowly, in piecemeal fashion, if at all. The big payoff is a minimum

of three to five years away, if not ten. Governments are also not inclined to single source technology, which means that interoperability issues within biometric categories must be resolved. This is no small task.

To date, there is no interoperability from one vendor product or device to another. This is particularly true for fingerscanning, which boasts the largest array of capture technologies and template and matching algorithms of any biometric category. And, in spite of the popular misconception among many government officials and bureaucrats, the BioAPI standard does not solve interoperability issues for biometrics. It simply allows multiple devices to operate in a single system environment.

In addition, COTS (commercial off the shelf) technologies are becoming the de facto preference for government solutions the world over. Customization of proven commercially available products provides a faster, more cost effective path to deployment than total custom development.

The bottom line for the biometrics industry is that exclusive focus on government and civil programs, at the expense of commercial market development, is a poor strategy for individual biometric company success and accelerated market growth. The big winners with regards to government projects will be large integrators, who will profit from providing infrastructure and expertise in designing, deploying and managing these large scale systems.

Capital is available

Contrary to popular lament, capital investment is flowing into the biometrics industry. Nearly \$100M was invested in biometrics



companies in the first 9 months of 2003 through public and private placement. Some notable placements have been made - A4 Technologies received \$3 million in March, AuthenTec closed \$18 million in April, Bioscrypt raised \$5 million in April, Ultra Scan raised \$18 million in July and Viisage brought in over \$13 million in September.

It is certainly true that the "cool" factor has lost its appeal as an investment criterion. James Bond and Minority Report don't sell stock. "Coolness", however, has been replaced with stringent analysis and thorough due diligence. This is a good thing for the biometrics industry. Vendors have been forced to think hard about solving high priority end user problems and developing compelling business cases based on quantifiable market analysis - not techno-babble and wishful thinking. This represents a powerful force for elevating the level of biometrics industry competition and encouraging progress towards market maturity.

Shift from security to identity protection

Post 9/11 biometric "market explosion" fantasies have thankfully just about completely

faded. According to an ASIS International study released in June 2003, median corporate spending on security measures had increased only about 4% in the US between 9/11 and the report publication date. The classic precept holds. Emerging technology is adopted because of business process improvement and convenience. Security can open the door but quantifiable ROI must always close it.

In this respect, the overarching concept of "identity protection" offers a much stronger foundation and compelling value proposition for developing biometrically enabled applications than simply "enhancing security". In addition, it moves the discussion of biometrics away from the 100% accuracy and reliability problem to how much of an improvement or cost savings this technology can provide over existing processes and systems.

Recent research in the US and UK indicates that identity theft and fraud pose significant threats, not only to consumers but to businesses and governments as well. According to the FBI and the US Federal Trade Commission, identity theft is the fastest growing crime in America with more than

12% of the US population victimized in the past five years. Data from the UK's Fraud Prevention Service showed that identity fraud increased 462% from 1999 to 2000 and 122% from 2000 to 2001. The UK study also confirmed the linking of identity fraud to organized crime in a number of forms - including illegal immigration, money laundering and drug running - in addition to fraud perpetrated against the government and the private sector.

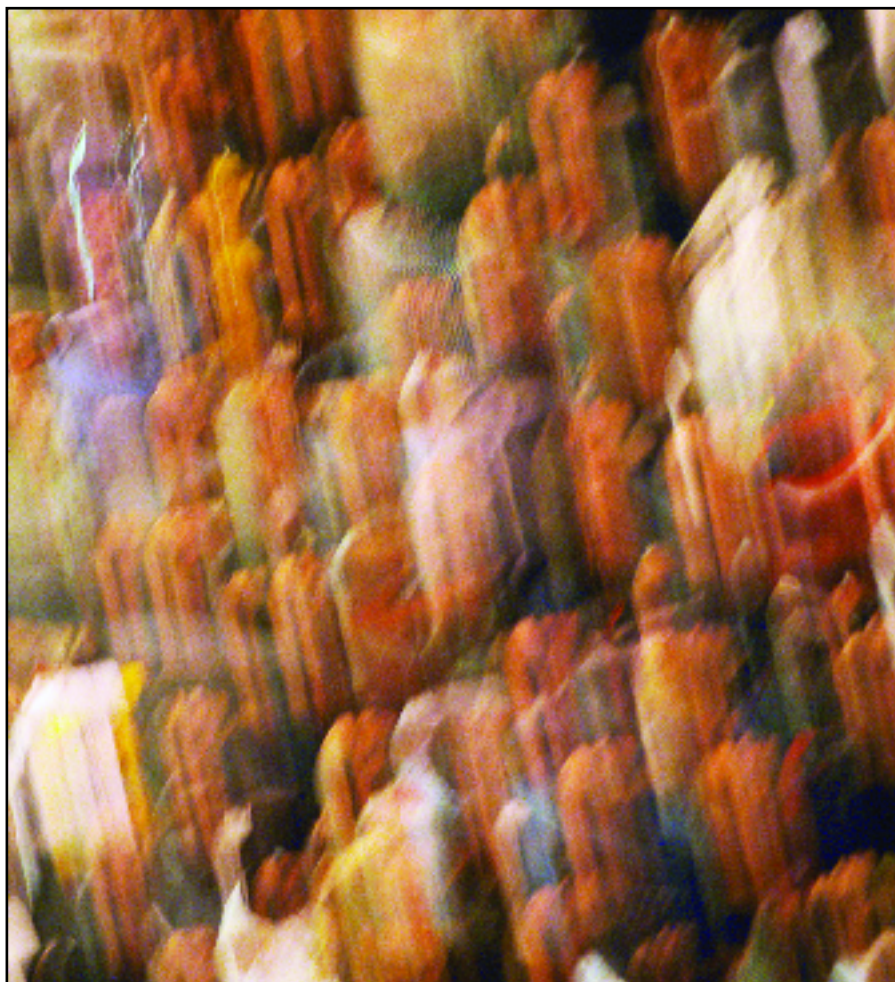
Not only did identity fraud enable the terrorist attacks of 9/11 but, according to Aberdeen Group research published in May 2003, identity-related crimes will rob the global economy of \$220 billion this year, on track at a 300% annual growth rate to reach \$2 trillion by 2005. If biometrics can be applied to protect identity, to reduce even a fraction of the financial repercussions of identity theft, the potential for commercial ROI is a much stronger argument for adoption than incremental improvements in security will ever be.

Co-opetition is key

Biometrics has a sordid history of industry infighting and competitive claims regarding which technology is best - hand, face, finger, iris, etc. Vendors now - publicly at least - embrace the notion that the choice of technology is environment and application dependent. There is no "best" biometric, just a best fit for a given set of situational constraints. In fact, the latest push is towards multiple biometrics fused together to increase the accuracy of the authentication process. This is a truly positive development, as industry focus has shifted from internal conflict to tackling the broader issues associated with large-scale deployments - standards, interoperability, enrollment, privacy, centralized versus distributed database management and exception handling.

Inevitable dominance of BASPs

Another bright spot in terms of addressing some of these broader issues is the market entry of a new class of players: BASPs or Biometrics Applications Solutions Providers. These are organizations focused on developing biometrically enabled solutions, i.e. integrating biometric technology into a useful system designed to solve real world problems. Some of the existing biometric core technology vendors are trying to transform themselves into BASPs. More often, though,





these are either newly formed organizations with specific application or vertical market expertise or established solutions providers incorporating biometrics into a family of existing vertically oriented products and services.

New market entrants have more room to maneuver. They are not tied to a specific technology or vendor nor do they carry the debt load their more established counterparts have accumulated through years of biometric R&D. BASPs are in a strong position to rapidly drive the market towards its next phase of evolution - bringing biometrics into the mainstream.

Larger scale deployments

Vendors are reporting logical access deployment sizes increasing from the sub 5,000-user range into the 5,000 to 20,000-user range. This is an important step in an iterative process of scaling the development of ever-larger biometrically enabled systems. Though vendors are prohibited from releasing the details of these recent deployments, at least three in healthcare and financial services are in the process of being rolled out.

Technology solutions typically confront system failures at certain size thresholds. These recent larger user base projects will enable biometrics vendors to address the next series of incremental thresholds that will open the door to even larger logical access deployments that approach the 50,000 to 100,000-user range.

The future - convergence, consolidation, morphing

In many ways, the ubiquitous adoption of biometrics is highly dependent on its increasing unobtrusiveness. The less pronounced the technology, the greater the acceptance. Biometrics must be integrated into daily processes in a way that offers users ease and convenience, protects personal privacy and preserves civil liberties. In addition, biometrics must also integrate seamlessly with a myriad of other existing and emerging technologies, which includes everything from smart cards and RFID to federated ID systems, web services, 3G wireless and GPS tracking systems.

Over time biometrics capture devices for most routine applications will become low-cost, reliable commodities compressed into tiny form factors that will be embedded in everything from PDAs and PCs to POS terminals, ATMS and airport kiosks. As with most technologies, these devices will blend into the landscape of modern life and become essentially invisible. Do you know who makes the hard drive in your PC? How the bank processes your pin number at an ATM? What the kiosk at the airport does with the credit card you insert to identify yourself when checking in for a flight?

Finally, mainstream adoption will occur as massive convergence takes hold and individual biometric categories disappear. This is more than just consolidation of the key players or one technology winning out over

another - it is the actual merging and morphing of the capture devices and the algorithms. Today biometrics involves the capture, creation, storage and matching of mathematical representations, of two- or three-dimensional patterns, whether they be the image of a face, finger or iris, the sound of the voice or the rhythm, pressure and speed of a signature. Ultimately, capture devices and algorithms will be mostly indifferent, regardless of scale, to the nature of the type of pattern-data being captured.

Convenience will rule and except for high security applications or high value transactions, where more specialized equipment may be required, biometrics will become utterly mundane and the technology to process them virtually interchangeable.

This path is certainly not predetermined and though the mainstreaming of biometrics seems inevitable, many technologies with similar promise have suddenly and irreversibly faded away. While the opportunity to break-through to advanced market evolutions is real, it is only through clear vision, directed leadership, well defined strategies, focused effort and incremental and iterative steps that biometrics will mature from R&D novelty to commonplace ubiquity.

by C. Maxine Most,
Acuity Market Intelligence