The Future of Biometrics

Market Analysis, Segmentation & Forecasts

Insight into the Trends, Drivers & Opportunities that will Shape the Industry through 2020

includes detailed market forecast 2009—2017

Published
August 2009

by

ACUITY
MARKET INTELLIGENCE

About Acuity Market Intelligence

Acuity Market Intelligence is the biometric industry's leading independent strategic consultancy. Acuity cuts through the clutter of information overload to provide technology-neutral and vendor-independent industry analysis for the biometrics industry and other emerging technology markets. Acuity's established reputation for candid, "hype free" insight is based on a proven record of accurately anticipating biometric and associated identification solutions market trends. Acuity relies on *rigorous intuition*—a combination of quantifiable, data driven analysis and insight honed over two decades—to consistently provide original, thought provoking, accurate, and reliable industry analysis.

The core of Acuity's knowledge base is a fundamental understanding of technology market development, technology evolution in emerging markets, and how technology is adopted and deployed most effectively in targeted vertical markets. This knowledge is applied through proven tools and techniques to help vendors, integrators, investors, and end-users:

- Identify, prioritize, and size lucrative market opportunities.
- Define and analyze targeted vertical solutions.
- Create and evaluate market development and adoption strategies.
- Achieve sustainable market dominance.
- Evaluate deployment plans within the context of generating quantifiable ROI.

Market Development Expertise

Acuity's singular focus is on the development of emerging technology markets providing expertise in the following areas:

Market Analysis – Identification and evaluation of key technological developments, market trends, industry players, and deployment effectiveness.
Opportunity Analysis – Highly granulated vertical market segmentation and identification, prioritization, and sizing of the most lucrative opportunities for a given product, service, or solution.
Solutions Analysis – Requirements and functional specifications for applications of emerging technology.
Due Diligence – Evaluation of market players to ensure:

- Opportunities have been adequately and accurately assessed.
- Financial, operational, and strategic plans are in place to create sustained market viability.
- Product and service quality can be demonstrated.

Strategic Planning – Creation of highly leveragability plans to develop, evaluate and deploy emerging technology-based solutions with the objective of achieving the highest degree of customer satisfaction and sustained market dominance.

Client Services

Clients leverage Acuity's knowledge and expertise through a range of off-the-shelf, semi-custom, and fully custom product and service offerings. These include:

Executive Briefings & Strategy Sessions – Interactive sessions provide targeted insight to Client Executives.
Consulting – Custom projects designed to support specific Client objectives.
Segment Tracking – On-going coverage of technologies, players, market drivers and dynamics of a particular industry sector or technology marketplace.
Reports – Periodic and one-off targeted analyses focused on a range of topics including: technology evolution, application development, vertical market adoption, and competitive analysis.
Research – Standard and semi-custom research projects designed to address specific industry knowledge gaps.
Workshops – One to two day intensives presenting Acuity's proprietary methodology for applying proven tools and techniques to identify, prioritize, and size market opportunities.

Please contact **Acuity Market Intelligence** for additional information
on services, availability and fee structures.

Online	www.acuity-mi.com
Phone	+1 303 449 1897
Email	info@acuity-mi.com

Report Overview

SCOPE: This report presents unique insight into how the biometrics market will evolve through 2020, what will drive and shape this market evolution, and where the most lucrative biometric market opportunities will be. This report is not a biometric primer or a comprehensive overview of the industry. ***It is an advanced strategic market analysis that requires a basic understanding of the biometrics industry and associated market dynamics and technologies.*** *The report is presented in two parts.* Part One contains the strategic analysis and Part Two provides detailed market segmentation and market-based forecasts for 2009 through 2017

OBJECTIVE: This report provides a basis for short-term, mid-range, and long-term strategic planning for technology and solution development, market investment, and phased adoption of biometrics for both Public Sector and Commercial deployments.

AUDIENCE: Individuals responsible for strategic planning, business and market development, and sales within the biometrics community including: vendors, integrators, investors, consultants, distributors, solution providers, as well as Public Sector and Commercial end-users.

METHODOLOGY: Analysis is drawn from on-going market coverage of the industry including: significant market and technical developments, tests, pilots and deployments, as well as public domain and private data sources, research and reports, surveys, and interviews with vendors, integrators, intermediaries, customers, privacy and civil liberties advocates, and other relevant technology and vertical market industry experts. Forecasts are derived from modeling total potential market opportunities for the enhancement or replacement of existing technology and non-technology based processes and solutions, and the introduction of new processes and solutions based on the unique capabilities of biometric technology. Models rely on public domain and proprietary primary data sources and are flexibly structured to account for known and predictive factors. Primary sources determine known model data. These include data points like population, population age distribution and assocated government services and benefits, number of port facilities and border control points in a given country or region, annual passports issued, the number and type of enterprises in a given country or regin, government and enterprise employment, and deployed military and civilian staff and contractors. Models are then adjusted to account for existing market conditions, current deployments, anticipated projects, and existing and planned infrastructure. Conservative assumptions for predictive factors - such as technology pricing and anticipated adoption rates – are introduced to determine forecasts. Final forecasts represent the predicted penetration of the total market value over the forecast range.

KEY CONCLUSION**:** Over the next ten years the infrastructure to enable mainstream, ubiquitous biometric authentication will be developed. Biometrics will be a fundamental embedded component of the digital world, as it becomes a key enabler of trusted transaction control – data access and flow - for personal, commercial, and government use. This trusted transaction capability will ultimately define the genuine opportunity for revenue associated with deployment of biometric technologies. The technology itself will, in many respects, become inconsequential as the applications it delivers become essential components of twenty-first century life.

AUTHOR: C. Maxine Most, Principal, Acuity Market Intelligence

Introduction

What is *The Future of Biometrics*? Strong consensus amidst well-founded apprehension indicates biometrics will become mainstream, ubiquitous technology. Opportunities abound and there has been successful initial market penetration for of physical and logical access, identification services, and surveillance applications. From passports and ATMs to corporate network access and mobile phones, from the White Castle fast food chain, and Pictet & Cie Banquiers, a renowned Swiss bank, to the Denver Rapid Transit Department Treasury and nuclear power plants, biometric technologies are used by tens of millions of individuals across the globe for personal, commercial, and civil applications every day. The most interesting and relevant question about the future of biometrics is not whether biometrics will prevail or even how quickly, but what is the path from today's limited—though effective—use to what most industry experts agree and most privacy advocates and civil libertarians fear is biometrics ultimate destiny: ubiquity.

***The Future of Biometrics* provides insight into how the biometrics industry will evolve through 2020, what will drive this evolution, and where the most lucrative market opportunities will be. It is intended to provide a basis for short-term and long-term strategic planning for technology, as well as solution development and deployment for both Public Sector and Commercial applications. The report is presented in two parts. Part One contains the strategic analysis and Part Two includes market segmentation and forecasts for 2009 through 2017.**

Biometric industry revenue as defined in this report is limited to the sale, licensing, and installation of the hardware and software required to deploy biometrics as standalone solutions or integrate biometrics as part of larger identification solution. It does not include any revenue associated with the development, deployment, or integration of the non-biometric components of large-scale identification solutions.

Part One: Analysis

The first half of the report addresses fundamental questions that provide the context for developing a comprehensive view of the likely evolution of the biometrics marketplace.

- What are the Mega and Meta forces shaping the evolution of the market?
- Which industries and applications hold the most promise for biometric deployment?
- How will market demand shape technology evolution and the development of biometrically enabled solutions?
- What is the current state of the marketplace?
- How will the technology evolve and impact overall market development?
- How will the most substantial opportunities for industry players evolve?

Context

The Future of Biometrics begins with a fictional scenario representing what may prove to be a real world experience by 2020. This provides context for understanding the far-reaching implications of biometrics fully integrated into daily life.

Mega Trends

The eight global *Mega Drivers* are trends that will profoundly impact all IT development through 2020 and have important, specific implications for biometrics. They are:

- Globalization and Developing Economies
- Borderless Economies
- Workforce Decentralization and Mobility
- Population Mobility
- Proliferation of Mobile Devices and the Rise of Trusted Access Anywhere
- Central Role of Digital Identity
- Inevitability of eGovernment
- Rise of Cloud Computing

Meta Drivers

Application Solution and Technology Evolution *Meta Drivers* shape both opportunities for widespread deployment of biometrics as well as determine the technological capabilities required to address these applications.

The three key Public Sector *Application Solution Meta Drivers* are: eBorders, eID, and eGovernment.

The three key Commercial *Application Solution Meta* Drivers are: Enterprise Security, Information Transactions, Financial Transactions.

The four key *Technology Evolution Meta Drivers* are: Secure Identity Core, Secure Mobility, Secure Credentials, and Secure Transactions.

Obstacles and Opportunities
Biometric technology has the potential to enhance or threaten consumer and citizen rights and civil liberties, and exacerbate or eliminate opportunities for identity theft and fraud. Core biometric issues as well as those considered outside the direct purview of biometrics, but directly impacted by their use, are assessed relative to this inherent conflict. Central to this component of the analysis is the notion that these obstacles pose challenges that can be harnessed and transformed to provide significant opportunities for market leadership and dominance.

The State of the Market
The evolution of the biometrics market, though plagued by strange twists and turns, is on track for sustained growth. The post 9/11 promise of biometrics may not be materializing as expected; however, key applications in critical market sectors represent significant opportunities for market players who strategically focus efforts on building cost-effective solutions to business-breaking problems. Though several recent setbacks and failures of Public Sector and Commercial biometrically enabled programs have generated bad PR for the industry, *it is not the biometrics that failed*. The industry needs to move-on and continue to demonstrate the unique capabilities and ROI potential of biometrically enabled identification solutions. For both Public Sector and Commercial markets, citizen and consumer transactions may be the largest revenue generators and drivers of biometric adoption.

Future for Key Technologies
Technology evolution is inevitable and evolving capabilities and limitations will impact the relative success/ubiquity of each biometric modality. Technology convergence is also inevitable as is the emergence of multimodal biometrics as a major factor in the development of practical, ubiquitous biometric solutions. “Conventional” biometrics— AFIS/livescan, Finger. Face, Iris, Hand, Vein, Voice, Signature, Keystroke—are included in this analysis along with some of the emerging modalities. The role of multimodal biometrics and the impact of ancillary identification technologies are also discussed.

Part Two: Market Segmentation and Forecasts
The second half of the report includes market segmentation and forecasts for 2009 through 2017. A market or solution based approach is applied to the market segmentation. This is atypical in the biometrics industry where most published forecasts take a technology-based approach. This means the market segmentation in this report analyze opportunities and associated revenues in terms of geographic regions, market-based solutions, and technology applications rather than defining the size of a market based on technology revenue – e.g. the market for eBorders or Financial Transactions rather than the market for AFIS or Iris recognition. *The Future of Biometrics* approach provides data and perspective that is designed to support strategic market development planning.

Market Segmentation
The two key Application Solution domains and their associated sub domains - Public Sector (eBorders, eID, and eGovernment) and Commercial (Enterprise Security, Information Transactions, Financial Transactions) - are mapped against four key application areas— Physical Access, Logical Access, Identity Services, and Surveillance and Monitoring - to create market segmentation matrices. The resulting market segments are ranked in terms of development priority and timeframe. Each target market is also assessed in terms of the technologies (biometrics modalities) most likely to be deployed. Forecasts for the Commercial and Public Sector Application Solution domains, their sub domains, and select target markets are presented globally, by region, by technology, and by application.

Forecasts
A quantitative approach is applied to the market forecasts. This approach is based on development of scenario modeling tools designed to project total market potential for biometrically–enabled solutions within select markets. These modeling tools predict total market value based on an analysis of how biometrically-enabled solutions can augment or replace existing manual and/or automated processes, or introduce new processes based on the unique capabilities of biometrics within the given market sector and segment.

The models rely on public domain and proprietary primary data sources and are flexibly structured to account for known and predictive factors. Primary sources determine known model data. These include data points like population, population age distribution and assocated government services and benefits, number of port facilities and border control points in a given country or region, annual passports issued, the number and type of enterprises in a given country or region, government and enterprise employment, and deployed military and civilian staff and contractors. Conservative assumptions for predictive factors—such as technology pricing and anticipated adoption rates—are then introduced to determine forecasts. Final Forecasts represent the predicted penetration of the total market value over the forecast range, which in this case is 2009 through 2017

Preface to the 2009 Edition

I came across the following in an article entitled *Another day in paradise as life gets cryptic*, by Sathnam Sanghera in The Times Online on July 20, 2009.

> "The other day we got a message from our IT department at *The Times* informing us that password policy was changing as part of an annual Finance and Technology Sarbanes-Oxley audit, and that passwords must now be "eight characters long, contain a letter in upper case, a letter in lower case, a number, and a non-alphanumeric character (e.g. ?, £, %, $)". Meaning that "fluffykins", "B1 9AR" or "anotherdayinparadise" are no longer permissible and that even "BuRpy%2x" will work only for a while, as one is required nowadays to change one's password more often than you change your underpants."
>
> "I use seven passwords and passcodes to deal with my bank alone. Recent research has found that 88 per cent of employees use between five and six passwords at work. And in 2006 *The Wall Street Journal* reported that there was an insurance company where the agents needed to use 40 passwords during the average working day. The other day I spent a whole hour trying and failing, with the aid of those seven passwords, to make an online bank transfer that would have taken seconds in the days that customers had personal relationships with managers. And according to a UK survey conducted in 2004 by Microsoft, 60 per cent of computer users have at some point exhibited "anti-social behavior" in the form of shouting, "pouting in silence" and hitting computers, because of forgotten passwords"

Unfortunately, these anecdotal comments are representative of life in the twenty-first century for far too many of us. One would think the reality of these common experiences would be enough to justify and propel rampant adoption of biometrics. Sadly, this Is not true. In the two years since the original 2007 publication of this report, the industry has seen both significant accomplishments and considerable setbacks. While some major government programs have been scaled back (TWIC), are seriously behind schedule (HSPD-12 PIV cards), or have an uncertain future (UK National ID), others have been initiated (India's 1.5 billion and Mexico's 100 million strong National ID programs). Commercial investments in all non-essential IT has slowed to a crawl in the current economic climate, however, there is renewed focus on short-term ROI-based investment like time and attendance solutions. So, in spite of industry setbacks and a faltering global economy, the biometrics market remains healthy and is well positioned for steady, but slow growth.

The 2009 forecast numbers average approximately 10% below original 2007 projections for the overlapping forecast period 2009 through 2015. This adjustment is mainly due to lower than expected 2009-2010 growth attributable to stalled economy. Interestingly, while Acuity has been criticized over the last two years for underestimating the revenues projections published in 2007, most analysts have recast their projections downward during this period and have now published forecasts that are in line with Acuity's projections.

In addition to providing revised forecasts, the 2009 edition has been updated and expanded in both minor and significant ways. The elements of the market analysis that provide the context and conceptual framework stand on their own and have largely been left in tact. Minor edits and additions have been made where appropriate. For example, the Rise of Cloud Computing has been added as an eighth Mega Trend. Dated facts and relevant technical and programmatic updates have been added throughout the document as well.

A new analysis section has been added to Part One entitled "The State of The Market". This section provides insight into the current evolution of market development, provides a review of some of the of large government post 9/11 ID programs, and offers analyses of two key applications—Time and Attendance and Surveillance—and two industry verticals—Financial Services and Healthcare.

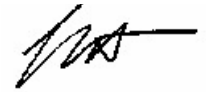
This section also takes a look at two highly visible commercial biometric business that went bust—Pay-by-Touch and the CLEAR registered traveler program. These programs together accounted for nearly half a billion US dollars in industry investment. Though each failed for their own reasons, each was doomed from their inception begging the question why is it that many small, viable biometric enterprises with great prospects for success are unable to acquire investment capital while these two ventures were able to attract significant investment with almost no chance of success?

A high-level view of the environment for market players is presented along with perspective on key developments that will impact the vendor landscape through 2020. A comprehensive competitive analysis is beyond the scope of this report and will be the subject of a follow-on report published later this year.

Finally, this section includes a discussion of the key market forecast findings from Part Two of this report. These market forecasts have been updated and greatly expanded from the original 2007 report. They now include forecasts by technology and application for the global market, for each public sector and commercial market sector, and for each region. Part Two features 29 new data tables, 27 new graphs, and 53 new charts as well as CAGR calculations for many of the existing market forecast graphs.

I hope that you find this document to be an insightful reference as you navigate the biometrics marketplace. As always, your comments, criticisms, suggestions, questions, and complaints are welcome!

Cheers,



C . Maxine Most
Principal, Acuity Market intelligence
July 22, 2009
cmaxmost@acuity-mi.com

Table of Contents

Table of Contents

*Regions: North America: US, CA, Mexico
EMEA: Europe, Middle East & Africa
Central and South America
Asia Pacific: Asia, Pacific Rim

Charts, Tables & Graphs—Part One

.

Charts, Tables & Graphs—Part TWO

Charts, Tables & Graphs—Part TWO

Charts, Tables & Graphs—Part TWO

Charts, Tables & Graphs—Part TWO

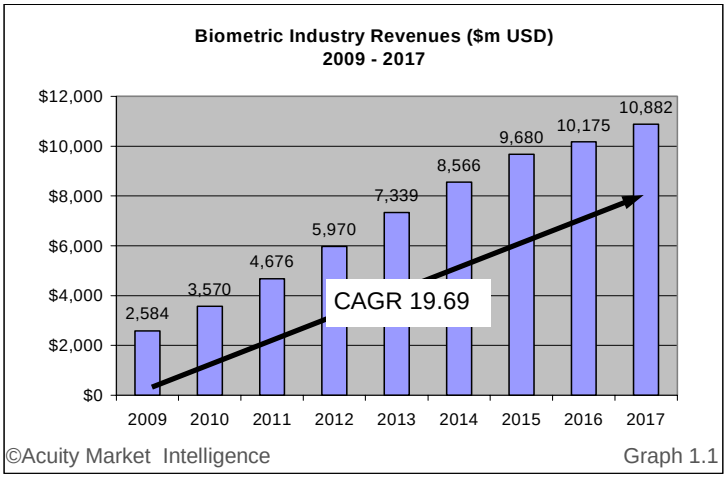
Charts, Tables & Graphs—Part TWO

Executive Summary

Executive Summary

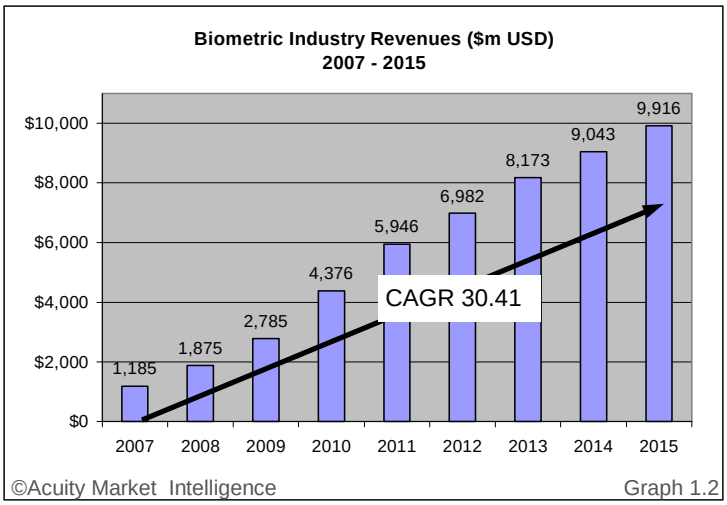
Biometric industry revenue as defined in this report is limited to the sale, licensing, and installation of the hardware and software required to deploy biometrics as standalone solutions and to integrate biometrics as part of larger identification solution. It does not include any revenue associated with the development, deployment, or integration of the non-biometric components of large-scale identification solutions.

Biometrics Industry Revenues 2009—2017



©Acuity Market Intelligence Graph 1.1

Biometrics Industry Revenues 2007—2015



©Acuity Market Intelligence Graph 1.2

Industry Overview

The biometrics industry remains on track to experience significant transformation over the next ten years. Technological capabilities will revolutionize ease of use, accuracy, and performance and greatly expand the use of biometrics for personal, commercial, and government applications. Maturing business models will evolve from product to service based offerings with the bulk of revenues generated from transaction-based opportunities.

Though there have been setbacks in a number of widely heralded biometrically-enabled identification programs—the failure of the US-VISIT Exit program, the scaling back of the US Transportation Worker Identification Credential (TWIC™) program from 12 million transportation workers to one million maritime only workers (and its slow uptake even in this limited incarnation), the transformation of the UK National ID card to an opt-in program and it's potential demise based on political outcomes, and the commercial implosions of Pay-by-Touch and the CLEAR Registered Traveler offering—overall momentum in this arena continues to strengthen and will result in sustained growth opportunities.

The impact of the 2008 global economic meltdown has been significant, but not devastating to the biometrics industry. Public Sector projects have slowed down and/or been scaled back. (The UK National ID may be one exception. While the state of the economy added fuel to the fire, the extreme civil liberties pushback and the political climate were the primary change agents). Commercial opportunities have generally shifted in response to economic realities. Major IT infrastructure projects are being cancelled or postponed in favor of targeted, incremental projects that impact bottom-line performance within a 12 to 18 month window. This bodes well for biometric-based time and attendance applications, which have a proven record of providing quantifiable, short-term, ROI rather than physical, or logical access solutions whose bottom line benefits are more difficult to quantify.

The bottom line for the biometrics industry is that there is good news and bad news. The good news: in spite of programmatic setbacks and the current worldwide economic malaise, overall identification market dynamics continue to be strong. This market environment is conducive to the level of expansion needed to realize the promise of biometrics. The not so good news: as growth continues and potential rewards increase so to will uncertainty and risk. While the inevitable outcome seems clear, the path to achieving this outcome is not. Successful navigation of this market will therefore require both a clear vision and a strategic market development approach that is flexible enough to exploit opportunities created by a market in flux.

Market Growth

The market for biometrics core technology is poised for sustained growth with global revenues reaching nearly $11 billion annually by 2017 representing a CAGR of 19.69% over the forecast period (Graph 1.1). These figures are reasonably consistent with original projections made in 2007 (Graph 1.2). The 2009 forecast model was updated to reflect the most recently available data and account for current market dynamics—economic and political as well as technical. Slower growth than originally anticipated in the 2009 to 2012 timeframe, due to the faltering economy, is balanced out by slightly stronger growth in the 2012 to 2015 timeframe. The result—projections that reach roughly the same revenue levels by 2015, but with a lower overall anticipated CAGR of 20% from 2009 through 2017 rather than the higher CAGR of 30% from 2007 through 2015.

Biometrics market growth will be driven by far reaching *Mega Trends* broadly impacting global IT development as a whole, as well as by more narrowly defined biometric solution *Meta Drivers* within specific application areas. Mega and Meta influences lead to the inevitability of biometrics and create a context for understanding the likely evolution of the marketplace and the associated strategic opportunities.

Mega Trends
Eight global *Mega Trends* will profoundly impact all IT development through 2020 and have important biometric specific implications. They are:

- Globalization and Third World Development
- Borderless Economies
- Workforce Decentralization and Mobility
- Population Mobility
- Proliferation of Mobile Devices and Trusted Access Anywhere
- Central Role of Digital Identity
- Inevitability of eGovernment
- Rise of Cloud Computing

Each of these trends impacts and is impacted by the management and linking of large populations to identity-based rights, privileges, actions, and services. The sheer volume and complexity of dealing with individual identification in a global community that is simultaneously shrinking (ever more connected) and expanding (ever more inclusive) is staggering. In this environment, the ability to establish and link an individual to an established or claimed identity is fundamental to creating and maintaining the digital infrastructure on which the global community increasingly relies.

Meta Drivers
Application Solution *Meta Drivers* shape the opportunities for widespread deployment of biometrics. Technology Evolution *Meta Drivers* are the capabilities that support the demands of these market forces.

The three key Public Sector *Application Solution Meta Drivers* are: eBorders, eID, and eGovernment. The most immediate drivers are worldwide government mandates for integrated border management systems. This includes the development of biometrically-enabled travel documents and the devices and border control systems that utilize them, expedited passenger programs, transportation worker identification and access control systems, and immigration and asylum seekers application, identification, and monitoring systems. Government endorsement of biometrics has begun to produce industry standards and create an environment where interoperable, large-scale systems are now transitioning from vision to practical reality. This endorsement is driving widespread government adoption of biometric authentication for government electronic identification programs (passports, National IDs, drivers licenses, etc.) and will ultimately lead to the adoption of biometrics for secure, fully transactional eGovernment capabilities.

The three key Commercial *Application Solution Meta* Drivers are: Enterprise Security, Information Transactions, and Financial Transactions. The Commercial market has benefited by the current drive towards large-scale interoperable systems for government applications. The rampant growth of identity theft and associated requirements for the protection and management of personal data will contribute significantly to growth in this area as well. Adoption in the enterprise market for time and attendance and physical and logical access will gain significant market traction over the next three years. This will be rapidly superseded by the much larger opportunity to secure information and financial transactions, which will emerge over the next three to seven years.

The four key *Technology Evolution Meta Drivers* are: Secure Identity Core, Secure Credentials, Secure Transaction, and Secure Mobility. These capabilities are essential components of the larger framework enabling the development of a reliable, secure, worldwide infrastructure that biometric authentication simultaneously plays a central role in creating and relies on for market expansion

Obstacles and Opportunities
Mainstream biometric deployment faces obstacles ranging from the inherent limitations of the technology and failure to adequately plan for and implement deployments, to fears about violations of privacy and civil liberties. These obstacles are primarily related to moving biometric deployments from relatively small, closed-loop, and technology-centric applications to large-scale, human-centric identification solutions. This requires the development of a secure standards-based technology infrastructure, a privacy respecting (if not enhancing) legal and regulatory framework, and human-factors based system design that paves the way for truly interoperable, user-accessible, and socially acceptable solutions.

One of the more intriguing aspects of the marketplace is that many of these real and perceived obstacles represent significant opportunities for biometrics market development as well. For example, privacy and civil liberties advocates fear that widespread use of biometrics will enable a surveillance society. However, they also complain vigorously about the woefully inadequate security measures in force to protect individuals from identity theft and fraud. In this case biometrics could be the problem or the solution blurring the distinction between obstacle and opportunity. The most effective strategic response is to transform obstacles into opportunities through the appropriate use of biometrics.

State of the Market

The market for biometrics is in a strange state and will most likely not follow the typical path of disruptive technology adoption. Biometrics have been considered a disruptive innovation on the verge of breakthrough for an extended period of time. Post 9/11 security concerns that were supposed to propel the biometrics market forward created an even greater expectation of rapid market acceleration that never materialized.

There has been far too much infatuation with the belief (wish?) that large government contracts—not targeted Commercial opportunities—would be the engine driving rapid market expansion. Progress on the government front has been substantial, but has not provided the scale of opportunity necessary for the industry to thrive. The result: market players—with few noteworthy exceptions—have failed to leverage the classic target market development phase of the adoption lifecycle to produce commercially viable, proven solutions which are directly applicable to large-scale identification systems.

The post 9/11 promise of biometrics provided the impetus for a series of biometrically enabled identification initiatives proposed in the US and across the globe beginning in late 2001 and 2002. Existing identification initiatives were given a strong boost and new initiatives were developed to create more reliable and secure identification documents, programs, and processes. Industry vendors, integrators, pundits, and the investment community were whipped up into a near hysterical frenzy believing this to be the basis of an on-going, thriving, biometrics marketplace. Nearly eight years later, the dust long settled, expectations have been greatly scaled back as these initiatives have varied significantly in the success they have achieved.

Two key application areas—Time and Attendance, a biometric stalwart, and Surveillance and Monitoring, a bleeding edge use of technology—are well positioned to leverage the unique capabilities of biometrics and experience significant growth over the forecast period.

Two key industry areas—Financial Services and Healthcare—have failed to materialize as primary drivers of global biometrics adoption as has been expected and projected for may years. There have been and continue to be strong justifications for these expectations. Both are highly regulated industries with compliance based identification and authentication needs. Both are required by law and consumer demand to protect the privacy of their customers. Both have obvious operations and service delivery issues that can be well served by implementing biometrics.

The segmentation applied in this analysis splits Healthcare and Financial Services into components within two Commercial market sectors—Enterprise Security and Information Transactions. There is also a third Commercial market sector devoted exclusively to Financial Transactions. Each of these sectors is divided into multiple targets and mapped against applications—Physical Access, Logical Access, Identity Services, and Surveillance—creating a complex targeted segmentation of these industries. It is within this context the possibilities for financial services and healthcare are examined.

Finally, the failure of two high profile commercial biometric endeavors has cast a shadow on biometrics technology. The demise of Pay-by-Touch in November 2007 and CLEAR in June 2009 sucked half a billion in investment capital out of the biometrics industry. Though both failures generated headlines, brought unwelcome attention to the biometrics industry, and seemed to shock the business community, these business failures had nothing to do with the biometrics.

Future for Key Technologies

Mainstream ubiquity will occur as capture devices for most routine applications will become cheap, reliable commodities available in multiple form factors embedded in everything from PDAs, PCs, POS terminals, and ATMS to vehicles, security gates, and even home appliances. As with most technology, 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? Convenience will rule and except for high-security applications or high value-transaction—where more specialized equipment may be required—biometrics will become nearly invisible and the technology to process them virtually interchangeable. In addition, biometrics will be routinely integrated with technologies such as RFID (Radio Frequency Identification) and NFC (Near Field Communications) linked by highly secure credentialing infrastructures to create seamless transactional and security environments.

In the more distant future—beyond the timeframe of this report—the actual distinctions between biometrics modalities will blur, massive convergence will take hold, and individual biometric categories will disappear. This is more than just one technology winning out over another; it is an actual merging and morphing of the capture devices and the algorithms. Ultimately, capture devices and algorithms will be mostly indifferent, regardless of scale, to the nature of the type of pattern-data being captured. Most biometrics will continue to improve in price/performance and accuracy until their maximum capability has been achieved. Others, such as hand recognition, may simply fade away as their relative performance and usability render them obsolete.

Public Sector Market Segmentation

©Acuity Market Intelligence 2009 * Solutions for these markets will likely be paid in part by commercial enterprises		Integrated eBorders					eID					eGovernment	
		Travel Docs	*Port Facilities	*Vehicles	*Expedited Travelers	Other	Civil - DL, Nat. ID, Voter	Criminal - Mobile ID, Booking, Prisoners, Prison Visits	Benefits - Health, Welfare, Pension/SS	Gov. Admin - Civil Servants	Military & Defense - Staff, Contractors, In-theatre	Citizen - Tax, License, Utilities, Court, Education	Commercial - Tax, License, Regulatory, Court
Physical Access – Facility Access, Security Checkpoints, Time & Attendance	Citizens		X	X	X	X		X					
	Staff & 3rd Party	X	X	X	X	X	X	X	X	X	X	X	X
Logical Access – PC, Networks, Mobile Devices, Kiosks	Citizens	X	X		X	X	X		X			X	X
	Staff & 3rd Party	X	X	X	X	X	X	X	X	X	X	X	X
Identity Services – Background Check, Enrollment, Credentialing, Document Issuance,	Citizens	X	X		X	X	X	X	X	X	X	X	X
	Staff & 3rd Party	X	X	X	X	X	X	X	X	X	X	X	X
Surveillance & Monitoring—Cooperative & Non-cooperative- watchlists	Citizens	X	X	X	X	X	X	X	X			X	X
	Staff & 3rd Party	X	X	X	X	X	X	X	X	X	X	X	X

Chart 1.1

Market Segmentation

The highest level of market segmentation is based on two key Application Solution domains—Public Sector and Commercial— and their respective sub-domains—eBorders, eID, and eGovernment and Enterprise Security, Information Transactions, Financial Transactions. These domains and sub-domains are segmented against four key application areas— Physical Access, Logical Access, Identity Services, and Surveillance and Monitoring —to create the market segmentation matrices that provide the framework for the forecasts. This segmentation is not comprehensive in reflecting every possible market opportunity, but rather focuses on key growth markets for biometrically enabled solutions in their respective Application Solution domains.

Public Sector

The *Public Sector Market Segmentation Chart* (above) identifies the markets that provide the most significant opportunities for biometrics solutions within the three sub domains of 1) Integrated eBorders—the full scope of electronic and automated border control management including travel documents, transportation worker IDs, vehicle access, immigrant Visas and IDs, and expedited passenger systems, 2) eID—which includes criminal and civil ID,national and other identity cards, benefits distribution, voter registration, drivers licenses, and 3) eGovernment—fully transactional interactive service delivery for citizens and Commercial enterprises. The specific markets within each sub domain selected for this segmentation represent areas of most probable and significant growth for biometrically enabled solutions over the analysis period, not the complete opportunity within that given sub-domain.

Commercial

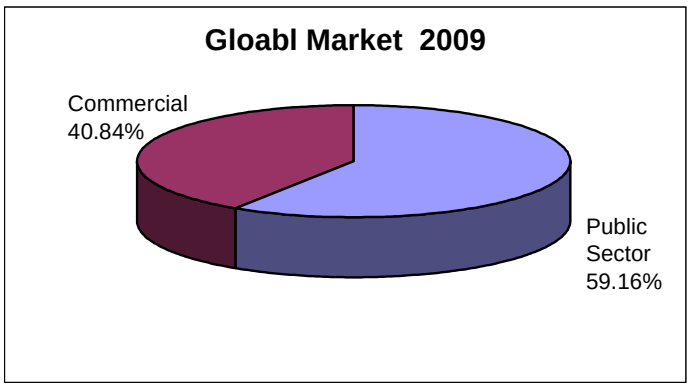
The Commercial *Market Segmentation Chart* (previous page) identifies the markets that provide the most significant opportunities for biometrics solutions within the three sub-domains of 1) Enterprise Security—which includes physical and logical access for employees and third parties (customers, vendors, etc.) as well as credentialing and surveillance, 2) Information

Commercial Market Segmentation

©Acuity Market Intelligence 2009		Enterprise Security				Information Transactions				Financial Transactions				
		Financial Service	Healthcare	Transportation	Other	Financial Services	Healthcare	Transportation	Other	Consumer	B2B	ATM	Inter-bank Transfer	Other
Physical Access – Facility, Access, Secure Area Access, Time & Attendance	Customers			X	X									
	Staff & 3rd Parties	X	X	X	X							X		X
Logical Access – PC, Networks, Mobile Devices, Kiosks, Accounts, IP	Customers	X	X	X	X	X	X	X	X	X	X	X	X	X
	Staff & 3rd Parties	X	X	X	X	X	X	X	X	X	X	X	X	X
Identity Services – Background Check, Enrollment, Credentialing, Document Issuance,	Customers	X	X	X	X	X	X	X	X	X	X	X	X	X
	Staff & 3rd Parties	X	X	X	X	X	X	X	X	X	X	X	X	X
Surveillance & Monitoring – Cooperative & Non-cooperative including Time & Attendance and Watchlists	Customers	X	X	X	X	X	X	X	X	X	X	X	X	X
	Staff & 3rd Parties	X	X	X	X	X	X	X	X	X	X	X	X	X

Chart 1.2

Biometrics Industry Market Share: Public Sector vs. Commercial 2009 and 2017



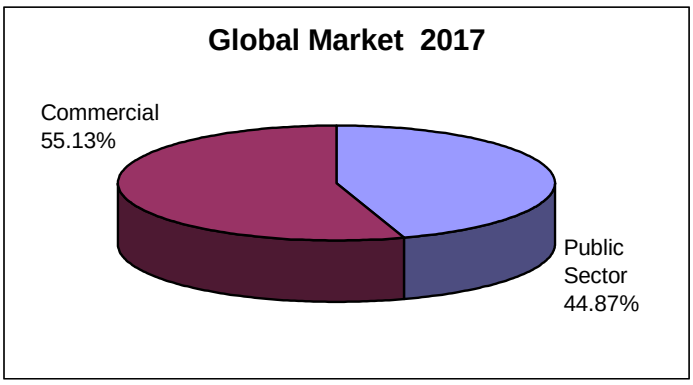


 Chart 1.3 Chart 1.4

Transactions—personal access to financial, healthcare, travel, or other service information, corporate access to financial, healthcare, vendor, supplier, customer information as well as IP management, 3) Financial Transactions—consumer, business-to-business, ATM, inter-bank, and central transactions. The specific markets within each sub-domain selected for this segmentation represent areas of most probable and significant growth for biometrically enabled solutions over the analysis period, not the complete opportunity within that given sub-domain.

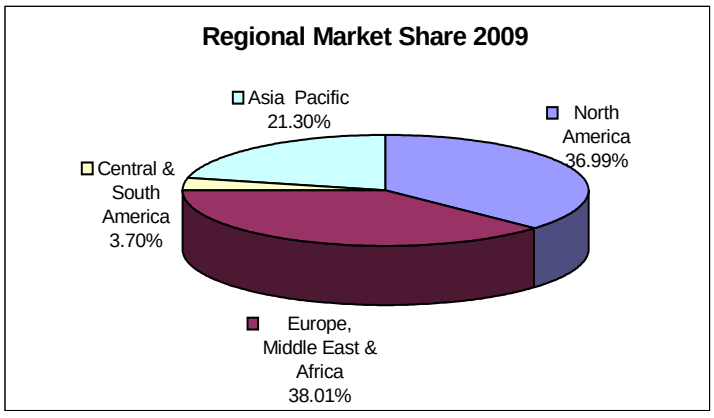
Major Research Findings

Over the next ten years the infrastructure to enable mainstream, ubiquitous biometric authentication will be developed. This infrastructure will both enable and be driven by true mass public deployment of biometrics for personal, commercial, and government applications representing the emergence of a new era of biometrics. As biometrics become a critical embedded component of the digital world, it will be a key enabler of trusted transaction control – data access and flow—for all IT systems. This secure transaction capability will ultimately define the genuine opportunity for revenue associated with deployment of biometric technologies.

Key Forecasts

- Commercial deployment revenues match Public Sector revenues by 2014 and then surpass Public Sector revenues by 2017 representing growth form nearly 41% to just over 55% of the total global market for biometrics core technology. The Public Sector revenue share declines form 59% to 45% over the period. The comparative CAGRs reflect this shift in market dominance as Public Sector grows as a respectable 16% while the Commercial marketplace grows at a much faster pace reaching 24% CAGR over the forecast period.
- The sectors with the highest CAGRs within the Public Sector and Commercial arenas are eGovernment with 42% and Information Transactions at 50%. The other sectors CAGRs are as follows: eBorders 10%, eID 12%, Enterprise Security 12%, and Financial Transactions 37%.
- Revenue growth rates vary significantly across regions. The Central and South American region will experience the highest CAGR over the forecast period of 39.46% while growing form nearly 4% to nearly 13% of total global revenues. Overall market dominance will shift from Europe (and the greater EMEA region) and the US (and the greater North

Market Share by Region 2009 and 2017



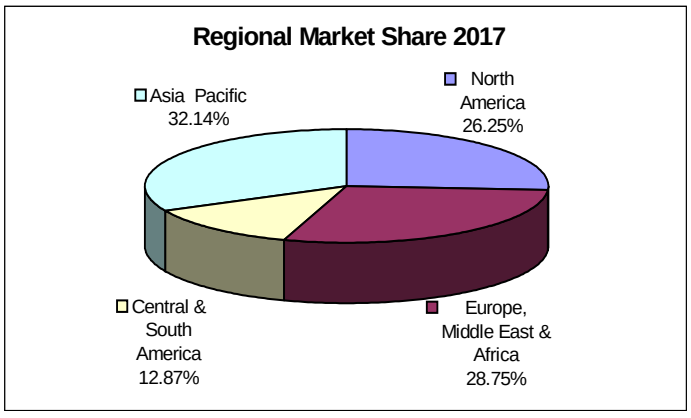


 Chart 1.5 Chart 1.6

Market Share by Technology 2009 and 2017

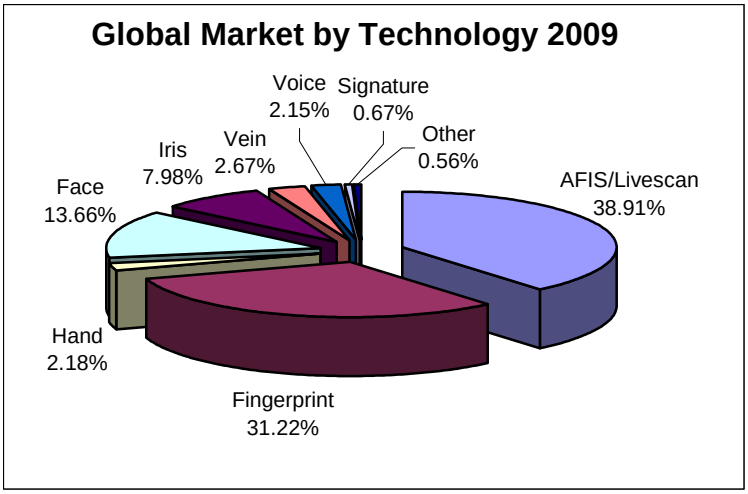


 Chart 1.7

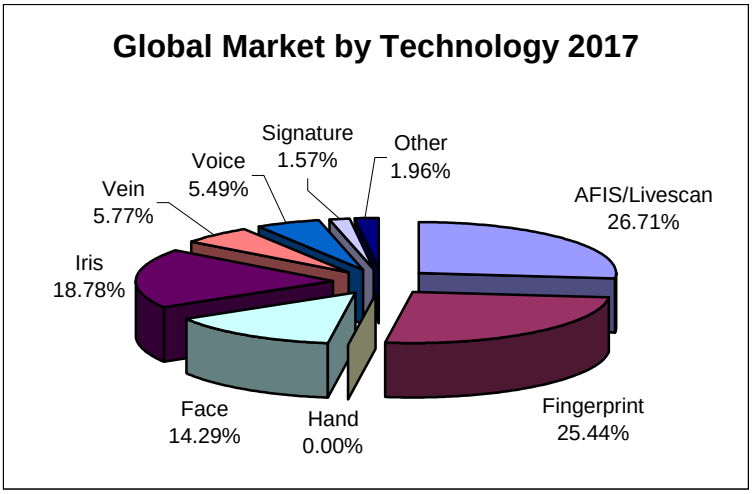


 Chart 1.8

America region) to Asia (and the greater Asia Pacific region). North America and EMEA's percentages of total global revenues will decrease over the forecast period from 37% to 26% and 38% to 29% respectively with associated modest CAGRs of 15% and 16%. By 2017, the Asia Pacific Region will generate the greatest percent of revenues for the biometrics industry with more than 32% of global revenues growing at a CAGR of 26%.

- The dominance of AFIS/Livescan and Fingerprint continues thorough the forecast period though the overall percent of total combined revenue for these technologies drops form a blistering 79% in 2009 to a more modest 52% in 2017. The prolonged dominance of finger-based biometrics rests on the legacy of finger-based identification. Identity Services including enrollment and credentialing will continue to represent the lion's share of biometric revenues over the forecast period as the digital identity infrastructure is established. This will continue to mean reliance on Fingerprint to establish/confirm baseline identity until other biometrics such as Iris and Face have made significant inroads.
- By 2017, Iris and Face recognition will begin to experience significant market penetration together accounting for more than 33% of global biometric revenues. This shift will continue beyond the forecast period as 1) these biometrics become as commonplace in the identity infrastructure as fingerprint records are today, 2) the advantages of biometrics that do not require active user participation for many physical and logical access control applications—passive iris and face capture—are understood and accepted, 3) and as the price/performance of Iris and Face make these solutions extremely cost effective.
- Vein, Voice, and Signature will experience modest growth from 3% to 6%, 2% to 5%, and 0.7% to 1.6% respectively, Hand Recognition will continue to be used but will experience a slow, steady decline from 2% of the market to 0% as it is replaced by other biometric modalities over the forecast period. Finger and Vein will benefit where a similar interface is desired and Face or Iris will benefit where a modality shift is acceptable and a more passive approach is preferred.

Market Share by Application 2009 and 2017

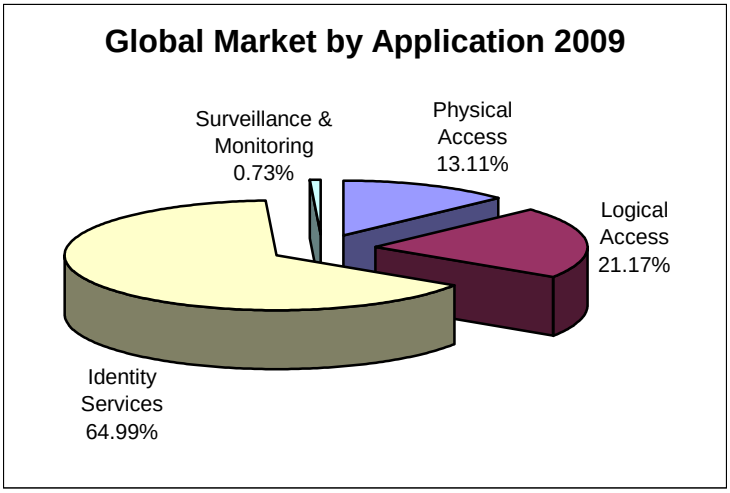


 Chart 1.9

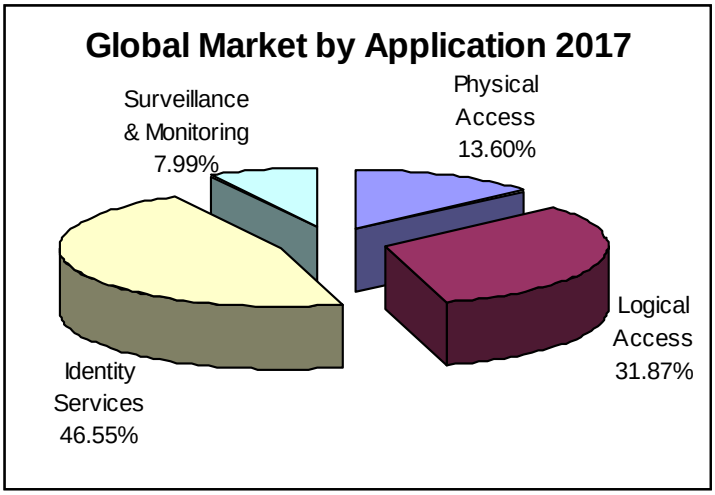


 Chart 1.10

- Transactions will ultimately provide the majority of industry revenue. Information and Financial Transactions for Commercial applications by 2012 and eGoverment for Public Sector applications by 2017. By 2017 Information Transactions will represent 12.21% of the global market, Financial Services 18.22% of the global market, and eGovernment will represent 14.23% of the global market.
- The percent of revenue from Identity Services declines over the forecast period but only from 65% to 47%. Surveillance and Monitoring posts the strongest percentage gain growing from less than 1% to nearly 8% of total market revenue representing a CAGR over the forecast period of a startling 60.99%. Physical Access control as a percent of total revenues will remain flat starting at 13% and ending up at 14%. Logical Access will grow from 21% to 31% over the same period.

Key Analysis Findings:

- A confluence of factors including the emerging central role of the Digital Identity in IT, Population Mobility and Workforce Decentralization, demand for eGovernment services, near ubiquitous reliance on digital transactions, the inevitability of broadband Access Everywhere, along with the rise of Cloud Computing will require a level of authentication available only through the use of biometrics.
- The entry of sophisticated, well funded market players with technology expertise in high-resolution image capture, large-scale data management and high-speed processing, and pattern recognition and matching algorithms from varied fields such as robotics, astronomy, and intelligent video elevate technological capability and provide the requisite knowledge for the industry to experience sustained growth.
- Biometrics as a class of disruptive or discontinuous technology has not moved completely through its revolutionary market development cycle and yet is now subject to significant evolutionary or continuous innovation. In other words, just as biometrics are beginning to stabilize and deliver on past promises, current expectations continue to be driven by “next generation” technologies. It is therefore likely that although there may be instances where specific markets and/or regions experience accelerated growth, the overall market will experience *sustained linear growth* rather than the exponential growth most readily associated with the *"hockey stick" growth* curve of innovations such as mobile phones or the Internet. Biometrics adoption will mimic the growth curve of ATMs, which achieved roughly 80% adoption through linear growth over a period of 20+ years.
- The identification legacy of AFIS is not easily overcome, especially in the US and EU. Even as the advantages of “do nothing”, user-acquiring biometrics proliferate for many high-throughput identification and consumer convenience scenarios, AFIS will remain an important tool for establishing claimed identities and checking individuals against “persons of interest” watchlists. Iris, or perhaps some combination of Iris and Face, will begin to encroach on AFIS’s turf over the forecast period as countries in the Middle East, India, and perhaps even Mexico fully integrate these biometric modalities into large-scale identification programs. As the surveillance capabilities of Iris and Face are refined and as the US FBI moves to integrate these and potentially other biometric modalities into their Next Generation Identification System, AFIS will slowly lose it’s status as the defacto mode of identification. Towards the end of the forecast period, there will be more flexibility in the choice of biometric modalities to establish claimed identity, and identification solutions that incorporate multiple biometrics will be routine.
- Identity Services will continue to represent the lion's share of biometric revenues for some time to come. Enrollment and credentialing are expensive, resource intensive processes and well-founded resistance to the idea of large, centralized repositories of personal information and biometrics will mean multiple enrollments for various applicants. Eventually, identity-centric infrastructures that can manage distributed storage models, anonymous identification, privacy-encrypted transmission of templates, personal biometric ownership, and temporary or revocable biometrics will be developed. This will lead to some consolidation of biometric data storage and lesson the requirement for on-going enrollment every time a new authorization or service is desired.
- Contactless, user-acquiring or passive biometrics (e.g. Face and Iris) will gain significant traction for two primary reasons. Capture technology will become increasingly more sophisticated operating accurately regardless of environmental conditions. Biometric authentication that does not require the user to “do anything” e.g. position themselves in relation to or have physical contact with a reader, will be prove faster (high throughput for volume applications) safer (no transmission of germs) and more convenient (no user action required) for users.
- Secure transaction capability will ultimately define the genuine opportunity for large-scale, widespread deployment of biometric technologies. As with most device driven industries, the money eventually flows from services. In technology markets the margins on “widgets” often falls close to zero at which point the widget is merely a vehicle for selling software or providing some kind of service. Viewed through a strategic lens this does not represent a threat but another opportunity to plan for market expansion in a way that leverages existing opportunities and anticipates future ones.
- In spite of the inevitable, and quite frankly important, resistance from privacy and civil liberties advocates, target applications of surveillance-based biometrics will be used in both cooperative and no-cooperative scenarios. While revenues from Surveillance and Monitoring applications will grow far faster than any other application this will continue to represent a small percent of the overall market for biometrics. Depending on how well these initial applications are developed and deployed, and what kind of issues and abuses arise, Surveillance and Monitoring could continue to show substantial growth, or be at the effect of a “snooper bowl” like debacle.

Part One: Market Analysis

Context

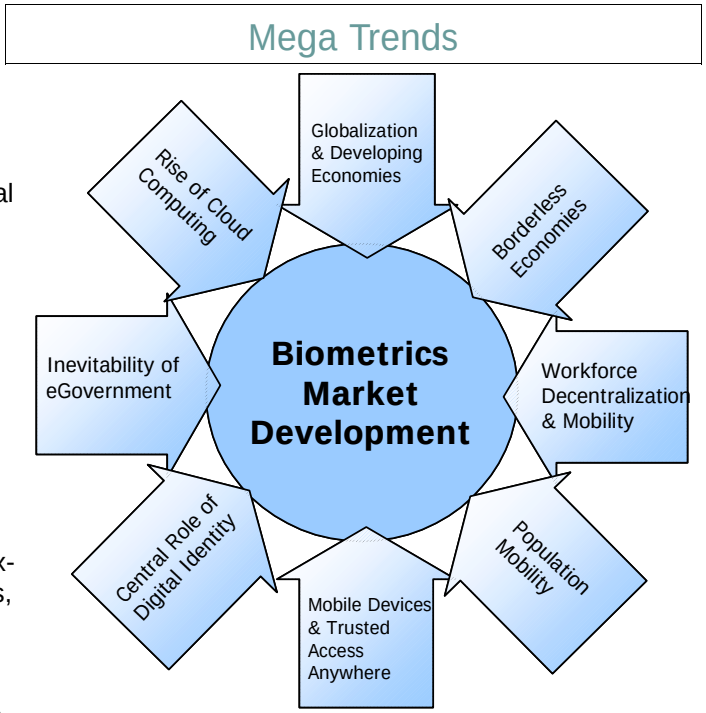
This fictional scenario of a typical "day in the life" routine anticipates some of the ways that biometrics may be embedded in our lives by the year 2020. While this is an extreme rather than accurate representation of the future, this glimpse of possibility provides a context for considering how the biometrics industry must evolve in terms of technology, usability, infrastructure (technical, legal, and social), and business models for the promise of biometrics to be realized.

Biometrics in 2020: A Day in the Life ...

7:00 am	Personalized voice-based alarm bids you a good morning and waits for your response to verify identity and provides details of overnight communications (phone, video, email, text) per your personal settings. Room lighting adjusts and the morning news broadcasts as you rise from bed.
7:30 am	Your personal environmental settings (messaging, media, lighting) follow you from the bedroom and are activated as you enter the kitchen. Once again your voice commands are used to verify identity. You continue to review any important messages and place an overseas call to confirm an international business transaction. An iris image captured from your PDA authorizes the transaction.
8:15 am	Your automobile senses your approach, verifies car access via RFID broadcast from the smart card in your PDA, unlocks the door, and confirms identity though scan of your fingers and palm as you grip the handle of the door and the steering wheel. As you drive, your voice activated PDA interface access provides a third confirmation of identity enabling you to attend to several personal matters—securing your mortgage payment, reviewing the results of a recent medical exam, and ordering flowers for your spouse.
9:00 am	You arrive at a government client site where facial recognition confirms you are not on any watchlist as you enter the building and your government contractor PIV compatible ID credential embedded in your PDA grants access to client facilities and IT systems. Your touch screen PC captures dynamic signatures as you complete a new contract which is then encrypted and distributed electronically to the legal, contract, and sales departments of your and your client's organization.
Noon	As you approach an ATM your identity is confirmed via iris recognition and you withdraw $100. You are meeting a friend for lunch and your favorite family owned diner prefers cash.
1:15 pm	You pull up the driveway and the garage door opens in response to your car transmitting it's vehicle ID along with a confirmation of you being the operator of the vehicle via an encrypted RFID signal. You enter your secure home/office. Motion detection triggers facial identity confirmation, the lights and temperature are adjusted to your personal preferences, and the computer is turned on with your personal settings. As you sit in your desk chair iris recognition confirms your identity and you are simultaneously granted access to your company's network and appropriate applications and files.
3:00 pm	You log off your company's network and check bank balances, pay a few bills, and send a biometrically signed document via email to complete your mortgage refinancing contract. Your computer captures fingerprints, keystroke dynamics, and iris images to allow you to access accounts, complete transactions, and send secure email.
4:30 pm	You arrive at a client meeting with representatives of the Department of Transportation at the city airport. Unfortunately, you experience a delay clearing facility security, as the TWIC system and the PIV system are still not communicating well with each other. Your review of the latest upgrades to the Registered Traveler system indicates throughput continues to increase with enrollment now stabilized at roughly 85% of local frequent travelers. The fully automated enrollment stations capturing face, iris and ten-print slaps have been effectively integrated with Passport, DMV, and FBI databases anonymously approving or rejecting candidates. The upgrades have been well received and have successfully resolved both front and back-end usability issues freeing up TSA staff from full-time monitoring responsibilities.
7:00 pm	A quick trip to the supermarket on the way home to pick up a few items. You fill your cart and walk through the fast purchase lane. Each of your items is scanned and your bank account charged via a fused facial and iris recognition authorization tied to the smart card in your PDA as you roll your cart through without stopping.
8:00 pm	Your presence is detected in the entertainment room and identity confirmed through a facial image as you are asked which of your favorite programs you would like to view. Your incoming messages are held and you settle down to watch as you are reminded that it is garbage night.
10:50 pm	As you enter the bedroom, the lights adjust and you are alerted to one non-critical message waiting for you. You leave it until morning and your identity is confirmed as you issue the voice command override your scheduled 11:00 pm sleep settings.

Mega Trends

Critical global trends impacting the requirements and associated development of worldwide IT solutions will have profound implications for the biometrics industry. These *Mega Trends* (Chart 1.8) will continue to drive the adoption of identity-centric, service-based IT models that rely on the trusted linkage of individuals with established identities to specific physical and logical privileges, access, and tasks. Biometrics are a key enabling component of the authentication infrastructure required to support this type of trusted linkage. Therefore, the evolution of these Mega Trends and the IT market demand they create, are integrally linked to the evolution of the biometrics marketplace.



©Acuity Market Intelligence Figure 1.1

1) Globalization and Developing Economies

The nature of commerce and information and resource sharing are in the process of a fundamental transformation. The interconnected networks—human and technology—that are making this transformation possible will continue to increase in complexity and capacity as the nature and volume of information, goods, and services being shared continues to grow. This growth means ever increasing reliance on technology processes that must be reliable, transparent, and secure. The ability to bridge the gap between individuals and their digital identities make biometrics not only a perfect fit but an absolute requirement to sustain this level of trusted digital connectivity.

The on-going evolution of Developing Economies will continue to increase the size and scope of local and global markets. Many of these market environments are skipping twentieth century style industrialization and progressing directly to information based economies. This type of expanding commerce will require stringent authorization and authentication as critical goods and services originate from and are delivered to locations across the globe that lack established and trusted political and economic infrastructures. Whether it is a help desk in India, a parts manufacturer in China, a software engineer in Venezuela, or a consultation with a medical specialist in South Africa, organizations traversing the digital world will no longer have a choice about tightly controlling their environments. The notion of security based on a bounded environment—physical or logical—must give way to a digital world controlled through the use of identity. "Who goes there?" and "What do you have access too?" will become the keys to trusted communication and transactions that drive twenty-first century global trade and economic development.

2) Borderless Economies

The notion of Borderless Economies is nothing new. However, the realization of the concept has accelerated over the last ten years by the near ubiquity of the Internet for personal, commercial, and government use. This is particularly true in the Financial Services arena where near instantaneous access to global transactions has created an unprecedented global financial community. While Globalization and it's associated "off shoring" of manufacturing, technical development, and a range of other business and consumer services are impacting the development of Borderless Economies, an expanding European Union and trade agreements such as NAFTA and CAFTA are breaking down traditional physical and logical borders.

Unfortunately, free flowing global 24/7 trade is on a direct collision course with urgent 21st century security requirements at ports and borders and in cyberspace. The ideal of unencumbered movement of goods and services across the globe came to a rather existential halt post 9/11. The magnitude of the potential threat posed by a world with no borders was suddenly recognized both in the physical and virtual realms.

To date, limited safeguards have been put into place to combat these threats. Some improvement in process and technology has been applied to tracking and monitoring people and the transportation and management of good and containers. Increased logical security and surveillance has also been initiated. However, over the next several decades there will be continued efforts to balance the desire for seamless movement of goods and services with the acknowledgement that physical and logical borderless access pose genuine threats. The identification, authorization, and authentication of individuals involved in accessing everything from port facilities, shipped goods and containers, to manifests, data bases, personnel files, and computer systems must be a central component of providing a secure Borderless Economy.

3) Workforce Decentralization and Mobility
Workforce Decentralization and Mobility are closely related to Borderless Economies and Globalization. The virtual and non-virtual infrastructures that are required for each to thrive are utterly interdependent. As more and more people regularly move across the globe to work, organizations will continually rely on remote and often scattered human resources. This makes accurate, fast, reliable identification and authentication integral to successful commerce. Interestingly, as with Globalization and Borderless Economies, this also links the fate of Commercial entities to the establishment of successful government civil identification programs. These include frequent international travelers or foreign nationals working or residing abroad, truck drivers crossing international land borders, seafarers moving through seaports, off-shored IT workers, and holiday-makers trying to receive time critical emails. As the expectations for location-independent business grow, so too will the requirements for knowing "Who goes there?".

4) Population Mobility
Another closely related IT driver is Population Mobility—much of which is attributable to the pursuit of economic advantage as well as more generalized opportunity e.g. human rights, personal freedom, response to displacement, refugee status, or relocation due to natural and manmade events. Workforce Mobility is usually associated with developed nations' proactive pursuits and Population Mobility with developing nations' forced dynamics. However, these assumptions will increasingly prove inaccurate as global market dynamics shift and create more flexibility in terms of virtual access and more restrictions in terms of physical access. This is a result of a range of market influencers including continued industrial off shoring, the emergence of IT development enclaves in places like India, China, and Latin America, and global climate change impacting agriculture, industrial development, and consumer behavior.

Cross border movements will continue to become both more common and more scrutinized and invariably lead to more sophisticated civil identification and border control mechanisms. This is happening now with the advent of ePassport development in Europe and other nations across the globe and the introduction of biometric-based secure border programs in the UK, across Europe, Australia, and the Middle East. Progress will continue as additional nations impose US-Visit like requirements (Japan has, Canada is considering doing do), and a complex interconnected system of border management is established across the globe.

5) Proliferation of Mobile Devices and Trusted *Access Anywhere*
Trusted, freely available, high-speed network access is a corollary of these other significant *Mega Trends*. It is both an enabler and a result of the evolution of the IT infrastructure that must be developed to support the demands of these changing global dynamics.

There is no question that personal mobile devices—a phone or PDA today or some incarnation in the future—will continue to proliferate. Expectations in developed nations to be utterly connected at all times combined with the relative ease of implementation in developing nations with minimal established communication infrastructures have created a billion unit per year business experiencing sustained growth. Even as circulation of mobile phones approaches—and may possibly exceed— world population, device profit margins will continue to decline and business opportunities will increasingly shift to service based revenues.

The ubiquity of the platform, the need for service-based revenue, and the relative ease and low-cost of expanding networks to remote locations will necessitate the progression of the mobile device as phone to the mobile device as personal access device for communication, information, and transactions. This requires a full-service high-bandwidth wireless network where routine access for low impact and/or cost tasks is essentially free and high-value capabilities are paid for on a subscription or transaction-based model. This model not only requires a reliable, risk-based security framework that requests an appropriate level of user authentication based on the type and value of the information request or transaction, it also means these devices must be available only to those who are authorized to use them and lock-out anyone else who attempts to gain access.

Biometrics have already found their way onto millions of personal devices and will likely become a standard feature within five years. This will accelerate the use of biometric authentication as users familiarize themselves with the technology and service providers have an existing platform to integrate biometric capabilities. This is especially true as Near Field Communication (NFC) technology gains market traction. Mainstream deployment of NFC enabled mobile devices will create a transactional infrastructure that cries out for biometrics.

6) Central Role of Digital Identity
This digital world is already populated with identity information that may or may not be accurate, legitimate, or known to the subject of the information. Creating an orderly, functioning, secure and owner-controlled system given the current state of affairs is not trivial. *However, it is inevitable*. It is very likely that identity infrastructures will be mainstream by 2020. The inevitability of identity-centric IT leads inexorably to the inevitability of biometrics. There simply is no practical way to link a

human identity to a digital identity with any degree of certainty without employing some type of biometric. Biometrics bridges the *human-machine identity gap* in a way that no other technology can.

While there are a host of technical, policy, and process concerns associated with the transformation to identity-centric IT infrastructures, biometrics further complicate the issue. In particular, data ownership, control, and management raise unprecedented levels of concern when the data is biometrics. This is true for personal, commercial, and government applications. While most biometrics are not inherently secret and in many cases (e.g. face, voice) not even private, they are considered intimate personal details which belong to the individual. The drive towards biometrics will therefore require that appropriate protections be embedded in the technology and systems that preserve anonymity to the extent possible for any given interaction. This data is just too sensitive for the responsibility to be left to politicians, regulators, and holders of the data.

7) Inevitability of eGovernment

There are two practical issues driving the Inevitability of eGovernment. They are the costs of providing government services and citizen expectations for improvements in service and security.

Cost of Providing Government Services

It is simply no longer possible for modern states to provide the type and level of government service citizens expect without introducing extensive technology-based access and service. The cost of maintaining manual and semi-automated legacy systems is too high and will continue to increase without substantial automation. In addition, widespread Internet access provides the necessary citizen interface when supported by targeted government investment to achieve universal access.

In developing nations, the inefficiencies and potential for abuse of labor-based systems, even where labor costs are low, simply cannot be justified with the relatively low-cost and proven benefits of implementing technology based systems. Direct citizen access is an issue today with limited Internet accessibility in many nations. However, the need for direct citizen/government contact is often also limited and can be managed through mobile devices and fixed community kiosk-based interfaces in centralized locations. For both developed and developing nations, even where start-up investment is required, the long-term benefits of providing eGovernment services are substantial.

Citizen Demand for Improved Government: Service, Security, Privacy

Citizen demand for convenience in the administration and distribution of government services is rising. The expectation that government can and should match the level of automation and self-service offered by commercial enterprises Is driving these expectations. While it is true not all commercial automation improves the customer experience, services like online banking, account management, and bill pay significantly increase convenience while lowering service delivery costs. This is creating the expectation for a similar service level for routine interactions with the government such as applying for IDs e.g. passports and driver's licenses, paying taxes and fees, or applying for benefits like social security, and unemployment.

There has also been increased concern about the privacy and security of personal information held by the government. Repeated incidents of poor management of citizen data that is lost or stolen coupled with well-documented failures to uphold data protection laws or protect civil liberties in response to increased pressure to pursue intelligence on illegal immigrants or terrorists has eroded citizen trust in government. Citizens want assurances that they have an appropriate level of control over personal information and are not subject to malicious or incompetent misuse of that information. This level of service and security is also an issue for Commercial organizations that have a vested interest in streamlining their interactions with government to improve operational efficiencies and reduce costs.

Together these drivers exert external and internal pressure to develop eGovernment infrastructures that increase efficiency and service delivery, and improve citizen and commercial experience with and faith in government. Once again, biometrics will play a key role. Creating an automated infrastructure that safely and securely handles the volume of transactions required to establish viable eGovernment will require sophisticated identification and authentication capabilities. Individual citizens and appropriate representatives of commercial organizations must be properly identified in order to establish a trusted environment where automated information inquiries and financial transactions can be securely linked to the relevant parties and where personal and proprietary data can be securely managed and stored.

8) Rise of Cloud Computing

Cloud Computing is the ultimate evolution of hosted IT services. These services can be broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Cloud services are fully managed by the provider and sold on demand to a user that has 24/7 access but only pays for the services that are consumed. This "as-a-service" approach requires a level of user-management, accountability, and auditing far beyond what is routinely available in today's hosted IT environments. For the consumer of services—government, Commercial, or individual– the attractiveness of this type of model will be weighed against the risk of essentially co-mingling one's data and resources with an unknown and potentially limitless user base. For the provider of services, the potential for an increased customer base and the ability to leverage economies of scale in delivering services, will be weighed against the potential for abuse and fraud and associated lost revenues. In both cases, biometrics can provide assurance that only authorized, authenticated individuals are accessing services and resources they have paid for and are entitled to.

Meta Drivers

Application Solution Meta Drivers

The Application Solution Meta Drivers are market demand drivers that define a framework for identifying the most lucrative market opportunities. The biometrics industry can be broadly divided into two major Application Solution domains-—Public Sector and Commercial—where each domain has three key Meta Drivers. This framework is not comprehensive in reflecting every possible market opportunity, but rather focuses on key growth markets for biometrically enabled solutions in their respective Application Solution domains. Charts 1.9: Public Sector Meta Drivers (below) and Chart 1.10: Commercial Meta Drivers (next page) show the demand curves for each of the key Meta Drivers. Demand curves indicate the relative intensity of market demand of a given product, service or solution over a given period of time. While they generally parallel the growth curve of a market, they do not quantify actual revenue for the specified Market.

Public Sector Meta Drivers

The three key Public Sector Application Solution Meta Drivers are: 1) Integrated eBorders—the full scope of electronic and automated border control management including travel documents, transportation worker IDs, vehicle access, immigrant Visas and IDs, and expedited passenger systems, 2) eID—includes civil and criminal ID, national and other identity cards, benefits distribution, voter registration, drivers licenses, criminal identification, and other physical and virtual credentials, and 3) eGovernment—fully transactional interactive service delivery for citizens and commercial entities.

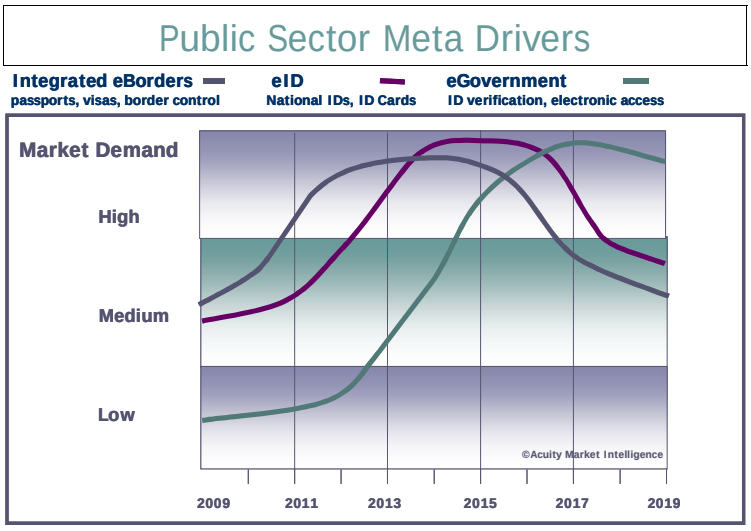


Chart 1.11

The three key Public Sector Meta Drivers are integrally linked. They demonstrate a high-level sequential dependence. Learnings from the development of solutions in eBorders enables the development of solutions for eID which will lay the groundwork for the development of interactive eGovernment services. Public sector ID solutions will therefore progress from highly targeted groups of participants —e.g. expedited air travelers—to broader based groups—e.g. recipients of government healthcare services—and finally to citizen-wide applications—e.g. citizen access to electronic government/ services.

Post 9/11, 3/11, 7/7 terrorist fears acelerate the deployment of US-VISIT and other biometrically-enabled international border control systems. The initial eBorders demand peak has already begun in Europe and the US and will remain in force through 2013. The subsequent demand curve for eID solutions–which benefits from the systems architected for use in integrated eBorders applications–peaks around 2015. Demand for eGovernment will lag sustaining peak demand around 2017 as the authentication implications of large-scale, transactional eGovernment systems are recognized and solutions implemented. As millions of citizens worldwide rotuinely rely on biometrically-enabled identification to travel, identify themselves in various ways, and interact and transact with local, regional and federal governments, human-machine authentication will become an integral component of twenty first century government operations.

eBorders: Post 9/11 eBorders initiatives were introduced to identity unwanted individuals and prevent them from entering sovereign nations. They have been expanded to include expediting low security threat travelers via automated border control systems in Europe, Australia, the US, and the Middle East. To date, there has been a near exclusive focus on managing the “front end” of the border control problem—moving travelers across borders. This includes the issuance of roughly $100 million ePassports worldwide. However, in many respects the “back end” of the problem such as background and ID checks on staff, crew and third-party employee facility access, securing tarmac, shipping lanes, and vehicle access, and protecting the corresponding IT infrastructures pose larger, potentially more dangerous security threats. While there is significant demand in this area, it is likely that sustained growth will occur at a measured pace as countries across the globe continue to develop and deploy customized eBorders solutions.

eID: There are ten EU nations with existing National ID programs. Another thirteen in development, and recently both India (populations 1.8 billion, and Mexico (population 110 million) have announced pans to issue biometrically enabled National IDs. There is even discussion in the US giving citizens the “option” of having a biometrically enabled Social Security card. One of the key issues for any type of electronic identification program is the reliability of the originating documentation and the process used to establish initial ID. In many cases, initial identification is based on documents and processes that are woefully inadequate for establishing a “trusted” identity. This creates the potential for validating and integrating identities that may have been acquired fraudulently. Establishment of an initial, non-reputable identity is key to a reliable, comprehensive identity program. However, managing this risk within the constraints of data protection and civil liberties legislation is no small challenge. Biometrics are an essential element of this proc-

ess even in cases where services or benefits derived form the eIDs do not require biometric authentication as biometrics provide the capability to maintain a chain of trust during the eID issuance process.

eGovernment: eGovernment continues to expand worldwide in an effort to improve efficiency, drive down administration costs, and address government transparency. The number of people using the Internet to obtain government information, pay taxes, apply for permits, and conduct other business is surprisingly high, especially in Europe and Asia. Accessing government services online is an increasingly attractive alternative to standing in line at a government office. As the complexity and volume of eGovernment services increase, so too will the need for trusted authentication. By the time demand for eGovernment peaks, an established biometrics infrastructure will provide the required platform for integrating biometric authentication into the delivery of various eGovernment services.

Commercial Meta Drivers

The three key Commercial Application Solution Meta Drivers are: 1) Enterprise Security - which includes physical and logical access for employees and third parties (customers, vendors, etc.) as well as credentialing and surveillance, 2) Information Transactions – corporate and personal access to travel, financial and healthcare information, business account, supplier and customer information, as well as IP management for technical, scientific and research firms, and 3) Financial Transactions – consumer, business to business, ATM, central bank, and inter-bank transactions. As security threats multiply and various forms of identity theft, fraud, and abuse schemes proliferate, biometrics will offer an extremely cost-effective and truly reliable alternative to more traditional and less secure and convenient forms of authentication.

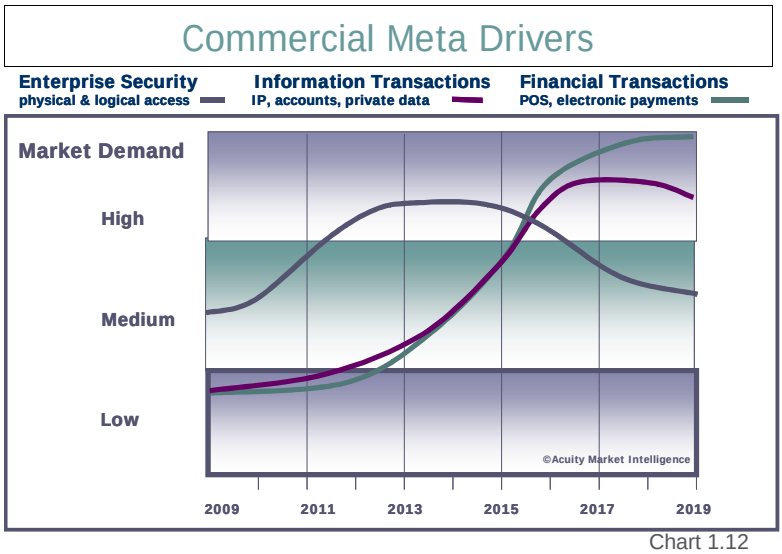


Chart 1.12

Commercial market demand for Enterprise Security will increase thorugh 2013 then begin to trail off slightly after 2015 unitl the market stabalizes and demand remains relatively consistant. Market demand for Information and Financial Transactions will grow slowly through 2013 then begin to accelerate through 2017 when market demand stabilizes as the biometrically-enabled the global authentication infrastructure becomes mainstream. There may also be a large, second wave of Enterprise Security adoption, particularly in Financial Services in response to the development of a mainstream biometric-based transaction infrastructure.

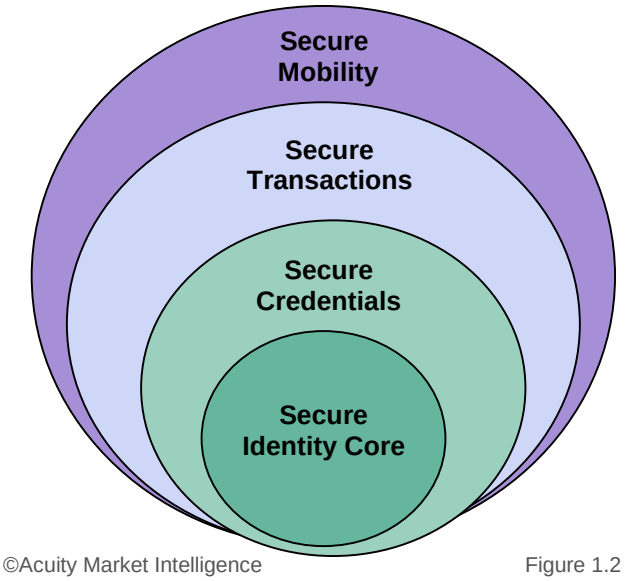
Enterprise Security: Biometrics will become a crucial element of networked solutions for the increasingly porous and ever-expanding physical and logical boundaries of the twenty-first century enterprise. Enterprise computing architectures can no longer be driven by the cyber equivalent of a "perimeter." Interdependent global commerce infrastructures and interrelated value chains for physical goods and intellectual property can no longer be cleanly separated. A new model for understanding the dynamics of the enterprise is required. One that is identity centric—defining and authorizing the roles and privileges of an individual—and includes the entire value chain —the management of the flow of goods, services, ideas and documents. The enterprise is everywhere and defining the "us" on the inside and the "them" on the outside is no longer a meaningful way to manage commercial operations. The "us" and "them" of employees, customers, partners, suppliers, and investors all need to be identified and authorized effectively, efficiently, and reliably as they access the enterprise. The economic crisis of 2008 has slowed major IT investment and impacted market demand in this area, however, applications like time and attendance offer clear, short-tem ROI that can provide immediate bottom-line benefit in lean economic times. Moreover, ever increasing compliance requirements will drive additional biometric adoption, particulalry for logical access to provide non-repudiated audit trails.

Information Transactions: Privacy and security concerns on the part of consumers and security and liability concerns on the part of commercial entities will drive the adoption of biometrically enabled Information Transactions. As complete solutions become available and price/performance curves drop, cost/benefit analysis will begin to weigh in favor of implementing biometrics. Momentum will create an environment where organizations that have not incorporated biometrics to protect storage of and access to personal and confidential information will at the very least appear negligent and at worst be subject to penalties and even criminal negligence for not using a readily available technology to secure their data. The evolution of Cloud Computing will accelerate this process as shared, on-demand service become mainstream increasing requirements for secure authentication.

Financial Transactions.: The development of tightly integrated biometric-based financial service systems that serve millions will take time to develop and deploy. Interestingly, one issue that appears to be a non-issue is consumer acceptance. This is especially true at the point of sale. Vendors are taking biometrics directly to consumers in retail applications and much to the surprise of many industry pundits and privacy advocates alike, consumers are responding with enthusiasm. Large-scale, widespread POS deployments face daunting infrastructure and integration issues, however, there are other roadblocks constraining the rapid development of an infrastructure that has the capacity to incorporate a variety of new payment interfaces and mechanisms as well as service existing ones. Mainstream payment processors have not shown a strong interest in biometrics. Considerable pressure will have to be exerted on established financial service and payment processing organizations to adopt such significant change. This is beginning to happen as biometric payment solutions encroach on their turf and offer viable alternative to traditional payment mechanisms.

Technology Evolution Meta Drivers

Technology Evolution Meta Drivers represent a set of foundational capabilities that must be developed to adequately address the requirements of the Application Solution Meta Drivers. They are: Secure Identity Core, Secure Credentials, Secure Transactions, and Secure Mobility. These capabilities are key components of a larger evolving framework that will enable the development of a reliable, secure, worldwide identity-centric IT infrastructure that biometric authentication simultaneously plays a central part in creating and relies on for significant market expansion.



©Acuity Market Intelligence Figure 1.2

Secure Identity Core

The Secure Identity Core is the safe house for *digital identity*. It is a conceptual model rather than a physical construct reflecting how identity data ought to be handled. Developing this identity core is a complex and multidimensional problem involving many facets of IT. Biometrics related issues include preventing raw image data from being network accessible, distributed storage of various biometrics—image and templates—for a given individual, separation of biometric from other personal details, secure transmission of local authentication for networked applications and secure transmission of centralized authentication for local applications, and standards that allow proprietary devices and algorithms to interoperate. While there is still much to be done, standards are emerging and encryption technology is improving for both storage and transmission of data. And, biometrics solution providers are beginning to integrate these capabilities into their offerings.

Secure Credentials

Secure Credentials, both physical and virtual, facilitate the link between an established identity and a claimed identity. Even in cases where biometrics are not required to confirm the credential holder's identity to complete a given task, biometrics are essential to maintaining the chain of trust throughout the credential issuance process. This ensures that the individual who initiated the process is the same individual present at each step. A Secure Credential therefore both validates an individual's claimed digital identity and enables Secure Transactions to take place. To date, most of the investment in large-scale biometric identification programs has been spent on the enrollment and credentialing process e.g. the US TWIC program, ePassports across Europe, voter registration and authentication programs in Mexico, Uganda, etc..

Secure Transactions

Secure Transactions bind individuals to actions such as information inquiries or payments. The level of security for any given transaction will vary greatly with the sensitivity and/or value of the specific action as well as the particular circumstances. Is the individual present? Is the transaction routine? Is there an established relationship between the entities involved? All of these factors must be considered within the context of dynamic risk analysis that determines the appropriate level of required authentication. This all takes place near instantaneously within a network capable of securely, anonymously (as appropriate), privately (as required), and seamlessly conducting information, financial, and eGovernment transactions. The use of biometrics—which modality, multiple, none—may be also dynamically determined based on the level of risk for a given transaction. Today a number of biometrically-enabled transaction capabilities have been deployed for healthcare information, POS, ATM, and check cashing applications. These initial closed-loop applications provide a glimpse into the range of possibility for a fully biometrically enabled Secure Transaction environment.

Secure Mobility

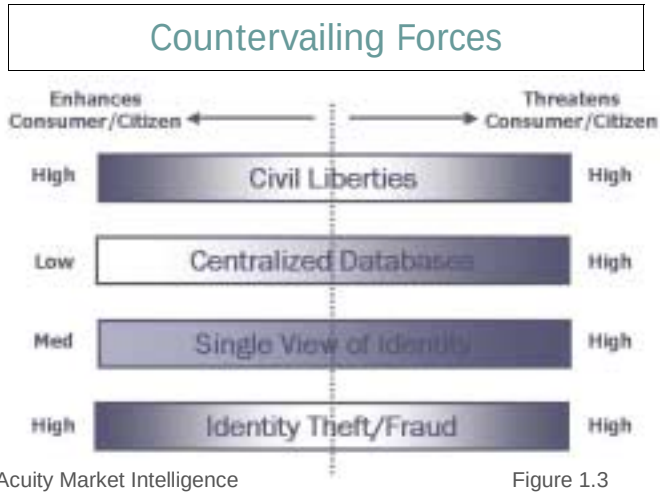
Secure Mobility is a result of the implementation of other three Technology Evolution Meta Drive capabilities. With a trusted Secure Identity Core, Secure Credentials, and the ability to Secure Transactions, individuals will move freely whether it be virtually across IT networks or physically through transportation systems and borders. Secure Mobility therefore involves creating a vast interoperable environment where various credentials and established identities can be used to gain virtual or physical access. This requires 1) defining standards for equivalent credentials such as passports, drivers' licenses, or travel cards, 2) determining what constitutes authentication within a given context such as access to a passenger's travel plans, expedited access through airports, or conducting financial transactions, and 3) dynamically evaluating risk and adjusting authentication requirements appropriately. The ability to integrate disparate systems relying on only as much data as is minimally necessary to perform a specific task while protecting sensitive data and sharing it in some universal and standard way is an ideal that supports the goal of creating a "seamless" experience. This seamless experience is by definition Secure Mobility and based on recent successful pilots and deployments, it is likely to be built upon the imminent widespread uptake of mobile phone-based NFC technology.

Obstacles and Opportunities

Mainstream biometric deployment faces obstacles ranging from inherent limitations of the technology and failure to adequately plan for and implement deployments to fears about violations of privacy and civil liberties. One of the more intriguing aspects of the marketplace is that many of these real and perceived obstacles represent significant opportunities for biometrics market development as well. For example, privacy advocates and civil libertarians fear that widespread use of biometrics will enable a surveillance society, however, they also complain vigorously about the woefully inadequate security measures in force to protect individuals from identity theft and fraud. In this case biometrics could be the problem or the solution blurring the distinction between obstacle and opportunity. The most effective strategic response to this dynamic is to transform obstacles into opportunities through the appropriate use of biometrics.

Countervailing Forces

Four key areas of concern considered outside the purview of biometrics—nonetheless critical to the mainstreaming of biometrics—reflect this phenomenon. They are: Civil Liberties, Centralized Databases, Single View of Identity, and Identity Theft/Fraud. Proactive engagement by market players can ensure that biometrics enhance rather than threaten consumer and citizens within each of area of concern. The potential repercussions of poorly applied or managed biometrics in any of these areas could prove catastrophic for the industry. The onus is therefore on organizations vying for market leadership to build safeguards directly into the technology and application solutions that address these concerns. In the end, regardless of fault, the biometrics industry as a whole will shoulder the blame for any failure or misappropriate use or abuse of biometrically enabled systems.



©Acuity Market Intelligence Figure 1.3

Civil Liberties

Civil liberties considerations are paramount to the acceptance of widespread deployment of biometrics for government, Commercial and consumer applications. The industry has learned through flagrant miscalculation such as the infamous "Snooper Bowl" incident where facial recognition was used for crowd surveillance without the knowledge or consent of the subjects, that the violation — or even the appearance of the violation — of civil liberties can instantaneously transform an innovative application into a nearly unrecoverable public relations fiasco.

In response to this type of blunder and the increasing digitizing of our lives, worldwide concern over the proper use and abuse of electronic data has created a new class of legislative and policy initiatives that address data protection, civil liberties, and privacy. Though it may seem counterintuitive, biometrics industry players must actively engage in the development of public policy and legislation to limit the potential abuse of biometrics data and data protected or secured by biometrics technology. They must take responsibility, not only for the capabilities of the technology, but for the potential harm as well.

However, policy and regulations are not enough. **The industry must embrace civil liberties as part of the overall problem to be solved by biometrics from both a technology and solutions perspective.** This creates the opportunity to drive the agenda rather than continually devoting resources to deflecting criticism and quelling public concern. This type of proactive stance is not a luxury but rather a requirement for serious market players, else civil liberties concerns have the potential to completely overshadow the demonstrable benefits of biometrically-enabled solutions.

Centralized Databases

Digital identification is a defining characteristic of twenty-first century life. It is nearly impossible to avoid having some form of personal information stored in a database somewhere. Health, financial and insurance records, customer loyalty programs, even library cards place everyone in somebody's database. The reality of scattered databases is now unavoidable, however, the development and use of massive centralized databases for civil or commercial applications is the subject of intense debate.

For many in civil, criminal, and commercial applications, the massive Centralized Database is the holy grail of data management. And while some may argue the contrary, it is generally accepted that storing complete identity profiles, particularly those that include biometrics, in one massive data repository—regardless of how much security is applied—is a bad idea. There are instances where centralized data storage does make sense. This is the case for anonymous biometrics identification where the goal is to confirm whether or not an individual is already in the database. This type of solution would not include other personal data and would not pose a risk that an individual's biometric data could be compromised as there is no way to connect the data to an existing identity. It can, however, provide significant benefits like preventing

fraud in government distribution programs with very little downside. This was, in fact, the compromise recently brokered in the Israeli Knesset where the establishment of biometrically enabled national IDs with centralized storage of citizen data created political controversy and was on track to derail the program. The proposed compromise: biometric data will be secured in an "unconnected" database managed by one government agency, and personal data will be stored and managed in another database by another agency. The two will be linked by a unique ID code. The biometrics industry would do well to learn from this example: the centralized database was far more objectionable than the collection of biometrics.

Single View of Identity

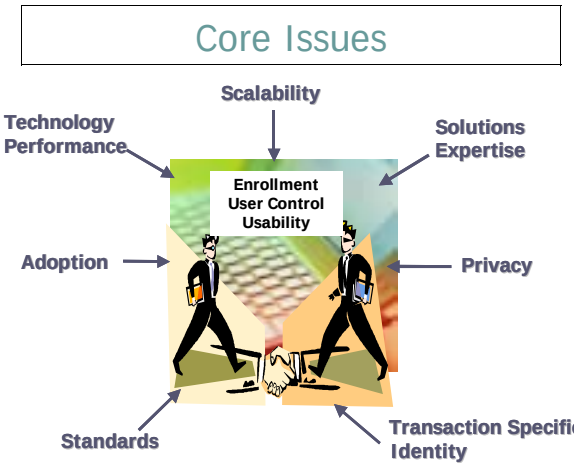
A corollary to the holy grail of Centralized Databases is the notion of a Single View of Identity. All information about a single individual is tied together so that any information on an individual leads to all information on an individual. This type of centralized identity is considered antithetical to democratic values by most privacy and civil liberties advocates who see biometrics as a fundamental enabler of this kind of system. It is important to separate the use of biometrics from this type of identity architecture. In fact, biometrics can actually provide a solution, not by preserving anonymity but by using an individual's biometrics to control all of their personal information. In addition, data storage should be distributed so that there is no single physical or virtual location where an individual's identity and personal information reside.

Identity Theft/Fraud

Biometrics has the potential to help eliminate or exacerbate identity theft and fraud. The worst-case scenario—and the one critics of the technology focus on—is that someone could "steal" an individual's biometrics and assume their identity. While it is not yet clear how this would work in practice, the fear persists. The more ideal scenario is where an individual's biometrics are used as keys to access personal information and conduct transactions. Given the frequency of data breaches—Privacy Rights Clearinghouse reports that more than 250 million US records have been breached since 2005—this may pave the way for the biometrics systems that promise to provide a unique lock on data that only the rightful owner can grant access to.

Core Issues

There are also *issues central to deploying biometrics* where obstacles and opportunities are integrally linked. Two categories of concern are how to Bridge the Human-Machine Identity Gap and what it takes to achieve complete Solutions Development.



©Acuity Market Intelligence Figure 1.4

Bridging the Human-Machine Identity Gap

The complexity of developing and implementing biometrics rests in the nature of the technology itself; biometrics is a science of human-machine interaction. Biometrics success in bridging this human-machine divide will depend on how well three critical issues are managed: Enrollment, Human Factors, and Privacy.

Enrollment: While enrollment can easily be considered an aspect of Human Factors, it plays such a significant role in terms of user experience, system performance, and cost that it is singled out for consideration. Enrollment requires the highest quality biometric data capture while providing a convenient, standardized—or at least familiar—user-friendly experience. There is simply no way to scale biometrics applications to global identity solutions without adequately addressing enrollment. In fact, the majority of spending to date, on biometrically enabled identification programs has been on enrollment. This is because enrollment is managed on a brute force basis with significant attendant intervention. Though it is the most time-consuming, labor intensive, and costly part of introducing a biometrics, enrollment receives relatively little focus as a key enabler of a successful deployment. This dynamic must change.

Human Factors: Human factors considerations are not a luxury but a necessity for any biometrically enabled system intended for widespread use. Human factors consideration have been incorporated on a limited basis into the design of biometric devices, however, the science of human factors has been largely ignored on the solutions front. Human factors in this context includes ease of use, intuitiveness, acceptability, convenience, ergonomics, and social acceptability for all constituent groups that may come in contact with the technology: end-users, design, support, operators and maintenance staff. In the same way that new human-machine interfaces were developed in the 1980's in response real-time 3D computer graphics capabilities,, significant human factors challenges exist in regards to designing user-friendly biometrically-enabled systems. Today's deployments often seem to have been developed in isolation with little shared leanings or human factors best practices applied.

Privacy: Policy makers, privacy advocates, and security experts have expressed serious concerns about how biometric data will be collected, used, stored, managed, and disposed of. The abrupt termination of the CLEAR registered traveller program brought these issues into focus as participants were left wondering about the fate of their personal and biometric information. Three is a valid fear that an individual's biometrics may be stolen or misused in a way that has permanent repercussions for the individual. As biometric surveillance capabilities become a reality via Face or Iris recognition, these concerns are exacerbated. One approach to addressing privacy concerns currently under development is the creation of a "revocable" biometric. Highly encrypted biometric identifiers could expire on a given date or be cancelled at the owner's or operator's discretion or if they are compromised.

Solutions Development

To date, development efforts in the biometrics industry have focused on the performance and reliability of the technology. This has been vital to elevating the technology to a level of being truly useful i.e. reliable, accurate, affordable. However, in order for biometrics to progress beyond this level of reasonable usefulness and become a true enabler of broad-based identification solutions, the technology must be developed and integrated within a larger solutions context. Four components crucial to effective biometrics solutions development are: *Extensible Security, Context Specific Identity, Price/ Performance,* and *Interoperability.*

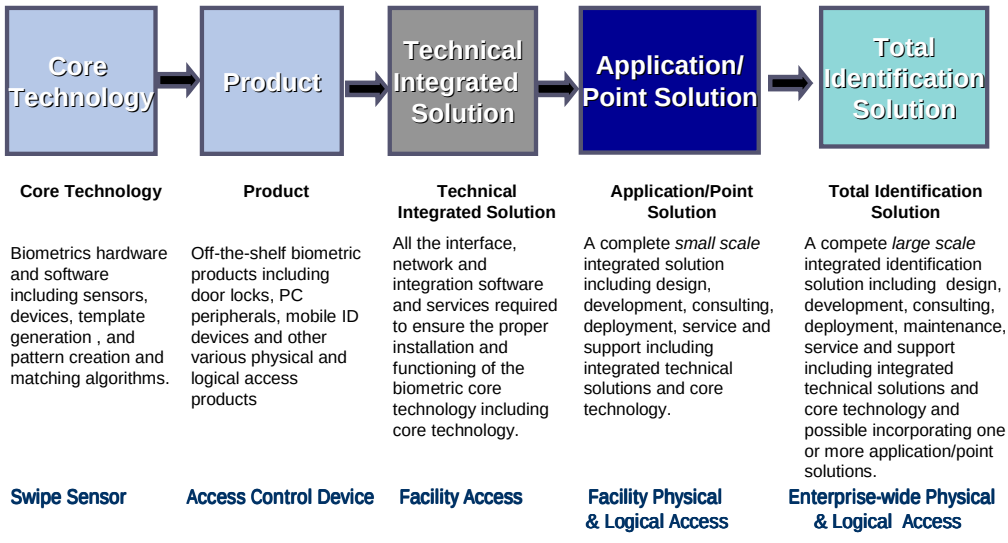
Extensible Security: The biometrics industry has yet to come terms with its inherent responsibility to address the issue of Extensible Security. Security must be built-in to technology and solutions to ensure data and communications integrity, protect privacy, and prevent misuse of data. While much emphasis has been placed on spoofing, it is far easier to compromise a simple authentication confirmation—essentially a yes or no—than it is to create a gummy finger or a false contact lens. Though biometrics will be a small component of complex IT infrastructures, biometric vendors must work with solution providers and integrators to ensure that security extends beyond the device or software throughout the system that depends on biometric authentication.

Context Specific Identity: All the possibility and challenge of creating and managing a worldwide identity centric network is dependent on defining "Who goes there? And "What does this identity have access to?". This includes defining the "Who" and the "What" in a context specific way so that only as much identity and associated content information as is needed for a specific action is revealed. When considering the ultimate scope of identity based applications, and biometrics in particular, it is hard to imagine a networked infrastructure of this magnitude not employing context specific identify. The perceived or genuine threat aside, data storage and processing requirements make any other approach untenable. Again, biometric vendors must proactively contribute to the development of this type of identity framework. Leaving it to others to work out is a recipe for market development disaster.

Price/Performance: Historically, biometrics have been expensive technologies with limited accuracy and reliability. Today they work well enough and are cost effective enough to support a wide range of solutions. However, over the analysis period price/ performance curves for the various modalities will drop to the point where for most applications cost and performance will not be factors in deployment decisions. There will continue to be specialized and high security uses of biometrics that demand increased accuracy and reliability. These non-price sensitive solutions will encourage leading-edge technology development by providing the impetus and research and development funds that will continue to improve performance and drive prices down for existing biometric modalities and encourage the development of new modalities. For the majority of applications, biometrics as a commodity is essential for widespread success.

Interoperability: Interoperability has been a key obstacle to solutions development and, until recently, a bitter point of contention within the industry. Though there are still internal battles regarding proprietary technology approaches and solutions, it is widely accepted that the industry as a whole will not progress unless uniform standards allow the integration of technologies from various vendors. Many large commercial and government contracts will not be undertaken without the ability to select image capture devices and algorithms from multiple vendors. Standards are evolving and some third party vendors are taking on the interoperability challenge, but much work remains to be done.

Solutions Value Chain



The progression from Core Technology to total solution is illustrated in the Solutions Value Chain chart .

While the progression across the value chain from Core Technology to Total Identification Solution seems intuitive, its practical application is convoluted at best. As with all models, the market realities do not reflect such neatly defined categories. It does, however, provide a conceptual framework for understanding the iterative nature of the evolution of biometric-based solutions.

The further across the chain a vendor plays, the greater the potential revenue and the more important the ability to address the solutions development issues.

Figure 1.5

State of the Market

The NEW STATE of the Biometrics Market

The market for biometrics is in a strange state and will most likely not follow the typical path of disruptive technology adoption. Biometrics have been considered a disruptive innovation on the verge of breakthrough for an extended period of time. Post 9/11 security concerns that were meant to propel the biometrics market forward, created an even greater expectation of rapid market acceleration that never materialized.

In terms of classic emerging technology adoption as defined by Geoffrey Moore in his high-technology market development bible, "Crossing the Chasm", this translates into an expectation of rapid *Chasm Crossing* from early to mainstream markets, followed by a phase of highly targeted and leveraged *Bowling Alley* market development, progressing to a period of nearly insatiable market demand— the *Tornado*. Instead, over the past few years the market has essentially passed over the Chasm and stalled out. This is due to two critical factors: 1) the failure of technologies to deliver promised capabilities, and 2) the failure of market players to develop complete, commercially viable solutions to targeted business-breaking problems based on currently available technology capabilities.

There has been far too much infatuation with the belief (wish?) that large government contracts – not targeted commercial opportunities – would be the engine driving rapid market expansion. Progress on the government front has been substantial, but has not provided the scale of opportunity necessary for the industry to thrive. The result: market players—with few noteworthy exceptions—have failed to leverage the classic target market development phase of the adoption lifecycle to produce commercially viable, proven solutions which would then be directly applicable to large-scale ID systems.

This has created a market dynamic where biometrics as a class of disruptive or discontinuous technology has not moved completely through its revolutionary market development cycle and yet is now subject to significant evolutionary or continuous innovation. In other words, just as biometrics are beginning to stabilize and deliver on past promises, current expectations continue to be driven by “next generation” technologies.

While there is now clear industry momentum towards solutions development, the *market making* opportunity has passed. The industry is no longer in a position to define the marketplace but rather is increasingly subject to *very specific* market driven requirements and customer demands. It is therefore likely that market will experience linear growth rather than the exponential growth most readily associated with Moore's technology lifecycle. Rather than the typical "hockey stick" curve of recent innovations such as mobile phones or the Internet, biometrics adoption will mimic the growth curve of ATMs, which achieved roughly 80% adoption through linear growth over a period of 20 years.

This has significant strategic market development implications. In a classic market development scenario, target market penetration precedes concern with larger opportunities. This is the process of developing dominant category positioning to leverage the ensuing "Tornado" phase. However, given the current state of the marketplace, biometrics players—across the value chain—must simultaneously manage progress towards expansion into large looming market opportunities while rigorously and systematically building a target penetration strategy. The industry must relinquish the mantle of disruption innovation and focus on *truly delivering* on the promise of biometrics by providing working solutions to real problems based on existing capabilities. *Biometrics that actually work*.

Post 9/11 Government Bonanza – Taking Stock

The post 9/11 promise of biometrics was integrally linked to a series of initiatives proposed by the US and other governments beginning in late 2001 and 2002. 9/11 essentially provided the impetus for biometrically enabled ID programs in the US and across the globe. Existing ID initiatives were given a strong boost and new initiatives were developed to create more reliable and secure identification documents, programs, and processes. Industry vendors, integrators, pundits, and the investment community were whipped up into a near hysterical frenzy believing this to be the basis of an on-going, thriving, biometrics marketplace. Nearly eight years later, the dust long settled, expectations have been greatly scaled back *as* these initiatives have varied significantly in the success they have achieved.

US-VISIT seems likely to remain an entry only program as multiple attempts to create the exit portion have failed. Registered Traveler (RT), once touted as “an enhanced security program” for frequent fliers, was scaled back to a cut-to-the-front-of-the-line opportunity whose future crashed with the abrupt collapse of Verified Identity Pass’s CLEAR program in June 2009. Just prior to CLEAR’s demise, the US House of Representatives passed a bill to reinstate the TSA background checks for RT. However, given the status of CLEAR and the long list of legislative priorities, it is unlikely the US Senate’s companion bill can be expected any time soon. Meanwhile, The latest “potential” biometrics boon is wrapped around the illegal immigration debate. There is discussion in the Senate of creating a biometric identification for all US workers—a smart Social Security card?. This will no doubt receive much hoopla in the biometrics industry and be the subject of grandiose plans. However, it is just as likely to face the kind of obstacles thrown up over REAL-ID and be subject to the type of scaling back the TWIC program experienced.

There are any number of reasons why these and other biometrically-enabled programs have been less successful than originally planned. The reasons range from overly ambitious objectives relative to technology capabilities and underestimating the overall systemic and infrastructure implications, to poor planning and implementation and relying on unfunded mandates. The Post 9/11 Program Review chart (below) provides a glimpse into some of the most visible of these initiatives and highlights the initial objectives and results to date.

Post 9/11 Program Review

Program	Program Objectives	Status/Results
US-VISIT	Initial program required automated entry-exit program be implemented at the 50 busiest land ports of entry by December 31, 2004. First mandated for immigration control. Post 9/11 shift in priority to border security. Biometric checks to ensure individuals crossing borders were individuals issued travel credentials. Established to secure border, understand who is entering and leaving the country, prevent terrorists form entering the US, and facilitate legitimate travel and trade.	Large AFIS two finger database (0 M+) converting to 10 print slaps. Effectiveness of system challenged. 2400 immigration violators and criminals identified since January 2004 – total cost to date? $15B+ and Cost per individual? No EXIT program—2 failed pilots. Extreme pushback against latest (April 2008) plan to have airlines collect biometrics on exit. DHS acknowledging may not be possible at land ports because of physical infrastructure requirements.
Registered Traveler (RT)	Background checks and biometric authentication of frequent or "Registered" Travelers. Proposed to address unmanageable post 9/11 airport security lines. Initially conceived as a government program. Morphed into a public-private partnership model. Commercial enterprise when introduced as a "cut to the front of the line" program when it finally emerged in 2007.	TSA dropped RF background checks. Most visible and "successful" operation—CLEAR—abruptly ceased operations in June 2009 due to the inability to secure additional financing. Usefulness of RT questioned as average security wait stabilized at 10 minutes & RT subject to standard security check.
UK National ID	Introduced May 2005. Each ID card would be unique, and combine \cardholder's biometric data with checked and confirmed identity details - a 'biographical footprint'. These identity details and the biometrics stored on the national identity register. Basic identity information held in a chip on the ID card itself. Cards linked to owners by unique biometric information.	Mandatory program cancelled in June 2009 after significant privacy, fiscal, and political pushback. Now an "opt-in" program that may be headed for total collapse base don political outcome. Some elements part of ePassport program.
EU ePassports	US-Visit program required 27 countries to begin issuing electronic passports to allow their citizens to qualify for visa waivers when traveling to the States. EU mandate for e-passports went into effect on Aug. 26, 2005, just prior to an Oct.26 deadline for the Visa Waiver countries. First generation' include biometric data consisting of a digital representation photograph. The 'second generation' will also contain fingerprint biometric.	100M ePassports issued to date. US nearly 15M. US reader deployments— DHS CBP has requested 5000 ePassport readers at 372 border entry points. Only 500 have been purchased, just 247 have been installed. Readers are at 33 US international airports, which covers 87% of visa waiver country travelers. EU deadlines are about issuance not deploying readers.
Transportation Worker Identification Credential (TWIC)	Tamper-resistant biometric credential issued to transportation workers who require unescorted access to secure areas of transportation facilities, port, hubs, etc. Initially envisioned to cover 9 to 12 million. Scaled back to maritime only—ports, vessels, outer continental shelf facilities and all credentialed merchant mariners.	Beset by delays, Oct. 16 2007, Wilmington, Del. became first port to enroll workers in TWIC. Sept 2008 deadline pushed back – only 500K enrollments, Finished June 2009 1.2 million. Run rate 1.2 million enrollment in 20 months, 60,000 a month—far too low for major ID program. In Feb 2009 first fraudulent TWIC cards found —physical security features caught perpetrators.
Schengen Information System II	Government database system used by several European countries to maintain and distribute information related to border security and law enforcement. Originally scheduled for 2007	Delayed until 2010. European Commission stated testing revealed problems with robustness of system and consistency of data.
HSPD-12	Post 9/11 executive order - August 2004 - requiring smart card IDs for all federal l government employees and contractors including military. Develop a common identification standard that ensues claimed identities can be confirmed and government facilities and sensitive information stored in networks remain protected. Unfunded mandate left to each individual agency to solve.	October 2007 deadlines to complete background checks and issue cards not met by any agency. GSA stepped in, created centralized solution offering for agencies that did not want to mange. As of April 2009 OMB reported agencies issued cards to more than 2.7 million accounting for 48 percent of contractors and 47.9 % of government employees who need the IDs
REAL-ID	2005 U.S. federal law that imposed security, authentication, and issuance procedures standards for the state driver's licenses and state ID cards, for them to be accepted by the federal government for "official purposes". Secretary of Homeland Security defined "official purposes" as presenting state driver's licenses and ID cards for boarding commercially operated airline flights and entering federal buildings & nuclear power plants.	Significant push back. Considered an attempt to create a National ID. Many states passed laws stating they would not comply. DHS under Obama is recasting REAL-ID to PASS ID which is suppose to be cheaper, less rigorous and partly funded by federal grants.

Chart 1.13

Application Analysis

Biometrics, like all emerging technologies, perform best in markets where inherent characteristics make them uniquely applicable to solve a significant, preferably a business-breaking, problem. Two application areas—one a biometric stalwart, the other a bleeding edge use of technology—are positioned to leverage the unique capabilities of biometrics and experience significant growth over the forecast period.

The Rise of Time and Attendance

In an economic climate where IT expenditures must be short-term and ROI based, proven results are driving market expansion in an arena where biometrics have moved well past the point of being considered “high-tech gimmickry” to hold an indispensable position as a technology that uniquely solves the problem of linking each worker to their personal labor record. Biometrics not only offers the only effective means of addressing this business-breaking problem, but also has more than a decade of proven performance, reliability, and cost savings in Time and Attendance applications. Recently, biometric have become an integral component of workforce management solutions as well as they rely on accurate and secure data to achieve their goals of optimization and reduction of labor costs.

Industry estimates place intentional and error-driven time theft in the range of 1.5% to 10% of gross payroll costing businesses hundreds of billions of dollars each year. Most organizations find the savings from eliminating buddy-punching (one person clocking in or out for another) alone justifies the investment in a biometric Time and Attendance solution. Additional cost savings are achieved from reductions in overtime and payroll expense, eliminating the need for time-clock supervision, and eliminating processes and supplies related to time card, badge, or PIN-based time and attendance systems. Finally, the cost of biometric devices and integrated solutions has fallen significantly over the last few years, making biometrically-enabled Time and Attendance a practical investment for companies of every size. Over the next few years, the uptake of biometrics in this understated market is poised to thrive. Time and Attendance forecasts are included in physical access projections, which will maintain is overall percent of global revenues between 13% and 14% but grow from $403 million to $1,541 million over the forecast period.

Minority Report: Distance-Based Surveillance

Surveillance is the ultimate dream application of intelligence and defense communities and the waking nightmare of privacy and civil liberty advocates. It has simultaneously provided the incentive for significant research and development and commercial investment while raising the profile of biometrics as a frightening threat to the fabric of democracy. Until now, the conflict and debate has been largely academic. However, today, there are biometric technologies providing distance-based, real-time, non-cooperative image capture i.e. surveillance.

Both Face and Iris recognition are commercially available in the two-meter range and are on the verge of operating in the ten-meter range. These biometrics are certainly not as accurate or reliable at ten-meter distances as they are within two meters, but the technology is rapidly improving. Another biometric of interest in the surveillance arena is gait recognition. This is particularly useful when trying to identify individuals whose Face and/or Iris are not visible.

Convenience-based applications for this type of technology include: increased throughput for airport passenger check-in and security lines, high-speed staff access control, ensuring every cruise passenger has re-boarded a ship before port of call departure, etc. There are also circumstances where identifying someone at a distance is a valuable and potentially life saving tool: identifying military threats on approach to facilities and checkpoints or alerting police to a kidnapped child being transported through an airport or train station. In spite of these kind of innovative solutions designed to protect the public or military, this capability opens Pandora's Box and provides highly combustible fuel to the fire of privacy and civil l liberties advocates who have long claimed that biometrics in and of themselves pose a significant threat to free and open societies. The ability to track an individual based on their biometrics takes the notion of a surveillance society to a level many are extremely uncomfortable with and fearful of. Given recent unrest in highly controlled societies like China and Iran and the revelations of warrantless wiretapping and other surveillance activities by US authorities against US citizens, these fears seem well founded.

There has already been significant pushback to biometrically enabled identification programs in the US and Europe e.g. passage of sate laws defying REAL-ID, the NO2ID group in the UK. As the surveillance capabilities of biometrics continue to expand, so to will the opposition of biometrics for these and other applications. However, in spite of these forces, surveillance is expected to grow as an astounding CAGR of 60.99% posting the strongest percentage gain of all applications from less than 1% to nearly 8% of total market revenue representing growth from approximately $19 million to $872 million annual revenue over the forecast period.

Hype versus Hype versus Reality for Biometrics in Financial Services and Healthcare

If you ask most biometric vendors to identify their most promising commercial market opportunities, nine out of ten would put Financial Services and Healthcare at or near the top of the list. There have and continue to be strong justifications for these choices. Both are highly regulated industries with compliance based identification and authentication needs. Both are required by law and consumer demand to protect the privacy of their customers. Both have obvious operations and service delivery issues that can be well served by implementing biometrics. Yet, both have failed to materialize as the biometrics "gold mines" as expected and projected for many years. Is this dynamic poised for significant change?

Possibly. But this depends on the lens through which market development is viewed. The notion that Financial Services and Healthcare each represent a single vertical market sector has been one of the barriers to market adoption. These are vastly complex industries with elaborate operational infrastructures and each represents a range of market opportunities for targeted biometric solutions. Biometric vendors tend to focus broadly on an industry rather than specifically on one solution to one problem within a narrowly defined target in these industries. As discussed in the *New State of the Biometrics Market* section of this report (page 1-20), this unwillingness to focus on clearly identified business-breaking problems within targeted segments has thwarted the long anticipated exponential market growth of biometrics for commercial applications in Financial Services and Healthcare.

The segmentation applied in this analysis splits Financial Services and Healthcare into components of the Commercial market sectors—Enterprise Security and Information Transactions. There is also a third Commercial market sector devoted exclusively to Financial Transactions. Each of these sectors is divided into multiple targets and mapped against applications—Physical Access, Logical Access, Identity Services, and Surveillance—creating a complex targeted segmentation of these industries. It is within this context the possibilities for financial services and healthcare are examined.

Will the Financial Meltdown of 2008 Drive Biometric Adoption?

Biometrics in c continues to be a mixed bag. Adoption for physical access is happening in isolated cases but there is no genuine market momentum. In spite of the increasing inconvenience and cost of password management, logical access Is also facing slow, sporadic adoption.

The economic crisis of 2008 is seen my many as yet another golden opportunity for biometric based logical access. The notion supporting this opportunity is that somehow providing more accountability within large Financial Service firms would reduce the risk of this type of calamity. It is not clear exactly how biometric would help, if governments are really going to follow through with significant restricting and regulation—and this is a big if—what specific problem will biometrics solve? Furthermore, why are organizations that made hundreds of billions in revenue in high-risk endeavors and paid little if any price going to be motivated to do anything differently e.g. adopt biometric authentication to secure logical access or transactions? This is yet another red herring for the industry.

This is not to say that there are not strong arguments to be made for biometrics adoption in this arena. For example, the fraud at Societe Genreale Bank in France where a single trader with prior back-office experience was able to circumvent controls and lose billions of euros is a great argument for biometrics authentication. Had biometrics been used for logical access, it would have been far more difficult, if not impossible, for this individual to borrow colleagues' log-in credentials and delete and forge transaction records to cover up his scheme. The problem here, as with most organizations of this size and stature, is that it is hard for them to realistically access the risk until a breech of this magnitude occurs. And other banks and brokers are loath to learn the lesson operating out of a "it can't happen here" mentality. This is one of man reasons that penetrating the Financial Services sector has been and remains an arduous task. It is in many ways inevitable that adoption will occur but not at the rate that would seem prudent to many outside of the industry.

In the end, not even calamities like the near total collapse of the global financial services market or the events at Societe Genreale Bank is enough to spur rapid biometrics adoption. There are, however, a number of bright spots for biometrics in Financial Services.

Biometrics are being introduced to provide financial services to the rural un or under-banked in India and Africa and have been used for this type of application effectively in Colombia with coffee bean farmers for years. Establishing the identity of a rural depositor through biometrics makes it possible for the illiterate or barely literate to become part of the banking user community. In India, banks have deployed biometric ATMs to boost micro financing initiatives. In Africa and in South America, initiatives evaluating the use of biometrics to access low-cost ewallet government benefits cards are underway.

Though the failure of Pay By Touch (discussed below) was a setback in the evolution of biometrically enabled consumer POS transactions, the check cashing operation that was originally purchased from BioPay was spun back off as BioPay Paycheck Secure. The company has recently been renamed AllTrust Networks and seems to be thriving. AllTrust claims to have enrolled more than 5 million users and processed 62 million biometric financial transactions worth $27 billion. This

company was very focused from its inception on the lucrative but high-risk check cashing business. They provide a biometric solution that manages check fraud in a way that reduces risk and increases profits and customer convenience.

The evolution of the NFC enabled mobile phones (and PDAs) could very well be the engine that ultimately drives the adoption of biometrics for Financial Services. There have been dozens of successful pilots and tests of this technology across the US, Europe, Asia, India, and Australia. Almost without exception, when the programs are completes, participants complain about giving up their phones. This infatuation with NFC will likely lead to fairly rapid development of integrated NFS transaction infrastructures that continue to enable more and more advanced information and financial transaction capability. This will be a problem crying out for biometrics. Not only to lock the devices, which will become increasingly more valuable as they hold more and more personal and financial information, but also to authenticate high-risk or high-value transactions. Tens of millions of mobile devices are already shipping with embedded biometrics with these numbers likely to rapidly increase over the next few years. It may very well be that as NFC proliferates and mobile phones and PDA's become personal authentication devices—holding everything from credit card information and boarding passes to healthcare records and ePassports—biometric authentication's essential role in this transaction infrastructure will then force more mainstream integration of biometrics in traditional information and transaction environments. It is possible, consumer uptake and demand may very well drive a secondary wave of Financial Service enterprise adoption of biometrics. (A conceptual model of the NFC enabled Personal Authentication Device (PAD) is shown in Figure 1.6).

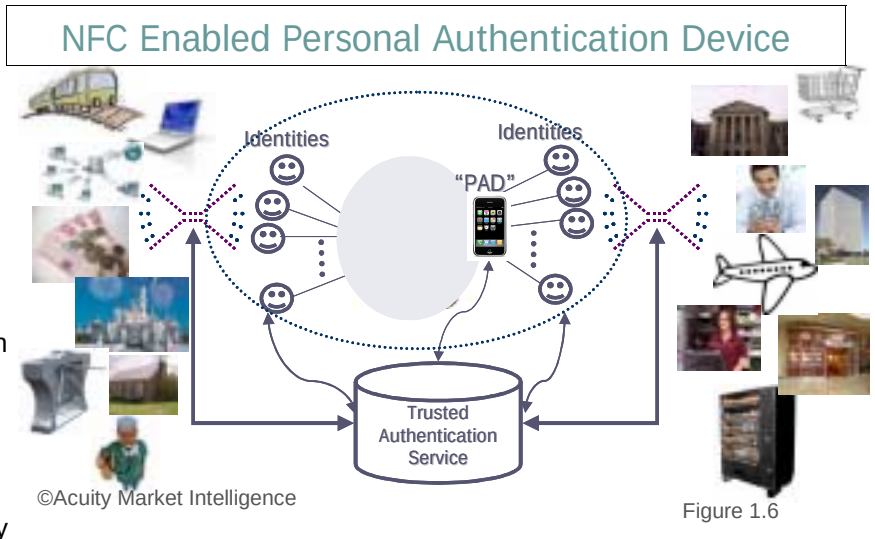


Figure 1.6

Is There Really a Revolution Coming to US Healthcare?

There has been some progress integrating biometrics in the Healthcare arena. Various individual practices, specialties within larger hospital or medical practices, and some large multi-location facilities are adopting biometrics for access to facilities, equipment, and drug cabinets and logical access to computers, networks, patient records, etc. However, widespread adoption remains elusive.

There is a strong possibility that major reform may finally break-open the US Healthcare market for significant biometrics adoption. The Obama administration has made conversion to electronic medical records a top priority in achieving improved healthcare outcomes and reducing costs. This transition would require massive efforts to convert paper records into electronic form and to create IT infrastructures to support secure, accurate, and reliable storage, management, and sharing of these records. This represents a significant opportunity to make the case that biometric authentication should be required for patients, medical practitioners, and administrators when accessing health or payment records, insurance information, etc.. The alternative would be a scenario that exists today for individual's personal and financial information, which is scattered across cyberspace in hundreds if not, thousands of locations with little security and no ownership control. This is an ideal opportunity to promote the use of biometrics as a lock to protect an individual's most personal information from unauthorized access.

In much the same way that the mobile phone based NFC transaction infrastructure may push financial service organization to incorporate biometrics to protect internal enterprise operations, biometric protection of electronic records may do the same for the Healthcare industry.

Biometric Blunders: The Pay By Touch and CLEAR Sagas

The failure of two high profile commercial biometric endeavors has cast a shadow on biometrics technology. The demise of Pay-by-Touch in November 2007 and the CLEAR Registered Traveler program in June 2009 sucked half a billion in investment capital out of the biometrics industry. Though both failures generated headlines, brought unwelcome attention to the biometrics industry, and seemed to shock the business community, the results were not surprising.

These businesses, like many less publicized commercial applications of biometrics succeed or fail based on the viability of the business mode, the solution, and the skills and expertise of the management team. These failures, like so many, had absolutely nothing to do with biometrics and everything to do with delusional management in one case and a delusional business model in the other.

Pay By Touch was the brainchild of John Rogers, an individual of questionable integrity, who was accused in a fraud lawsuit by a reputable former Pay By Touch Executive Vice President and investor of "concealing facts regarding an unsavory background". Rogers was able to raise more than $300 million of financing from sophisticated investors on charm and charisma, and structure the business in a way that gave him near total control. Investment firms included Plainfield Asset Management, Farallon Capital Management and Och-Ziff Capital Management and a number of wealthy individuals, including supermarket billionaire Ronald Burkle and the Gordon Getty Family Trust.

There was intrinsic value in the Pay By Touch business solution and they had a number of widely publicized successes signing deals with SuperValu to put its technology into Albertsons, Cub Foods, Jewel-Osco, and Farm Fresh. The unfortunate circumstances around the company's demise created the impression that biometrics had somehow failed or were not ready for consumer adoption. When in fact, the company had overcome significant obstacles and their solution was well received. The failure in this case had to do with poor management and inadequate vetting by investors who should have known better.

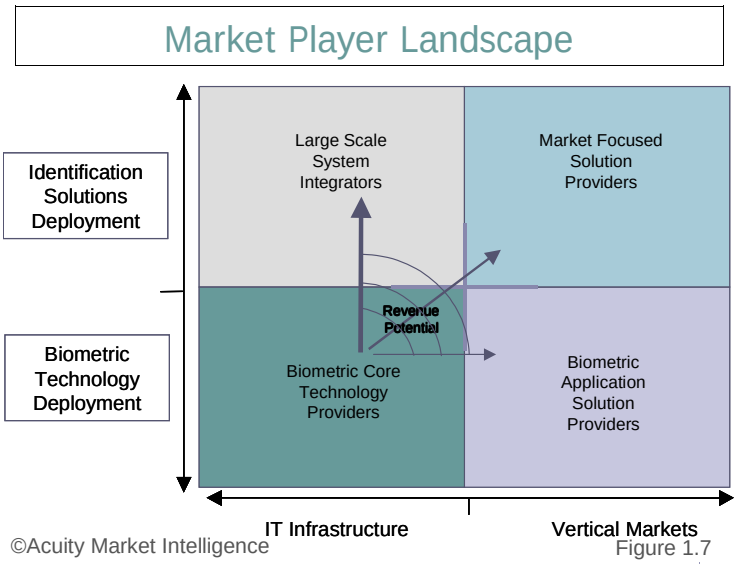
Verified Identity Pass's CLEAR program is on the other side of the spectrum. CLEAR demonstrates how a skilled and experienced management team can allow themselves to be convinced of the inevitability of a business model that has no hope of success. Stephen Brill was able to raise more than $100 million from another group of sophisticated investors—Spark Capital, Syncom Venture Partners, Lockheed Martin, GE Security, Baker Capital, and Lehman Brother—to fund a business that "napkin" math revealed was unsustainable. The cost of establishing and operating a biometric enrollment, credentialing, and authentication infrastructure for the number of available Registered Travelers could not justify the investment; let alone provide an ROI.

When CLEAR launched in 2005, travelers were charge $79 annually. By the time the company went bust, the annual fee had risen to $200. There were 250,000 enrolled in the program when it shut down. Even with the grand plans to extend the CLEAR card to provide access to concerts, sporting events, and other entertainment venues, the numbers just did not add up. Interestingly, the TSA immediately distanced themselves from the company with a spokesman stating "The CLEAR program was a market-driven, private sector venture, offered in partnership with airports and airlines in certain locations," In the end, the biometrics worked and had nothing to do with the program's failure. CLEAR was a hype-based opportunity that had far more sex appeal than any real chance of success.

Market Player Landscape

The biometrics industry has a history of domination by a highly fragmented core of technology vendors producing sensors, pattern recognition and matching algorithms, integrated biometric devices (sensors plus algorithms), and paltform level software. Until recently, the competitive focus has been limited to accuracy and performance. The dynamics of the market have changed of late with significant consolidation: the L-1 buying spree, Sagem's purchase of Motorola's AFIS business, even AuthenTec's purchase of Atrua Technologies. Players are staking their claims and securing and/or expanding market position by whatever means necessary or possible.

An analysis of individual market players is beyond the scope of this report. However, defining a framework for understating how players are positioned in the market landscape will provide insight into how they will be impacted by and how they can leverage evolving market dynamics and revenue opportunities. Figure 1.7 provides a high-level overview of the player landscape. As the diagram indicates, revenue potential increases as core technology providers move into solution and vertical market spaces. This reflects a good deal of the market consolidation as pure play biometrics companies try to increase opportunely and associated revenue potential.



©Acuity Market Intelligence Figure 1.7

Other factors impacted the competitive environment over the forecast period will be:

1) New market entrants from unrelated fields will contribute significantly to technology advancement for both capture and matching capabilities and performance.

2) A number of high profile specialty Biometric Application Solution Providers (BASPs) will emerge to address the expertise gap between core technology providers and large scale system integrators.

3) As biometrics march towards ubiquity, COTS (Commercial Off The Shelf) applications will enable many targeted vertical solution providers to integrate biometrics into their offerings without cultivating their own biometrics expertise.

Forecast Analysis

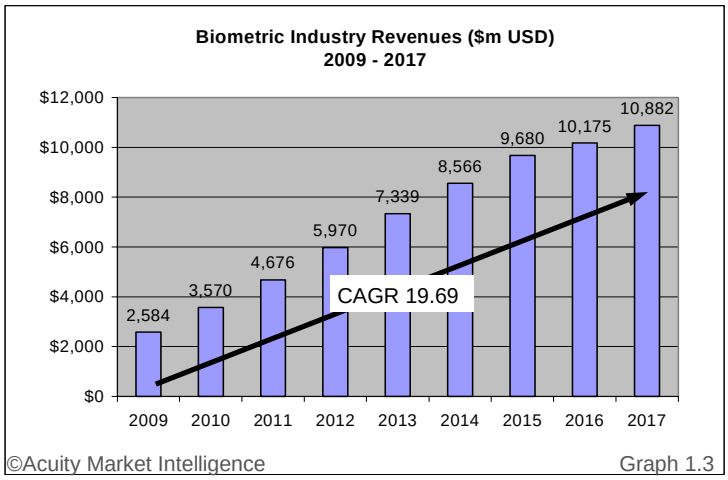
Over the next ten years the infrastructure to enable mainstream, ubiquitous biometric authentication will be developed. Biometrics will be a critical embedded component of the digital world, as it becomes a key enabler of trusted transaction control – data access and flow - for personal, commercial, and government use.

The market for biometrics core technology is poised for sustained growth with global revenues reaching nearly $11 billion annually by 2017 representing a CAGR of 19.69% over the forecast period (Graph 1.3). These figures are reasonably consistent with original projections made in 2007 (Graph 1.4). The 2009 forecast model was updated to reflect the most recently available data and account for current market dynamics—economic and political as well as technical. Slower growth than originally anticipated in the 2009 to 2012 timeframe due to the faltering economy is balanced out by slightly stronger growth in the 2012 to 2015 timeframe. The result—projections that reach roughly the same revenue levels by 2015 but with a lower overall anticipated CAGR of 20% from 2009 through 2017 rather than the higher CAGR of 30% from 2007 through 2015.

Commercial deployment revenues match Public Sector revenues by 2014 and then surpass Public Sector revenues by 2017 representing growth form nearly 41% to just over 55% of the total global market for biometrics core technology. The Public Sector revenue share declines form 59% to 45% over the period. The comparative CAGRs reflect this shift in market dominance as Public Sector grows as a respectable 16% while the Commercial marketplace grows at a much faster pace reaching 24% CAGR.

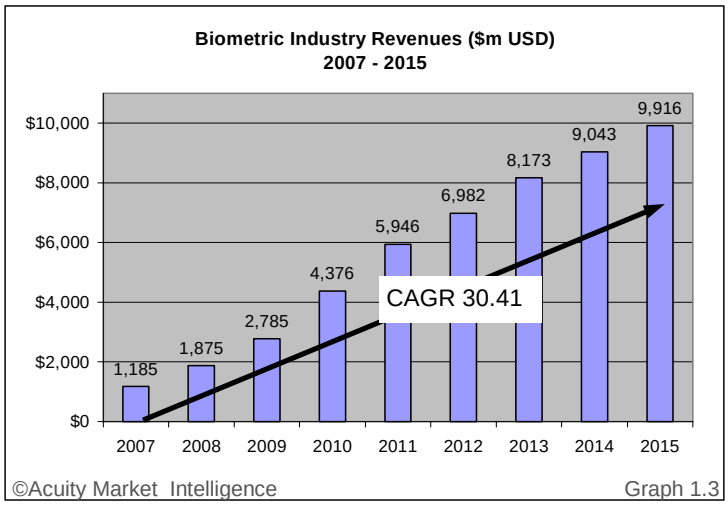
The sectors with the highest forecast period CAGRs within the Public Sector and Commercial arenas are eGovernment with 42% and Information Transactions at 50%. The other sectors CAGRs are as follows: eBorders 10%, eID 12%, Enterprise Security 12%, and Financial Transactions 37%.

Biometrics Industry Revenues 2009—2017



©Acuity Market Intelligence Graph 1.3

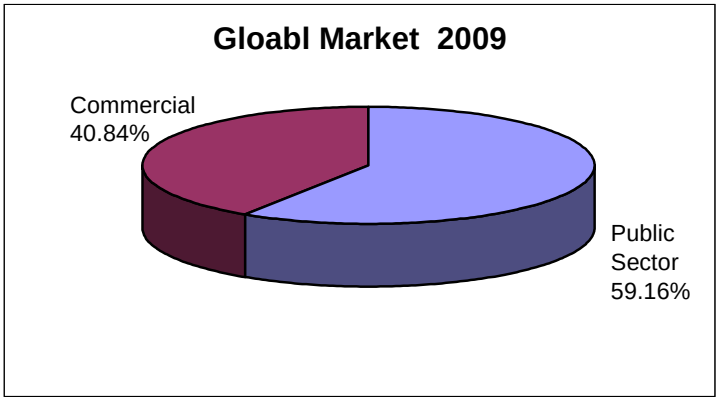
Biometrics Industry Revenues 2007—2015



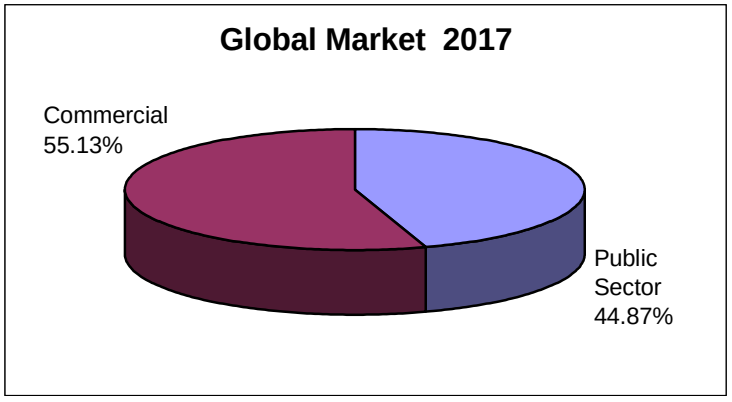
©Acuity Market Intelligence Graph 1.3

Revenue growth rates vary significantly across regions. The Central and South American region will experience the highest CAGR over the forecast period of 39.46% while growing form nearly 4% to nearly 13% of total global revenues. Over-

Biometrics Industry Market Share: Public Sector vs. Commercial 2009 and 2017

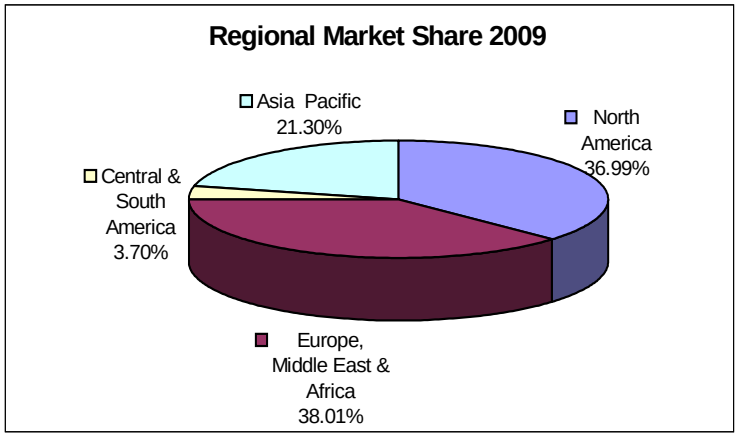


©Acuity Market Intelligence Chart 1.14



©Acuity Market Intelligence Chart 1.15

Market Share by Region 2009 and 2017



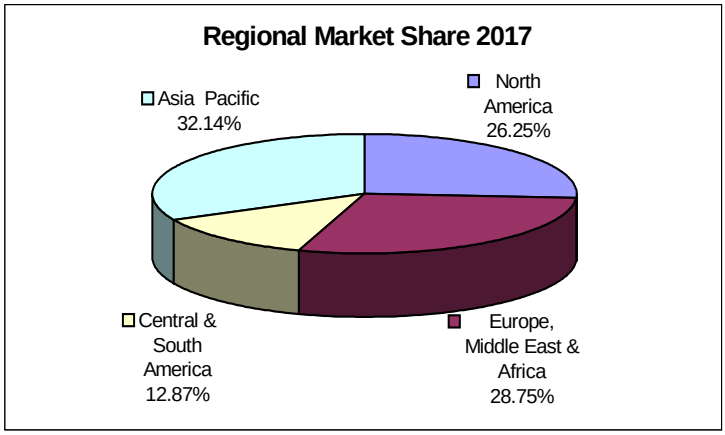


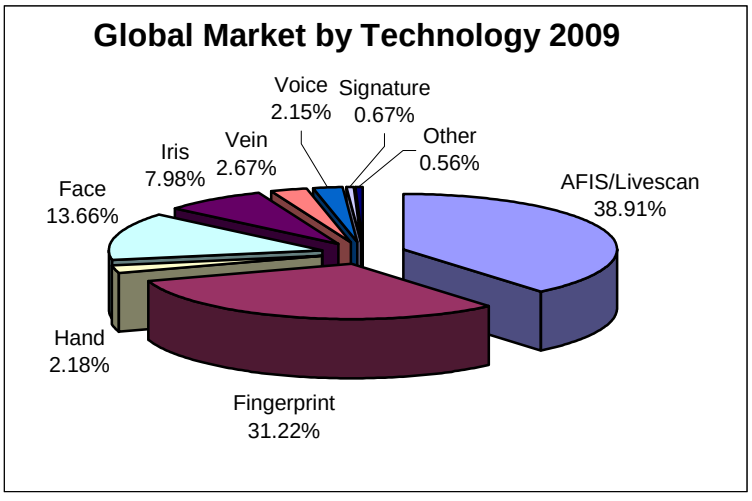
 Chart 1.16 Chart 1.17

all market dominance will shift from Europe (and the greater EMEA region) and the US (and the greater North America region) to Asia (and the greater Asia Pacific region). North America and EMEA's percentages of total global revenues will decrease over the forecast period form 37% to 26% and 38% to 29% respectively with associated modest CAGRs of 15% and 16%. By 2017, the Asia Pacific Region will generate the greatest percent of revenues for the biometrics industry with more than 32% of global revenues growing at a CAGR of 26%.

The dominance of AFIS/Livescan and Fingerprint continues thorough the forecast period though the overall percent of total revenue for these two technology categories drops form a blistering 79% in 2009 to a more modest 52% in 2017. The prolonged dominance of finger-based biometrics rests on the legacy of finger-based identification. Identity Services including enrollment and credentialing will continue to represent the lion's share of biometric revenues over the forecast period (Charts 1.17 and 1.18, Page 28) as the digital identity infrastructure is established. This will continue to mean reliance on Fingerprint to establish/confirm baseline identity until other biometrics such as Iris and Face have made significant inroads.

By 2017, Iris and Face recognition will have established significant market penetration together accounting for more than 33% of global biometric revenues. This shift will continue beyond the forecast period as 1) these biometrics become as commonplace in the identity infrastructure as fingerprint records are today, 2) the advantages of biometrics that do not require active user participation for many physical and logical access control applications– passive iris and face capture—are understood and accepted, 3) and as the price/performance of Iris and Face recognition make these solutions extremely cost effective.

Market Share by Technology 2009 and 2017



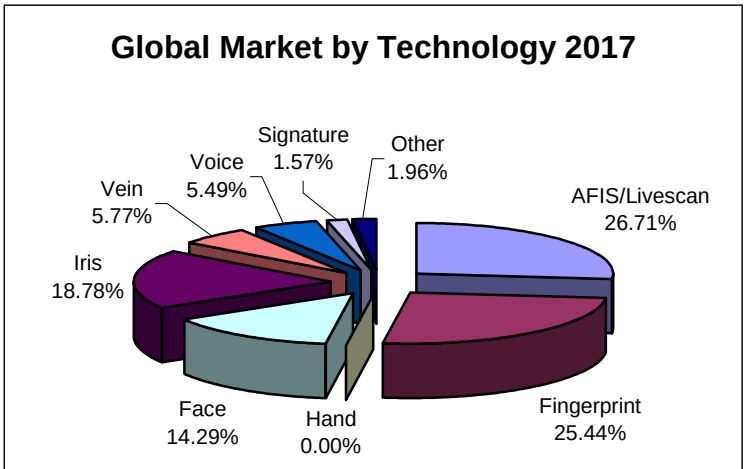


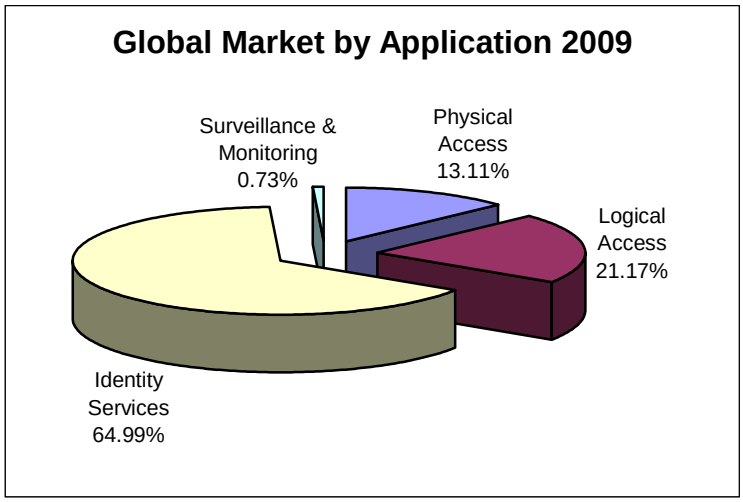
 Chart 1.18 Chart 1.10

Vein, Voice, and Signature will experience modest growth from 3% to 6%, 2% to 5%, and 0.7% to 1.6% respectively, Hand Recognition will continue to be used but will experience a slow, steady decline from 2% of the market to 0% as it is replaced by other biometric modalities over the forecast period. Finger and Vein will benefit where a similar interface is desired and Face or Iris will benefit where a modality shift is acceptable and a more passive approach is preferred .

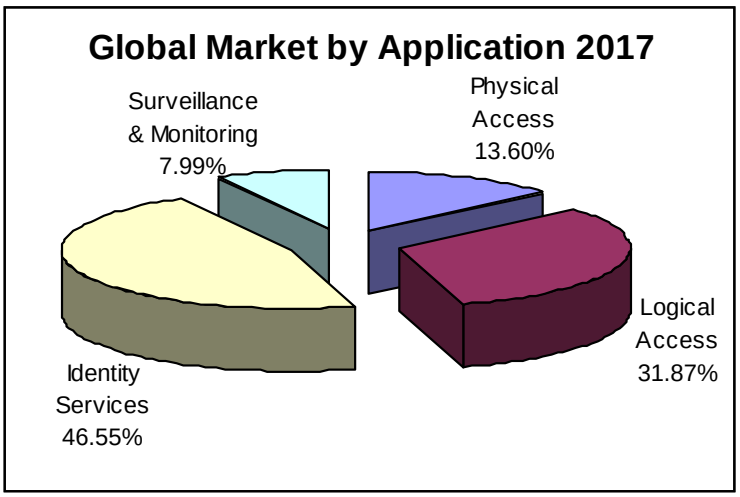
Transactions will ultimately provide the majority of industry revenue. Information and Financial Transactions for Commercial applications by 2012 and eGoverment for Public Sector applications by 2017. By 2017 Information Transactions will represent 12.21% of the global market, Financial Services 18.22% of the global market, and eGovernment will represent 14.23% of the global market.

The percent of revenue from Identity Services declines over the forecast period but only from 65% to 47%. Surveillance and Monitoring posts the strongest percentage gain growing from less than 1% to nearly 8% of total market revenue representing a CAGR over the forecast period of a startling 60.99%. Physical Access control as a percent of total revenues will essentially remain flat starting at 13% and ending up at 14%. Logical Access will grow modestly from 21% to 31% over the same period.

Market Share by Application 2009 and 2017



©Acuity Market Intelligence Chart 1.20



©Acuity Market Intelligence Chart 1.21

Future for Key Technologies

Mainstream ubiquity will occur as capture devices for most routine applications become low-cost, reliable commodities available in multiple form factors embedded in everything from PDAs, PCs, POS terminals, and ATMS to vehicles, security gates and appliances. As with most technology, 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? 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 process has already begun as finger sensors are routinely integrated into laptop PCs, and mobile phones and cameras on these devices are being used for Face, Iris recognition, and even image based Finger recognition.

In the more distant future—beyond the timeframe of this report—the actual distinctions between biometrics modalities will blur, massive convergence will take hold, and individual biometric categories will disappear. This is more than just one technology winning out over another but an actual merging and morphing of the capture devices and the algorithms. Ultimately, capture devices and algorithms will be mostly indifferent, regardless of scale, to the nature of the type of pattern-data being captured.

Capabilities and Limitations Impacting Ubiquity of Biometric Modalities

Most biometrics will continue to improve in performance and accuracy until their maximum capability has been achieved. Others, such as hand recognition, may simply fade away as their price/performance and usability as compared to other modalities no longer makes them viable. Regardless, over time the selection of biometric modalities will be based on the requirements and constrains of any given solution rather than specific concerns about the performance of a given technology.

AFIS/Livescan

AFIS has a unique place in the biometrics arena in that it is an established component of legacy identification especially for the criminal justice system. Even as other biometrics prove more accurate for identification—Iris today, others tomorrow—AFIS's legacy in the form of tens of millions of entries in databases across the globe provides staying power regardless of advancements in identification technology. AFIS will continue to be the standard for background checks and criminal investigations for the foreseeable future. And, as AFIS moves to flats that incorporate the entire palm prints and approaches the real-time response levels of other biometrics, it has the potential to displace these technologies for a broad range of identification and authentication applications. The most lucrative development for AFIS over the next three to five years will likely be it's market expansion as low-cost Livescan devices become available and dramatically increase overall market potential.

Finger

Finger scan capabilities will become ubiquitous in mobile personal devices within five years. The question over the longer timeframe is will Finger scanning remain a multiple technology solution—silicon, optical, ultrasound, vein—or will optical Finger scans be one of several image based biometrics (e.g. Face, Iris) that can be captured by a single "camera" embedded in a personal device. One significant advancement that must occur to make Finger scanning viable for applications beyond personal devices is true interoperability. This has been demonstrated today with minutia-based solutions but significant work remains to be done. Another possible evolution is a touchless image based Finger scan for deployments where user initiated action is desired.

Face

Facial recognition has tremendous potential across application domains for targeted purposes. 3D Face will become the standard for non-watchlist applications and work will continue to convert relatively poor image quality 2D existing facial database to higher quality 3D databases. Now that the initial post 9/11 blunders to rush Face recognition technology prematurely from the laboratory into the marketplace have faded and significant work has been completed to improve accuracy and performance, it is possible to identity realistic applications for the technology. It is highly unlikely that facial recognition will compete with iris for identification, but within appropriate contexts Face recognition is a powerful and cost effective tool. The two will end up complementary modalities used together to effectively screen and then identify individuals. Over the next five years, Face will continue to be deployed well to solve specific problems, overcome its previous foibles, and earn a solid position in the overall biometric marketplace. And it will, of course, continue to be used to search databases for applications like drivers' licenses, passports, and visas, as well as digital surveillance video.

Iris

Iris recognition is poised for significant growth over the next ten to fifteen years. Innovation that will enhance image capture capabilities e.g. subject finding capture at medium distances (one to four meters), long distance capture (ten meters and greater), and resolution of low and bright light issues will make iris a biometric of choice for many applications. In addition high-quality Iris image capture devices will become inexpensive, available in many form factors, and easily embedded

in everything from mobile phones and computers to POS Terminals and ATMs. Iris will become a biometric of choice particularly for public access applications where contactless solutions are preferred and where a "do nothing" biometric (i.e. user acquiring) is essential to meeting speed and throughput requirements. The obstacles to widespread use of Iris recognition that exist today will simply be irrelevant by 201 and beyond.

Hand

Hand Recognition has a solid history of providing unique reliability and stability at a time when other biometrics failed to deliver on their promises. This technology has been primarily used for solving access control and time and attendance problems. However, its ongoing usefulness is limited. Hand Recognition will continue to be used but will experience a slow, steady decline until it has essentially been replaced by other more effective, reliable, user-friendly, and accurate modalities such as Finger and Vein where a similar interface is desired and Face or Iris where a modality shift is acceptable and a 'do-nothing" approach is preferred .

Vein

Vein scan devices have made significant inroads in Asia and should continue to thrive as they spread to North America and Europe. Vein offers a strong alternative to finger for government and commercial applications in situations where active user involvement is desired, where a contactless approach is preferred, and where Finger related biometrics have strong criminal implications. Currently, Vein recognition comes in three form factors; a contact-based finger technology, a - contactless hand scanner, and a contactless back-of-the-hand scanner. Given the hygienic and operational advantages of a contactless approach—no transmission of germs, less wear and tear on the device—it is likely that the contactless technology will dominate and the contact based Finger technology will evolve to a contactless technology. There have been issues associated with the "contactless" options, as some kind of guide has been required. Recently, advances in high-speed capture have allowed for capture while in motion which should eventually eliminate the necessity for a guide.

Voice

The great promise of Voice recognition has never been realized. But that will change over the next few years. As channel conflicts are resolved, Voice is the natural choice for authentication in an environment where the platform—land and mobile phones—already exists. As Public Sector and Commercial information and financial transactions become routine, Voice recognition will increase in stature. In many instances Voice may be used as an initial verification in combination with additional biometrics for more secure transactions. The infrastructure that fully enables Secure Mobility will drive Voice biometrics to ubiquity. While Voice's market share will remain relatively small, overall industry growth will drive significant revenue growth for Voice recognition.

Signature

Dynamic Signature recognition has been a bit of a sleeper biometrics. Though the use of signature recognition has been limited, it has proven quite effective where it has been deployed. Signature recognition will become more interesting as legal frameworks for digital signatures catch up with technology capabilities. There is such a strong historical correlation between a written signature and the force of contracts that it seems inevitable that most binding signatures will be completed electronically on devices that capture digital images of signatures as well as biometrics. This biometric will not be used as a means of identifying an individual per se but rather as a component of a trusted electronic audit trail. Ultimately, this type of signature will replace the handwritten signature as the gold standard for legal contracts.

Keystroke

Keystroke Dynamics has not been considered a serious biometric contender. However, recent advancements have made it a viable alternative for logical access. Keystroke has a unique collection of characteristics, it is a software only solution, it relies on familiar keyboard-based passwords, it can be implemented without user knowledge, and it can be used as a surveillance technology for logical access. Even in environments where other biometric modalities are used for initial logical access authorization, Keystroke can be used to confirm the appropriate individual is interacting with the computer without additional surveillance technology.

Other Biometric Modalities

There are several other biometrics modalities currently being researched for possible product introduction.

Gait recognition may prove to be one of the most promising new biometrics. This is particularly true for surveillance applications including screening of individuals as they approach high-security civilian or military facilities or potential targets for theft or terrorism. There is a high level of interest within the intelligence community in gait recognition for applications where identification at a distance is required but the Face or Iris may not be visible.

.

Odor has been proposed as a biometric and while it may be true that individuals have a unique odor, building odor detecting technologies may depend on levels of bioengineering that will not available for some time. Perfecting "bomb sniffing" devices is still a

serious challenge (dogs are still better at it than machines) and this sort of biometric apparatus is magnitudes of complexity greater. *Ear* recognition has always been considered a somewhat fanciful biometric. Yet, if image capture, recognition, and matching algorithms advance as expected for Face and Iris, the ear may be just as reasonable a subject for analysis as any other physical attribute.

Retina scanning has essentially dropped out of the market. In recent years, several companies have tried to resuscitate retina as a highly accurate, cost effective biometric option. The legacy of invasiveness will have to be overcome as well as clear value added positioning over Iris. This may be reasonable for very high security applications, in strictly controlled environments where short distance capture is preferred.

Recent experimentation with *Brain Waves or* patterns has been promising. However, the equipment is cumbersome, expensive, and user invasive. Though this was true of many mainstream biometrics in their early stages as well.

Future For Key Technologies

Technology	Legacy	Today	Future
AFIS/ Livescan	Established Law Enforcement staple for 1:n searching. Approaching real-time performance	Continues to be a Law Enforcement focused technology though grown in use for civil and commercial background checks. 3 major AFIS vendors, 2 major livescan vendors with extreme barriers to entry.	Full hand slaps including palm print become standard. Real-time performance achieved for very large databases. Potential for integrating with vein. Low end systems drive market expansion
Finger	Multiple technologies – optical, silicon, ultra sound, (and vein see below), Many players trying to establish themselves as the technology of choice.	Widely used for range of applications – government, commercial, consumer. Making enterprise inroads. Shipping on close to 20% of laptops. Phone use in Asia significant. Over 100M sensors shipped worldwide. Minutia based interoperability is established. Market remains fragmented.	Good future for minutia based because of interoperability. Likely integrated with other technologies for more critical applications. Question long term viability of silicon because of optical image capabilities. Touchless image based alternative is likely. Ubiquitous in personal devices.
Face	Marginal performance for real time ID, Lots of bad PR. Established for database search e.g. drivers license, passport. Significant environmental issues.	High potential yet limited success – except image database and digital video search . Significant capability/performance fixes for 2D over past few years. 3D has also proven effective. Proven deployments commercial and government. Verification speed does not impact normal workflow. Environmental issues are being overcome.	Future is 3D especially 3D at a distance., Image capture on personal handheld devices. Significant potential for surveillance and cooperative touchless, user acquiring solutions. Significant improvements for image database and digital video search.
Iris	Accurate but expensive. Non-functional outdoors. Limited usefulness except for high-end applications.	Only technology for real-time large scale 1:n searching. Enrollment issues – positioning. Environmental issues being overcome Application with 80 million enrolled though database is not consolidated and duplicate searching has not begun. Widespread us in the Middle East. Price/ performance curves dropping.	Low-cost devices available as stand alone or embedded. Large real-time databases (100M+). Outdoor and other lighting problems solved enabling host of contactless, touchless applications especially kiosk based – financial services, border control, physical access, time and attendance.
Hand	Widely deployed for access control and time and attendance for government, commercial and consumer. Adequate for 1:1 verification for high security (nuclear power plants)	Considered somewhat limited but effective. Integrated with 3D face to improve capacities and appeal.	Use will decline . Replaced by other technologies. Vein and finger where similar user participation or iris or face where passive approach is preferred.
Signature	Significant potential but underutilized. Legal acceptance of electronic signatures an issue.	Still limited traction but looming large potential . Legal/structural basis for electronic signatures lacking .	Routine for contracts, payments, legal documents. Proliferates with widespread use of touch screen notebooks/PDAs.
Voice	Positive user experience but plagued with significant channel issues.	Channel issues being resolved. Uptake imminent especially in customer service arenas. Recent wins in Europe and Australia.	Widespread use by consumers especially in financial services and other phone based information transactions.
Vein	Not taken seriously as a challenge to finger based biometrics	Finger, palm, and back-of-the-hand based technologies. Palm is contactless. Finger and palm battling for Japan's ATMs—begrudging acceptance by customers due to cooperation issues among banks . Expanding in the US and EU markets. Recent move for cross enrolment.	Contactless has strong appeal from sanitation perspective (plays well in Asia). Palm based does not have law enforcement connotation like fingers. Strong replacement for hand.
Other	Lots of research and development but most suffer form a perception of quirkiness.	A number of serious researchers and funded start-ups are committed to developing breakthrough biometric technology.	Winners will be based on accuracy and speed, social acceptability, and price/ performance.

Chart 1.22

Impact and Role of Multimodal Solutions
It is highly likely that as biometrics become more commonplace the use of multimodal or fused biometrics will become routine. There are any number of scenarios that might require the use of multiple biometrics.

- High-security situations or high-value transactions require more than one biometric authentication.
- Multiple biometrics are used within a single organization for various access control applications: Face recognition for entry in to a building, Iris recognition for entry into a secure area, Keystroke for logical access to a network.
- One biometric is used to evaluate subjects against a watchlist while a second is used to perform a one-to-one authentication.
- There will always be some individuals who for any number of reasons may not be able to enroll or verify with a particular biometric modality—health conditions, cultural issues, racial characteristics, disabilities, or personal idiosyncrasies. At some point the investment in research and development to broaden the performance of biometrics to include every individual under every circumstance becomes cost prohibitive. All large-scale identification solutions will have to include one or more fallback biometrics.

The need for multiple biometrics will impact the marketplace in two fundamental ways.

- Biometrically enabled solutions will be more complex requiring expertise across a range of modalities. This will create a market dynamic that rewards relationship building across the spectrum of biometric core technology developers and solution providers. Even for those producing what would appear to be directly competitive products and services, forging alliances and strategic partnerships that promote co-opetition will be far more beneficial than strict competitive positioning.

- The role of Biometrics Application Solution Providers (BASPs) will grow substantially. Core technology providers will simply not have the requisite knowledge to understand the complexity of customer requirements. System Integrators will be focused on the larger issues of identity centric IT infrastructures and vertical market solutions providers will not have the knowledge to translate specific customer requirements into biometrics capabilities. This class of companies should be focused on evaluating technology, imposing/enforcing standards, ensuring adequate investment in human-factors, and generally supporting innovative research and development efforts across the industry. They should leverage their market position to act as gatekeepers ensuring the quality of available biometrics technology and the successful deployment of this biometrically enabled solutions.

Impact of Related Technology Development
The ongoing development of ancillary hardware and software technologies such as smart cards, mobile phones and other personal devices, cryptography, identity management, and various risk analysis tools are all essential components of the broad based identity-centric IT infrastructure required for biometrics to thrive. In turn, biometrics is an essential component of the authentication capability required for this infrastructure to be a secure, trusted operating environment. All of these technologies are therefore integrally related and dependent on each other for success and market growth and must be considered in the context of building this overarching infrastructure.

This is particularly true of Near Field Communications (NFC) enabled mobile phones. Over the past few years successful pilots and small-scale programs have been initiated on every continent. From transportation and entertainment ticket purchases to POS applications and integrated facility access and cafeteria purchases, the results have consistently proven a strong willingness on the part of users to adopt this technology and an extremely high-level of satisfaction. As NFC becomes a mobile phone (and PDA) standard, the volume and breadth of information and financial transactions will grow exponentially. This complex, high-volume transaction environment will be subject to all manner of fraud, theft, and compromise. Biometrics will play an important role in bringing this transaction infrastructure under control by providing enhanced authentication as required based on the vale and risk of a given transaction.

Finally, the biometrics industry will benefit directly from the entry of sophisticated, well-funded market players with technological expertise in areas such as high resolution image capture, large-scale data management, and high-speed processing, and pattern recognition and matching algorithms. These types of market entrants have already begun to elevate biometrics technological capabilities by introducing tools and techniques that have been successfully applied in various fields such as robotics, astronomy, quantum physics, and intelligent video where significant obstacles related to high-resolution and volume data capture and processing have been overcome. This will contribute significantly to generating the level of requisite knowledge necessary for the industry to leverage key opportunities and experience sustained growth.

Analysis Conclusions

The fundamental dynamics of the biometrics marketplace will change significantly through 2020. Over the next ten to fifteen years the infrastructure to enable mainstream, ubiquitous biometric authentication will be developed. This infrastructure will both enable and be driven by true mass public deployment of biometrics for personal, commercial, and government applications representing the emergence of a new era of biometrics. This transformation impacts all aspects of the biometrics industry well beyond technology capabilities and includes market requirements, solutions, and business models.

As biometrics become a critical embedded component of the digital world, it will be a key enabler of trusted transaction control – data access and flow—for all IT systems. This secure transaction capability will ultimately define the genuine opportunity for revenue associated with deployment of biometric technologies. The technology itself will, in many respects, become inconsequential as the applications it delivers become essential components of twenty-first century life

Market Transformation Components

The key components of this market transformation can be divided into four categories: Market Requirements, Technology Capabilities, Total Solutions, and Business Models.

Transformation Components

Market Requirements	Technology Capabilities
Embedded Low Cost/High Performance Built in Extensible Security No/Low user Impact Hygienic, Non Invasive 100% Solution	Flexible Form Factors Distance Capture Subject Finding Surveillance Environment Tolerant
Total Solutions	**Business Models**
Operating Environment Crafted Human Factors Considerations Ease of Enrollment Legal, Regulatory Privacy/Civil Liberty Protection	Transactions • Information & Financial • Personal, Commercial, & eGovernment Service Based

©Acuity Market Intelligence Figure 1.8

Market Requirements

A confluence of factors including the emerging critical role of digital identity and Cloud Computing in IT, population mobility and decentralization or workforces, demand for eGovernment services, near ubiquitous reliance on digital transactions, and the inevitability of broadband access everywhere will require a level of authentication available only through the use of biometrics. This will drive a host of requirements from increasingly more sophisticated customers and end-users that want solutions that easily integrate with their existing IT infrastructure and security policies, processes, and technologies.

Technology Capabilities

Many of the fundamental issues that plague existing biometrics technologies will be resolved and performance will no longer be a limiting factor. There will be a shake-out as more subtle refinement of individual modalities are matched to the specialized requirements of targeted applications. Convergence will also play a role enabling core image capture technology to be applied in various form factors and configurations for image-based biometrics. The market entry of sophisticated players from complementary technology arenas such as high resolution image capture, large scale data management and high speed processing, and pattern recognition and matching algorithms will help facilitate this process creating operating environment tolerant biometric technologies.

Total Solutions

The operating environment will define the solution as less emphasis is placed on idealized laboratory-based technology performance and more emphasis is placed on the actual human experience. Contactless, user-acquiring biometrics will become the preferred method of authentication for public deployments for two primary reasons. Capture technology will become increasingly more sophisticated operating accurately regardless of environmental conditions. Biometric authentication that does not require the user to “do anything” e.g. position themselves in relation to or have physical contact with a reader, will prove more acceptable and more convenient for users. User initiated and contact-based solutions will increasingly be targeted towards personal access to personal data and communication devices, consumer electronics, and home environments.

Business Models

As with many technologies that achieve ubiquity, prices drop, margins plummet, and revenue opportunities move towards service or transaction based models. Biometrics will be no exception. In the long run, companies that provide value-added services or facilitate transactions will be the most powerful and lucrative. Solutions providers in this realm will own the customer relationships and drive technology development establishing and maintaining dominant market position.

Making the Transition

How will biometrics make this transition from deployment within limited closed-loop solutions to an enabler of a fully interactive, transaction based, global authentication network? Through an incremental and iterative process where knowledge is acquired in nonlinear phases and learnings from each phase lay the groundwork for subsequent phases. This will require vision, commitment, strategic flexibility, and a great deal of patience. The longed for single, monumental event that will propel biometrics to the forefront of advanced technology development is, quite honestly, a pipe-dream.

However, consistent progress will be made. The eight Meta Trends will demand the evolution of an identity centric IT foundation. This has already begun to a limited extent and will increase dramatically through 2020. This role of biometrics in this IT revolution will be driven by the Application Solution Meta Drivers which in turn will require the development of a trusted authentication infrastructure based on the Technology Evolution Meta Drivers. This will create the dynamics that promote sustained, *not exponential*, growth of the biometrics marketplace through 2020.

The most significant, long-term opportunities for biometrics will revolve around problem solving at this level. As with all emerging technology markets, the more successful and mainstream the technology is, the less of a focal point it becomes. Biometrics true success will be unquestionable when there is no mention of biometrics. When biometric authentication is taken for granted and seems as innocuous as a keyboard, a mobile phone, or a cardkey Is today.

The Future

This report is by no means a comprehensive view of every aspect of biometrics market development from now through 2020. It does, however, provide an important context for those developing technologies and solutions or evaluating proposed deployments.

This is a tenuous time for the biometrics industry. Though all indications suggest that the breakthrough has begun, the industry must now truly deliver. To be trite but accurate—failure is not an option. The real test for the industry is twofold. Can the bridge be built from relatively small-scale deployments to full blown functional solutions operating at performance levels and within error constraints that build confidence In the capacities of the technology? And, can these large-scale systems be developed, implemented, and monitored in such a way that privacy and civil liberties concerns are addressed to satisfactory levels from both a public perspective and that of the most aggressive privacy and civil liberties organizations that have offered significant resistance to the use of biometrics?

Should one or more significant large-scale projects prove to be seriously flawed from either a technological or societal perspective, the possibly of market implosion rather than expansion is quite real. Those with a vested interest in the development of this industry—vendors, integrators, investors, and end users—must focus their efforts on ensuring that biometrically enabled solutions are designed, developed, and implemented for success.