NEC PUBLIC SAFETY WHITEPAPER

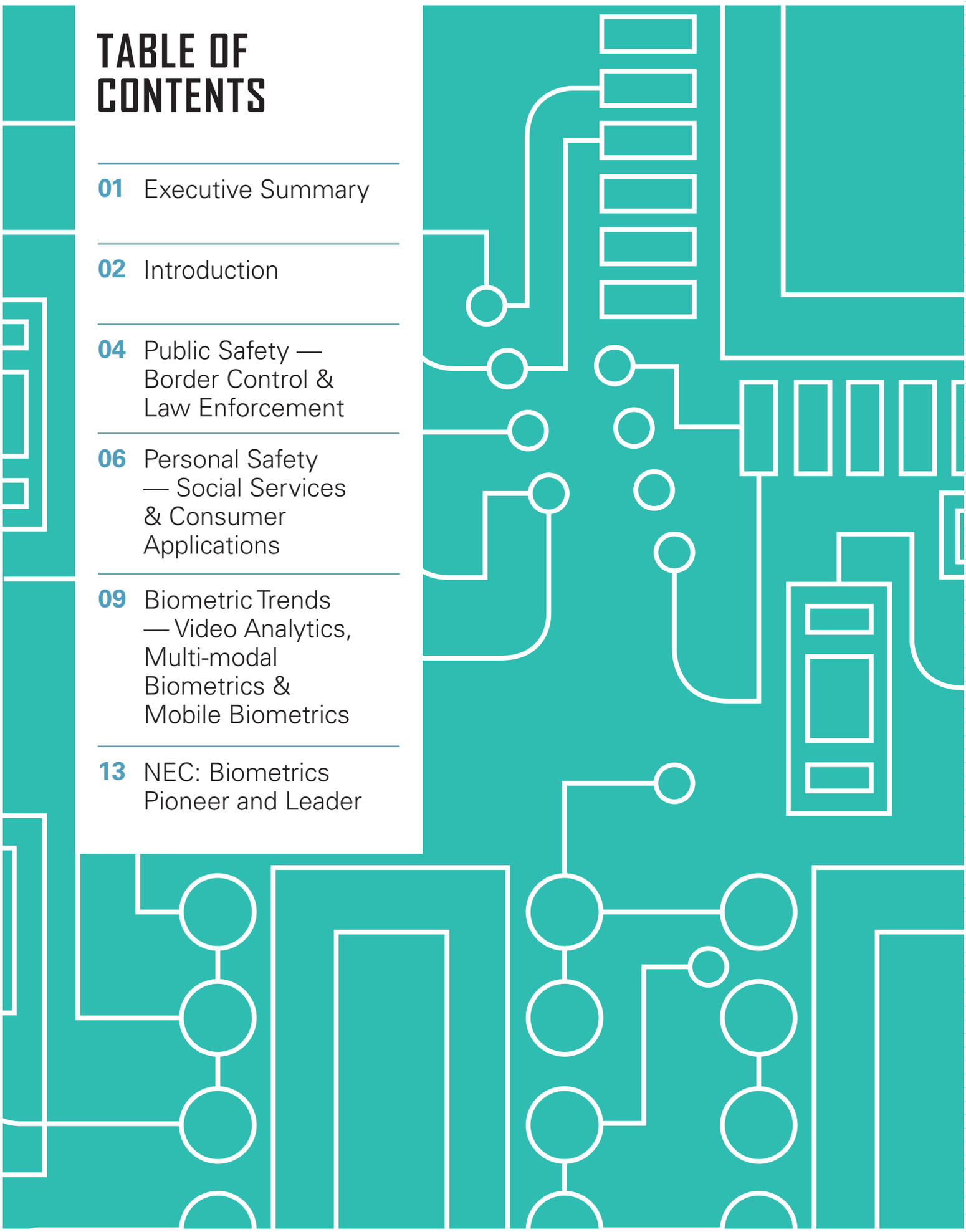
\Orchestrating a brighter world

NEC

The state of the art in public safety

BIOMETRICS

TABLE OF CONTENTS



EXECUTIVE SUMMARY

Biometric technologies use biological features such as fingerprints, veins, faces and irises to identify individuals. They greatly improve the accuracy and reliability of identification and verification systems by taking out the element of human error.

In the area of **public safety**, biometric technologies in the form of fingerprinting, iris and facial recognition have made a significant contribution to border control and law enforcement.

Biometrics has also played an important role in ensuring **personal security**, both in terms of facilitating the provision of social services at the national level as well as protecting personal devices and accounts from crackers.

Exciting new trends in biometrics include the rise of **multi-modal biometrics** which could be used to enhance public safety, user experience and protect personal privacy. The combination of multiple biometric parameters makes the technology much more robust against challenges.

Lastly, **mobile biometrics** and **biometrics on the move** are two other developments to look out for. The integration of biometrics technologies with mobile devices will reduce infrastructure costs, while the ease and convenience of non-invasive capture enabled by stand off biometrics will spur its widespread adoption.

INTRODUCTION

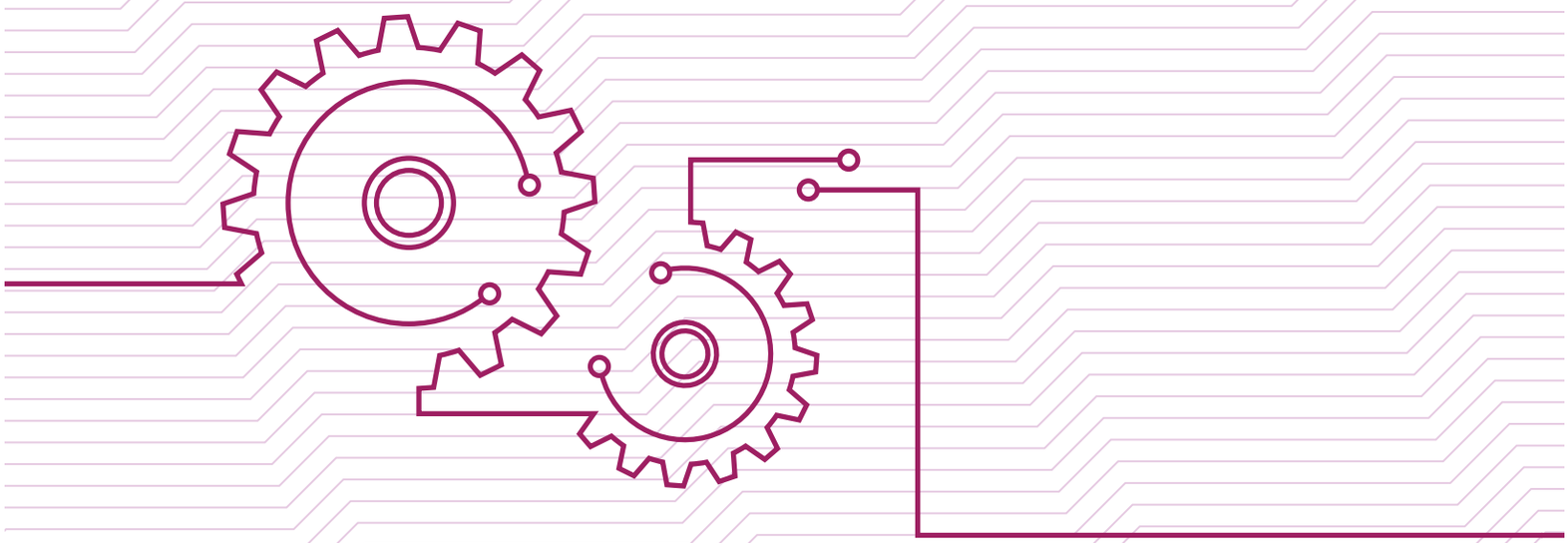
BIOMETRICS: FROM BASIC TO ADVANCED TECHNOLOGY

If you think about it, biometrics technologies have actually been in use since the dawn of human civilization. After all, biometrics can be thought of simply as the identification of individuals using physiological or behavioral traits. Whether it be a student's distinctive facial feature recognized by a teacher taking the class' attendance, your signature on a check which allows money to be withdrawn from your bank account or your profile picture on Facebook which helps your friends find you; "basic" biometrics are firmly a part of everyday life.

Despite our heavy reliance on them, our current methods of identification and authentication are far from ideal. A study of Australian passport officers published in the journal *PLoS ONE* showed that the officers missed one out of every seven fake passport photos, and that trained staff were no more accurate than student volunteers[i]. This high error rate of 14 percent is particularly worrying in the context of modern day air travel, where hundreds of thousands of people pass through airports each day. It is perhaps not altogether surprising then, that two out of the 227 people on-board the missing flight MH370 were traveling on false identities.

The main weakness of basic biometrics is the high rate of human error. A new haircut can dramatically alter the way a person looks and signatures can be forged, for example. Non-biometric technologies have sought to reduce this subjectivity by relying instead on passwords or physical tokens to establish identity. However, as anyone who has forgotten their password or left their staff card at home knows, these methods can sometimes lead to frustrating situations.

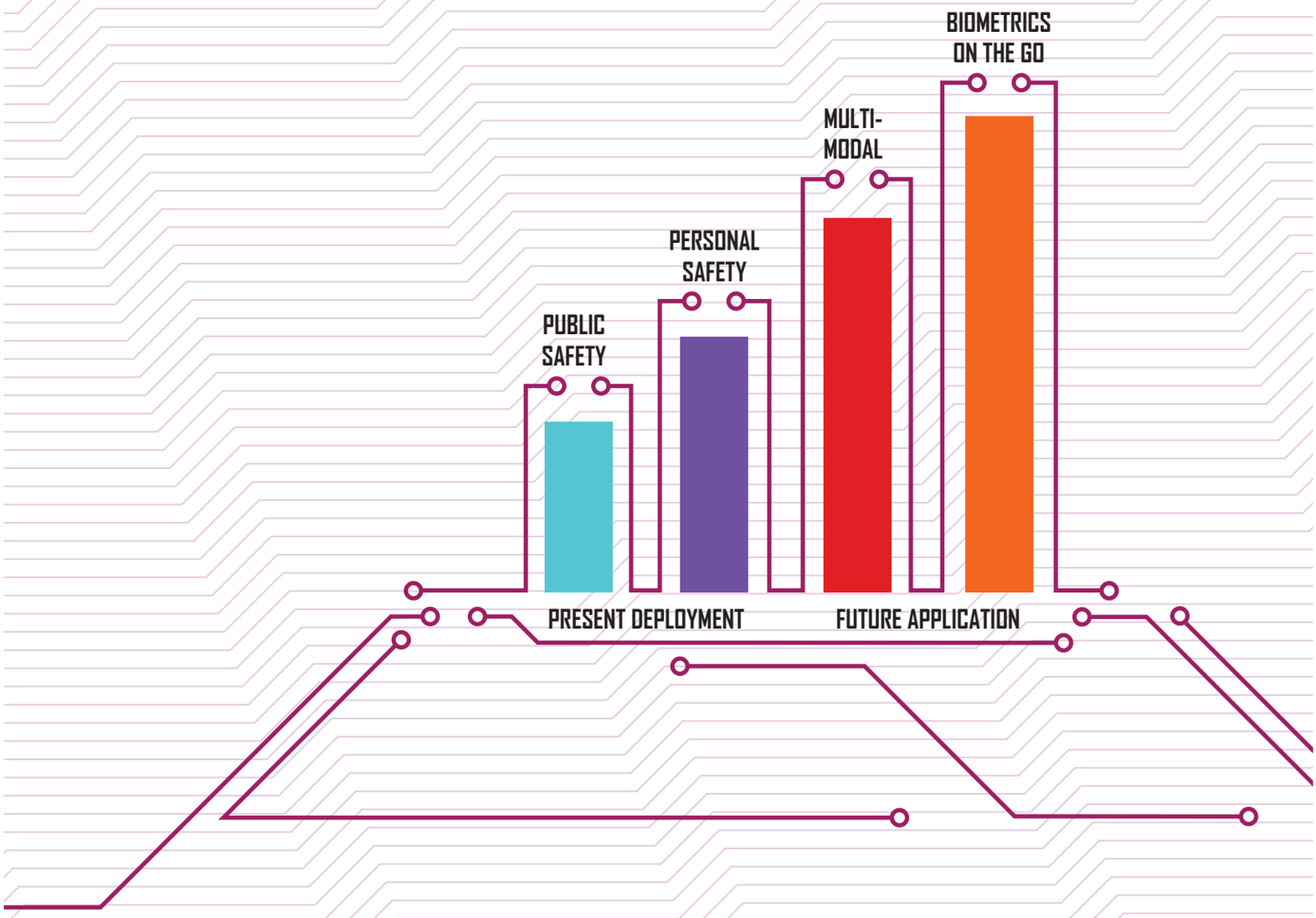
Rather than replace basic biometrics with non-biometric technologies, advanced biometrics make the identification of unique physiological or behavioral traits much more accurate and reliable. After more than two decades of research, biometric technologies have matured and advanced to the point where they are able to achieve sophisticated functions and outperform human abilities. A recent 2013 test by the U.S. National Institute of Standards and Technology (NIST) reports that a person can be picked out from 160,000 mug shots, with an error rate of only as low as 3.1% at very high speeds of 10,000 searches per second.



BIOMETRIC CAPABILITIES – PRESENT AND FUTURE

Ultimately, what biometrics enables is automated access control and identity management; replacing human, error-prone processes with technology. There are two main types of biometrics: i) *identification* or *recognition*, or one-to-many, where the aim is to match a single individual to multiple entries in a biometric database, or ii) *verification* or *authentication*, also known as one-to-one, where the aim is to prove that the person is really who one claims to be.

This white paper will look at how biometric technologies are currently in use, as well as future applications that are being developed. In the first two sections, examples of biometrics in public and personal safety are discussed, areas where biometrics has already made a substantial impact. The next two sections will cover exciting new developments in biometric technologies, namely, the rise of multi-modal biometrics and its potential to improve privacy, followed by the promise of integrating mobile devices with biometrics.



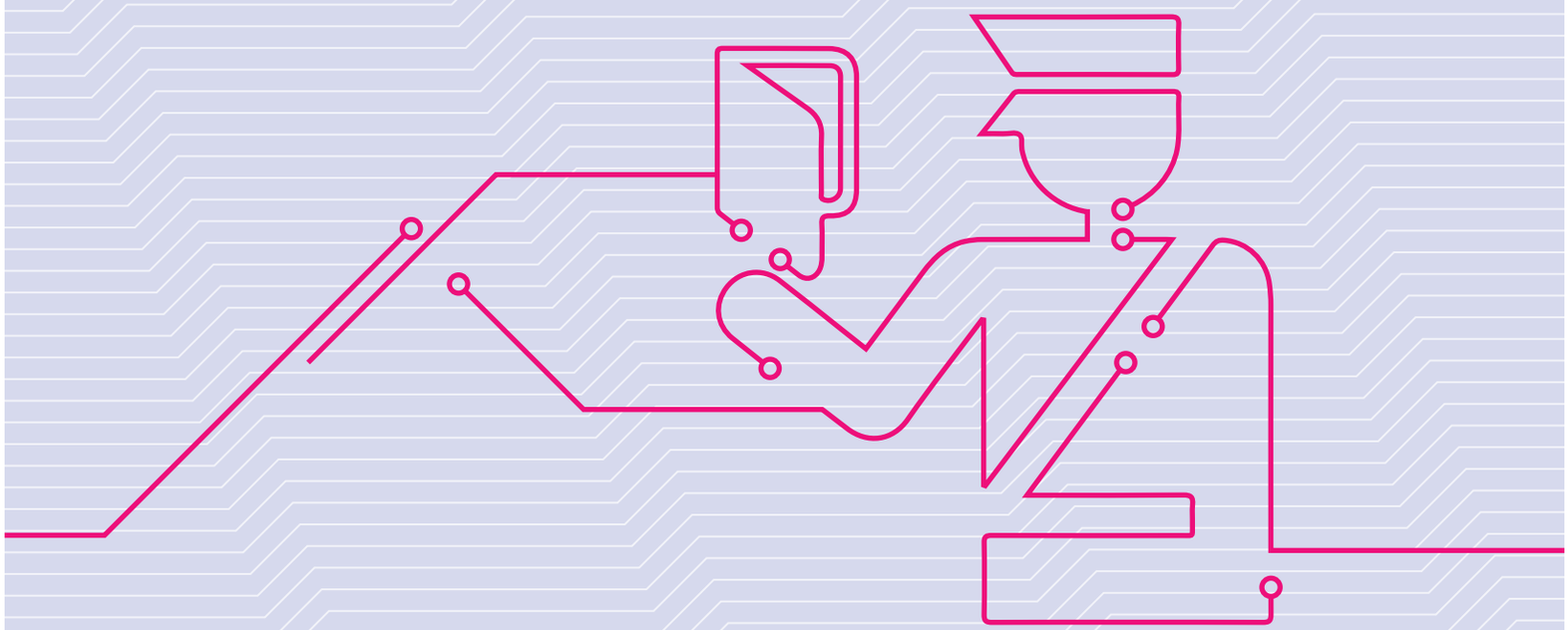
PUBLIC SAFETY

BORDER CONTROL

As the number of people moving across borders continues to increase, border control officials are faced with the challenge of increasing their processing capacity and speed without compromising on the stringency of their checks. Recognizing the role that technology can play in meeting this challenge, countries around the world have begun adopting biometric passports. To date, more than 60 countries have implemented or are planning to implement biometric passports or identity cards, including the European Union, the United States, China, India, Russia and Brazil.

In Singapore, a prosperous nation state highly dependent on trade and travel, biometric passports have been the norm since 2006. Like most modern and highly connected cities, it is a target for terrorism which could bring the economy to a standstill. Furthermore, the Singaporean passport is a frequent target for counterfeiters, valued for its list of visa waivers. In an attempt to both tighten security and speed up processing time, biometric passports and an automated clearance system were introduced. These have led to substantial improvements in processing times and yet low error rates; it now takes less than 12 seconds per passenger to clear immigration and has a false acceptance rate of only 0.001 percent.

To promote the adoption and international interoperability of biometric passports, the International Civil Aviation Organization (ICAO) has recommended the use of three standardized biometric features: fingerprint scanning, facial recognition and iris scanning. These represent the most mature and widely used biometric technologies at the moment.



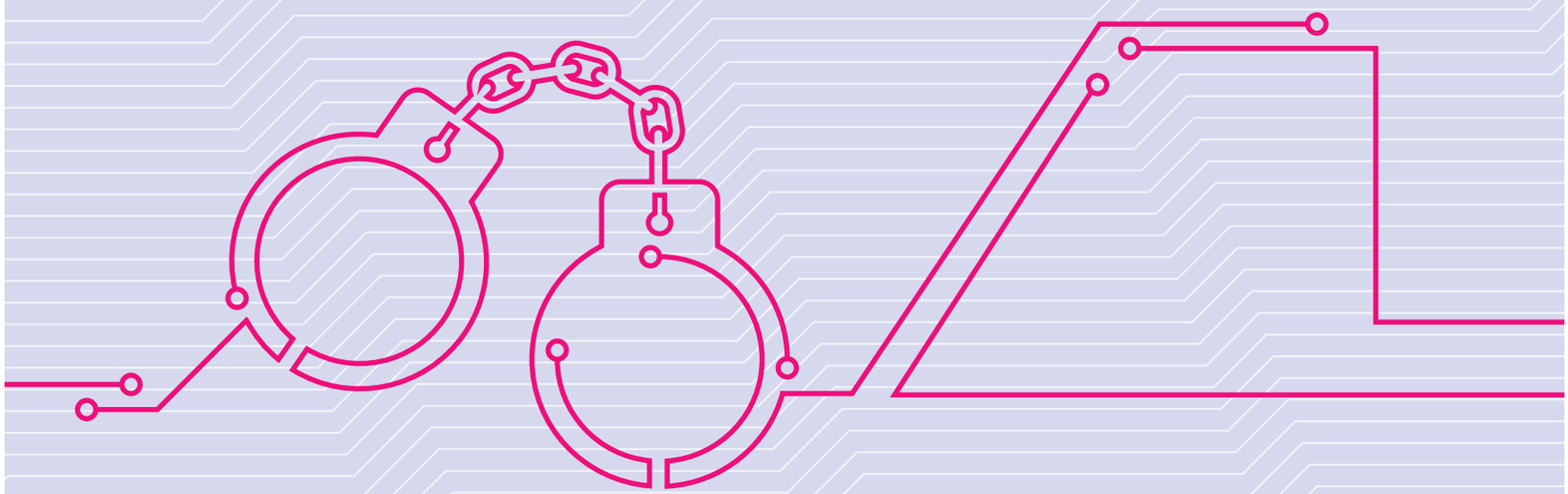
LAW ENFORCEMENT

Outside of airports, biometrics has also been a boon for law enforcement agencies. Criminal identification has relied on increasingly sophisticated and accurate methods, moving from distinctive marks such as tattoos to fingerprint databases and now facial analysis. Whatever the method used, the goal remains the same: to correctly identify criminals and exonerate the innocent.

Although fingerprint identification has been used for more than a hundred years, technology has greatly improved this process. Law enforcement agencies used to have to keep hardcopy ink prints which could become faded or lost. These days, millions of fingerprint entries are digitally stored and accessed, drastically reducing the amount of time taken to search through the database and freeing investigators to perform higher level tasks.

Facial recognition is another technology that plays a significant role in law enforcement, driven by two major trends. Due to the complexity of having to account for variation such as changes in appearance, lighting conditions and camera angles, human identification was the only feasible approach. However, the technology has now matured to the point where computerized facial recognition systems have surpassed human abilities. They are able to connect multiple types of information, whether it be from CCTV recordings, database records or photos from social media, and link them to a single individual. What used to require experienced personnel and many hours of scrutiny now can be automated and achieved in a matter of minutes.

Secondly, the proliferation of social media means that photographs are now easy to come by, changing the way facial recognition is used in law enforcement. Furthermore, social networks allow investigators not only to find photos of suspects, but to link them to the person's profile. Facial recognition driven by social media data has been used to combat terrorism, improve surveillance and even locate missing children. In all these cases, biometric information is often the only link.



PERSONAL SAFETY

SOCIAL SERVICES

Being able to verify identity is not only important for border control and law enforcement agencies, but could also help to prevent fraud, increase access to governmental services and even promote democratic participation. Biometrics, where the person serves as a marker of identity rather than a document, could be particularly useful in developing countries where literacy rates are low.

In 2009, the government of India embarked on a massive project to enroll its 1.2 billion residents into the biometrics-based Unique Identification Program, also known as Aadhaar. Intended as a means to fight corruption particularly in the issuing of subsidies, an Aadhaar social security number also provides the holder with access to other services such as healthcare and education. It also serves as a voter registration system, thereby helping to prevent electoral roll fraud.

Although costs have been substantial, amounting to US$574 million (3,496 Rs crore) as of September 2013 according to the Unique Identification Authority of India (UIDAI)[iii], benefits include fewer leakages, lower transaction costs and improved labor mobility. In fact, a cost-benefit analysis by the National Institute of Public Finance and Policy (NIPFP) shows that the implementation of Aadhaar yields an internal rate of returns of 53 percent[iv], even though it only takes into account the savings by the government. If intangible benefits and systemic benefits to the economy are also accounted for, the rate of return on investment in Aadhaar would be even higher.

INDIA'S UNIVERSAL ID PROGRAM BY THE NUMBERS

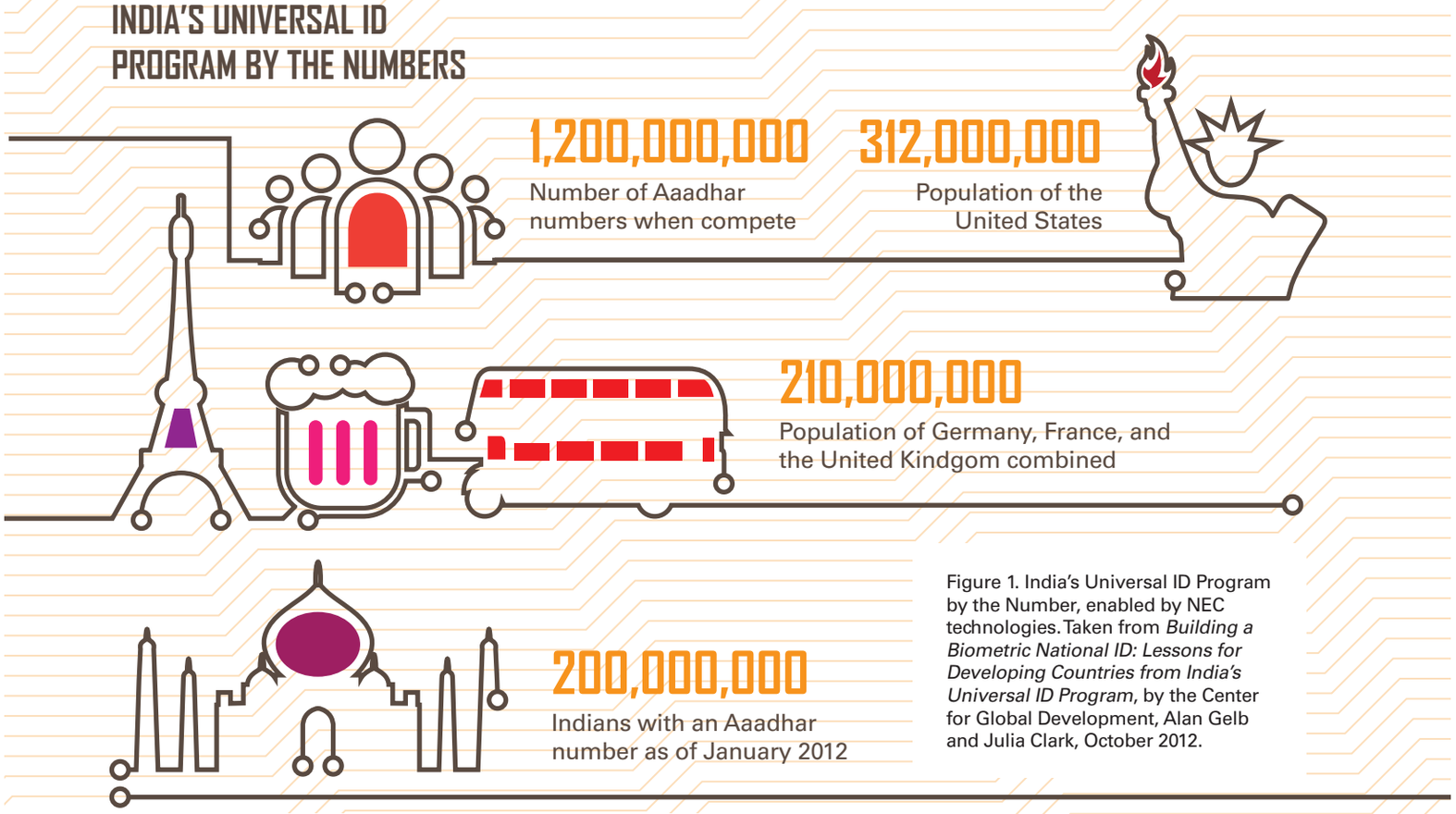


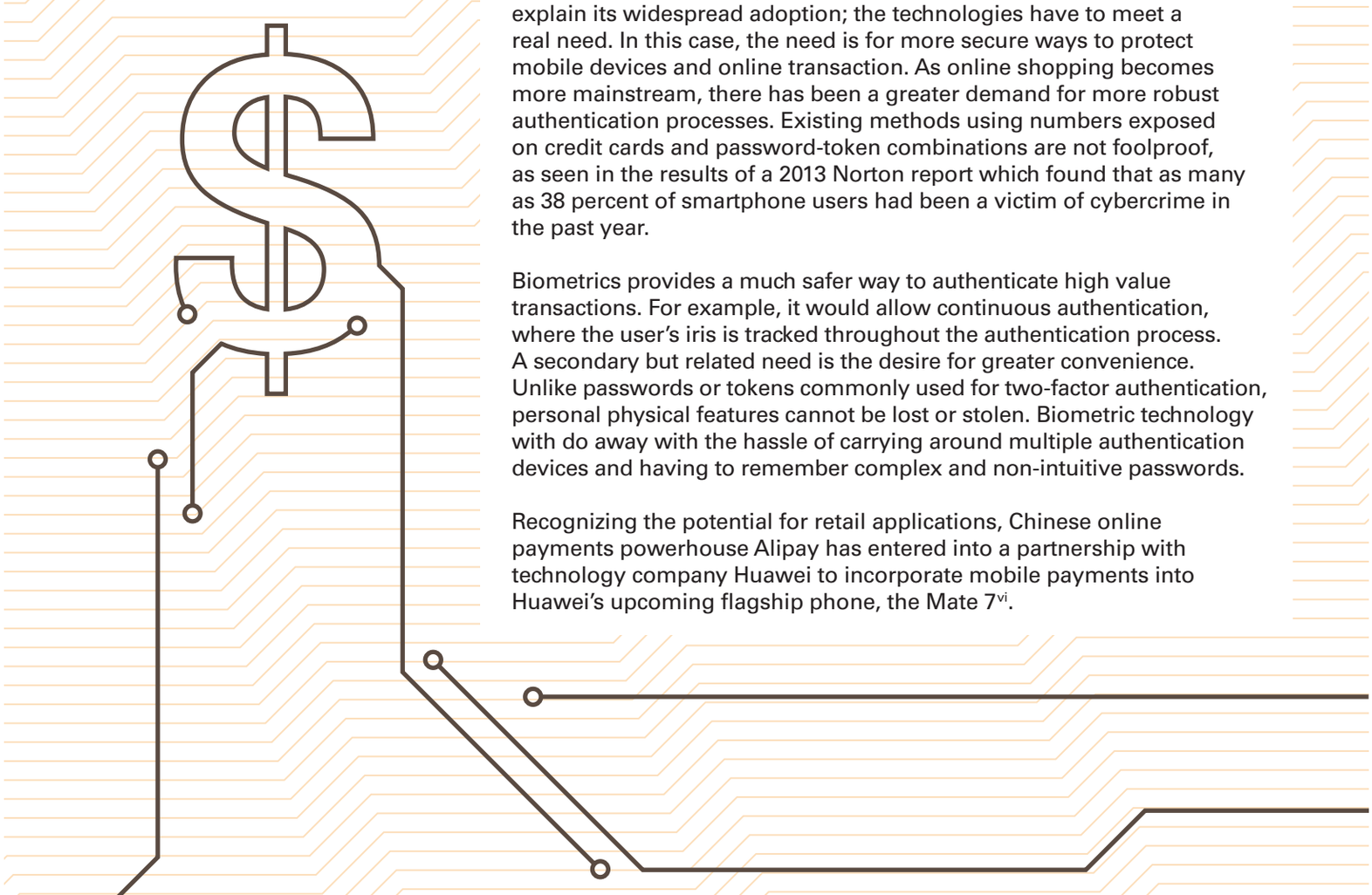
Figure 1. India's Universal ID Program by the Number, enabled by NEC technologies. Taken from *Building a Biometric National ID: Lessons for Developing Countries from India's Universal ID Program*, by the Center for Global Development, Alan Gelb and Julia Clark, October 2012.

CONSUMER APPLICATIONS

While government agencies have been quick to adopt biometric technologies, the take-up rate has been slower among individuals, largely hampered by high costs. Nonetheless, there is evidence that user acceptance is growing as the cost of mature biometric technologies falls.

In fact, a number of existing biometrics users is already substantial, driven largely by the adoption of biometrics technologies in the consumer smartphone market. Tech giant Apple first introduced their fingerprint locking system known as TouchID with the launch of the iPhone 5S in 2013, causing competitors Samsung to incorporate the same technology into the Galaxy Tab S. The recently launched iPhone 6 takes the technology further, integrating fingerprint scanning with near field communications (NFC) to enable mobile payments.

A market report by Frost and Sullivan predicts that there will be an explosive growth in the biometric smartphone market within the next few years, expanding more than ten times from 43 million in 2013 to 471 million in 2017[v]. With the staggering number of users, mobile adoption is likely to help biometric technologies to leapfrog into the mainstream.



However, the availability of biometric technologies alone does not explain its widespread adoption; the technologies have to meet a real need. In this case, the need is for more secure ways to protect mobile devices and online transaction. As online shopping becomes more mainstream, there has been a greater demand for more robust authentication processes. Existing methods using numbers exposed on credit cards and password-token combinations are not foolproof, as seen in the results of a 2013 Norton report which found that as many as 38 percent of smartphone users had been a victim of cybercrime in the past year.

Biometrics provides a much safer way to authenticate high value transactions. For example, it would allow continuous authentication, where the user's iris is tracked throughout the authentication process. A secondary but related need is the desire for greater convenience. Unlike passwords or tokens commonly used for two-factor authentication, personal physical features cannot be lost or stolen. Biometric technology with do away with the hassle of carrying around multiple authentication devices and having to remember complex and non-intuitive passwords.

Recognizing the potential for retail applications, Chinese online payments powerhouse Alipay has entered into a partnership with technology company Huawei to incorporate mobile payments into Huawei's upcoming flagship phone, the Mate 7[vi].

ADDRESSING PRIVACY CONCERNS

Aside from the cost factor, one of the considerations preventing the mass adoption of biometric technologies has been the issue of privacy. Although the fact that biometric features are irreplaceable makes them secure, it also means that steps must be taken that they do not fall into the wrong hands. In particular, consumers are concerned that biometric information in the form of facial photographs and fingerprints are easily available, and therefore open to theft.

However, what many consumers may not realize is that biometric technologies such as fingerprint and facial scanners do not store an actual image of the fingerprint, iris or face, but instead digitally encode the information in what is known as a template. Each device which captures biometric information would use different features to develop a template, making it difficult for a template captured on one device to be used to authenticate a device using a different template system. Furthermore, it is nearly impossible to reconstruct the original image based on the template data.

BIOMETRIC TRENDS

VIDEO ANALYTICS

As facial recognition technology continues to mature, the next key technology that looks set to grow in importance is video analytics. Traditionally, video surveillance has been used to secure restricted areas such as airport runways or hangars. This process is becoming increasingly automated, and predictive systems add an extra dimension to perimeter protection by enabling a proactive rather than reactive response.

Biometrics technologies are being embraced in video analytics particularly as we approach the limits of human operators. Human concentration, which can taper off after 20 minutes, means that human operators tend to have a high rate of overlooked events, especially when bored or fatigued. Furthermore, relying on human surveillance is not only inherently inefficient, but also increasingly expensive as manpower costs continue to rise.

Then there is the challenge of dealing with the sheer volume of video data being generated. With an estimated compound annual growth rate (CAGR) of 9-11 percent, video surveillance is predicted to reach a staggering 3.3 trillion hours of video in 2020, according to a report by Homeland Security Marketing Research[vii]. Going by a conservative assumption that only 20 percent of the most critical video will be reviewed by staff, this nonetheless entails a workforce of over 110 million security personnel worldwide, dedicated to video surveillance.

Not only will video analytic systems be inevitable, but they will also bring new capabilities to the table. Motion detection can be used to identify behaviors such as loitering or objects that have been stolen or left behind. These capabilities will be particularly useful in high security areas such as airports, alerting staff to suspicious persons and objects such as unattended baggage. Video analytics are also able to automatically track moving objects across multiple cameras and give real-time information on the movement of crowds.

The ability to sharpen images from low resolution video and the automated filtering of irrelevant images facilitate forensic video searches and post event analyses. For example, individuals identified by video surveillance can be checked against Interpol's stolen and lost passports list.

Video analytics is not restricted to facial recognition, but has also been very useful in vehicle and license plate recognition for security purposes. In the business setting, video analytics can also be used to gather business intelligence by counting people or analyzing the flow of traffic.

CASE STUDY: TRAIN VIDEO SURVEILLANCE

The 2005 London train bombings highlighted the fragility of public transport systems and exposed the inherent risks onboard trains and buses. The Yishun MRT bomb plot uncovered in 2001 showed that even relatively safe Singapore was not immune to the risk of terrorist attacks.

To improve safety across Singapore's Mass Rapid Transit system, NEC was selected to provide video surveillance for all existing lines. Slated for completion in 2018, the video surveillance system will provide real time monitoring of train operations and is expected to assist law enforcement agencies in even reconstruction. The system can also adapt to future needs, with the potential for upgrade to voice recording and video analytic capabilities.

MULTI-MODAL BIOMETRICS

Although biometric technologies are a vast improvement over existing identification and authentication methods, no technology is infallible. Though the chance is small, errors could potentially be introduced at each stage of the biometrics process, from enrolment and matching to database management.

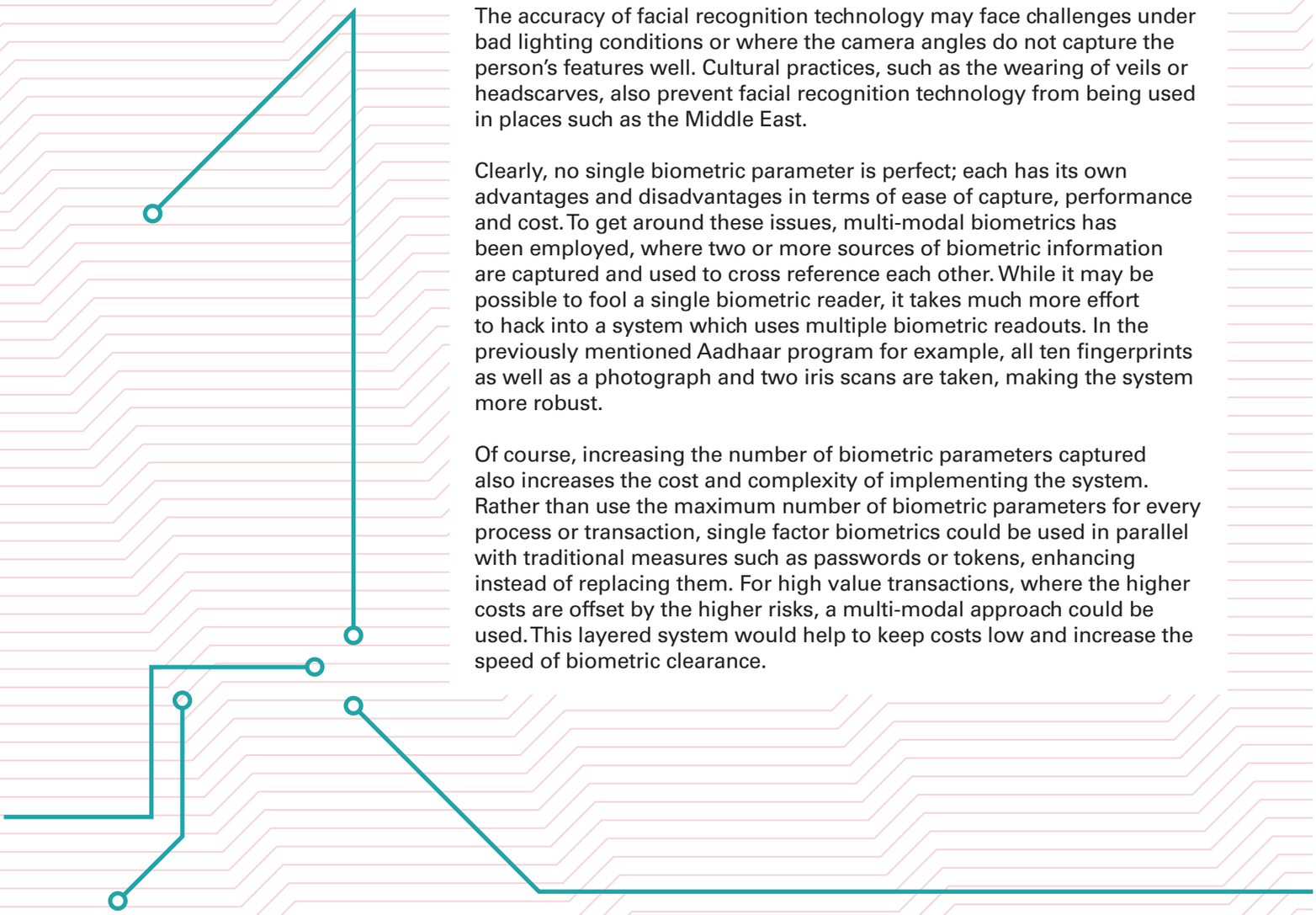
Apple's TouchID system was shown to be hackable within hours of its 2013 launch. Using a latent print from the phone, a laser printer, some white wood glue and a bit of breath to keep the fake print moist, the Germany-based Chaos Computer Club was able to bypass the fingerprint lock screen. Although much too complicated for the casual cracker, this breach demonstrates that relying on a single biometric method is not sufficiently secure.

Furthermore, there are situations in which single parameter biometrics fail. For example, two to three percent of the population has no usable fingerprint, such as laborers with worn fingerprints or people with a genetic condition called adermatoglyphia, also known as immigration delay disease.

The accuracy of facial recognition technology may face challenges under bad lighting conditions or where the camera angles do not capture the person's features well. Cultural practices, such as the wearing of veils or headscarves, also prevent facial recognition technology from being used in places such as the Middle East.

Clearly, no single biometric parameter is perfect; each has its own advantages and disadvantages in terms of ease of capture, performance and cost. To get around these issues, multi-modal biometrics has been employed, where two or more sources of biometric information are captured and used to cross reference each other. While it may be possible to fool a single biometric reader, it takes much more effort to hack into a system which uses multiple biometric readouts. In the previously mentioned Aadhaar program for example, all ten fingerprints as well as a photograph and two iris scans are taken, making the system more robust.

Of course, increasing the number of biometric parameters captured also increases the cost and complexity of implementing the system. Rather than use the maximum number of biometric parameters for every process or transaction, single factor biometrics could be used in parallel with traditional measures such as passwords or tokens, enhancing instead of replacing them. For high value transactions, where the higher costs are offset by the higher risks, a multi-modal approach could be used. This layered system would help to keep costs low and increase the speed of biometric clearance.



MOBILE BIOMETRICS

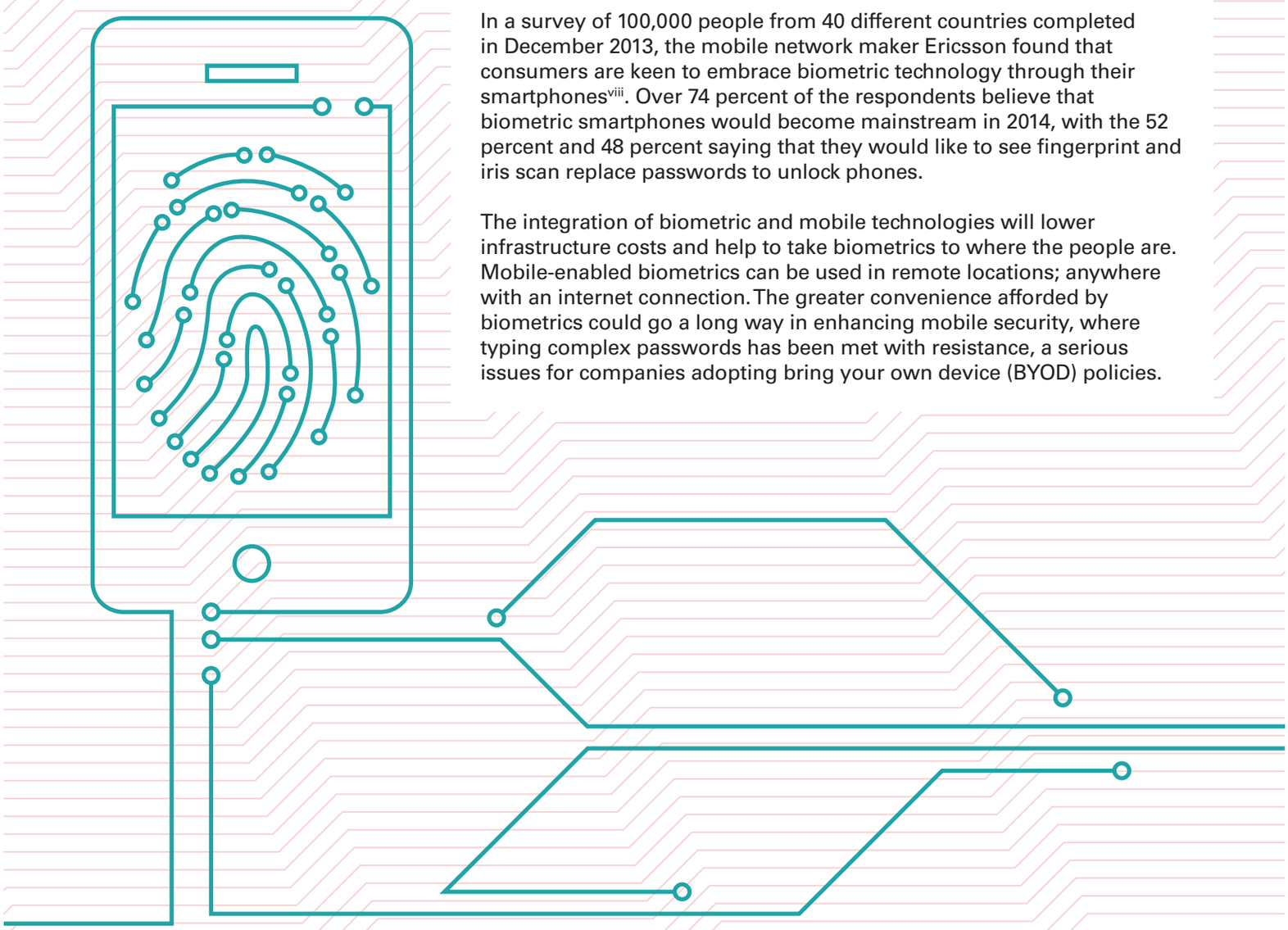
There is little doubt that the field of biometrics will continue to grow, spurred by both large government projects and wide-scale adoption by individuals. Of these two forces, personal adoption, and mobile biometric technologies in particular, are likely to shape the face of biometrics of the future.

With the ubiquity of mobile devices today, it is easy to take for granted the technology that has driven the mobile revolution. Each smartphone has processing power that was unattainable by desktop computers a generation ago crammed into a handset that fits into a pocket.

From the biometrics point of view, a smartphone is a ready-made biometric sensor, with a built-in high resolution scanner and camera, equipped with sophisticated gyroscopic measurement devices and internet connectivity. Being able to tap into these existing features rather than design and sell stand-alone biometric readers has the potential to revolutionize the use of biometrics.

In a survey of 100,000 people from 40 different countries completed in December 2013, the mobile network maker Ericsson found that consumers are keen to embrace biometric technology through their smartphones[viii]. Over 74 percent of the respondents believe that biometric smartphones would become mainstream in 2014, with the 52 percent and 48 percent saying that they would like to see fingerprint and iris scan replace passwords to unlock phones.

The integration of biometric and mobile technologies will lower infrastructure costs and help to take biometrics to where the people are. Mobile-enabled biometrics can be used in remote locations; anywhere with an internet connection. The greater convenience afforded by biometrics could go a long way in enhancing mobile security, where typing complex passwords has been met with resistance, a serious issues for companies adopting bring your own device (BYOD) policies.



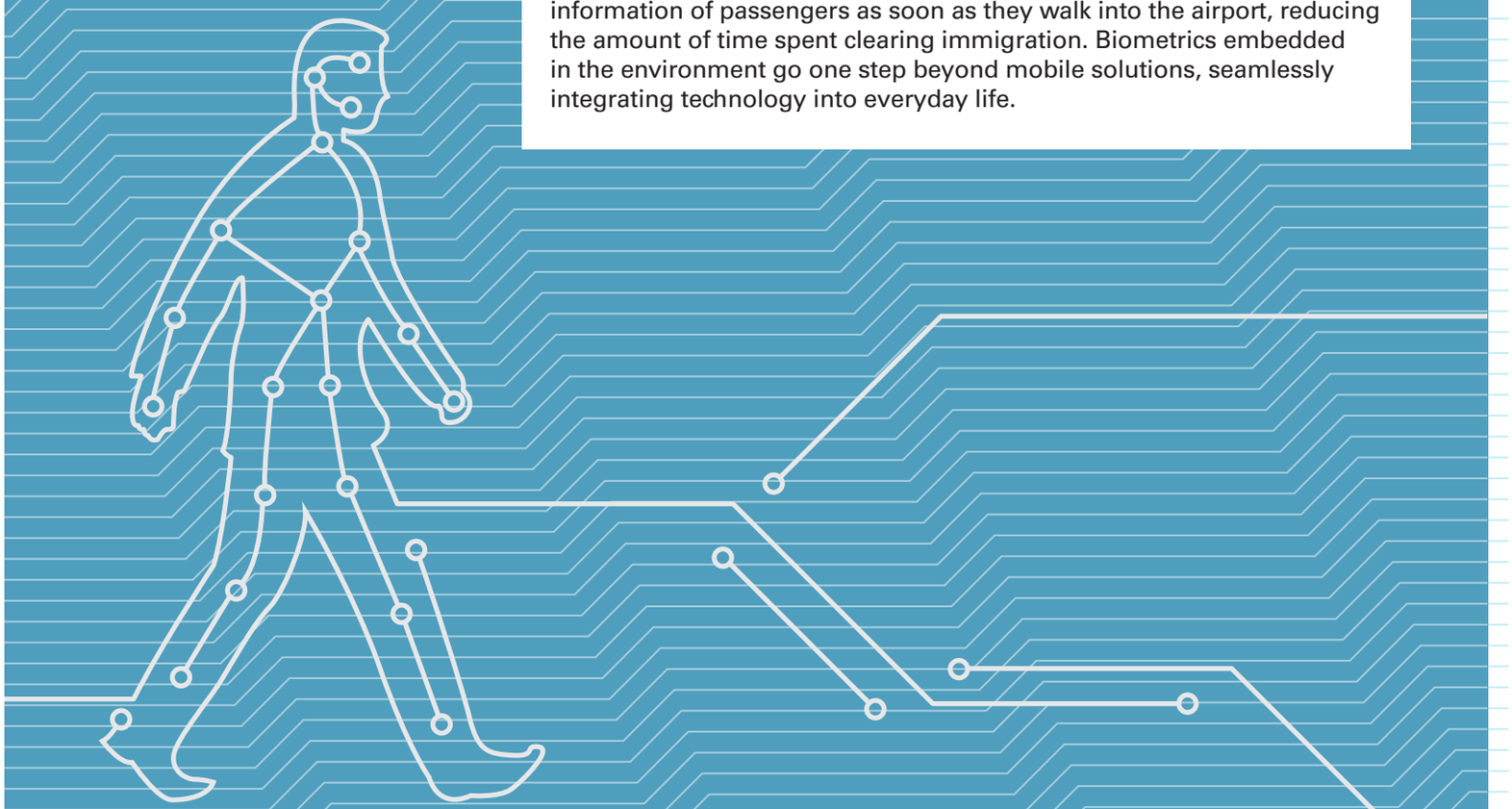
BIOMETRICS ON THE MOVE

Enabled by the latest advances in capture technology, biometrics on the move allows features to be taken without manual intervention and even while the subject is in motion. Also known as stand off biometrics, this technology enables contactless fingerprint capture and iris or face detection based on video surveillance. In contrast, older technologies are cumbersome and time consuming, requiring direct contact with a fingerprint scanner or for the subject to present themselves to the capture device, holding still to ensure a high quality scan.

Biometrics on the move could potentially revolutionize law enforcement, allowing real-time watchlist detection and monitoring of people moving through sensitive areas such as nuclear power plants and security facilities. In public safety, biometrics on the move could help with crowd control and flow management, automatically preventing bottlenecks which could potentially be dangerous or at the least, time wasting.

Biometrics on the move also finds many applications in providing business intelligence. Anonymous, non-intrusive real-time monitoring can capture "soft" biometric features such as age, gender and ethnicity, allowing retailers to provide targeted services dependent on demographic features. Information on the people walking through a mall, for example, could help retailers make decisions about how to design and stock their stores.

Most of all, biometrics on the move makes the adoption of biometric technology convenient for users. For example, it can be used to capture information of passengers as soon as they walk into the airport, reducing the amount of time spent clearing immigration. Biometrics embedded in the environment go one step beyond mobile solutions, seamlessly integrating technology into everyday life.



NEC: BIOMETRICS PIONEER AND LEADER

Technology adoption is driven not only by advances in the technology itself, important though it may be, but also the demand generated from positive user experience. A biometrics pioneer since the 1970s, no one knows this better than NEC. With over 500 contracts in over 40 countries, NEC has extensive experience in designing and deploying comprehensive biometrics solutions.

Far from resting on their laurels, NEC has constantly sought to innovate and keep their technologies at the bleeding edge of research. For instance, NEC's face recognition technology, NeoFace, achieved the highest performance evaluation in the 2013 Face Recognition Vendor Test performed by the U.S. National Institute of Standards and Technology (NIST), taking first place for the third consecutive year. NEC's Automated Finger Identification System (AFIS) has also been certified as the world's most accurate by independent NIST tests.

By combining our strengths in individual biometric technologies, NEC is well poised to capitalize on multi-modal biometrics and provide its customers with solutions above current market standards. Our Hybrid Finger Scanner simultaneously obtains fingerprint and finger vein information, robustly combining both features using our patented Fusion Identification Method. Lightweight and contactless, it is easy to use and compatible with existing desktop computers, requiring just a USB connection and power source.

NEC's solutions are also highly flexible, with a modular architecture that facilitates customization. At the same time, NEC technology supports internationally recognized standards, ensuring interoperability across different countries and smooth integration with legacy systems.

As a recognized leader in biometrics and a trusted partner of organizations such as Interpol, NEC's public safety solutions are sought after by the world's leading identity management and security programs in law enforcement, criminal justice, border control, civil identification and defense personnel safety. We remain ready to offer our expertise at all levels of integrated security solutions–from hardware and networking to applications and service.

http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf

[i] White et al (2014). Passport Officers' Errors in Face Matching. PLoS ONE. http://dx.doi.org/10.1371/journal.pone.0103510

[ii] http://www.cpr.cuhk.edu.hk/en/press_detail.php?id=1856

[iii] http://uidai.gov.in/images/web_exp_sep2013.pdf

[iv] A cost-benefit analysis of Aadhaar, National Institute of Public Finance and Policy, November 2012. http://macrofinance.nipfp.org.in/FILES/uid_cba_paper.pdf

[v] http://ww2.frost.com/news/press-releases/frost-sullivan-biometrics-can-be-alternative-conventional-authentication-technologies-mobiles/

[vi] http://www.planetbiometrics.com/article-details/i/2139/

[vii] Intelligent Video Surveillance, ISR & Video Analytics: Technologies and Global Market 2013-2020. Homeland Security Research.

[viii] 10 Hot consumer trends 2014. Ericsson Consumer Labs. http://www.ericsson.com/res/docs/2013/consumerlab/10-hot-consumer-trends-report-2014.pdf

Contributors:
Kris Ranganath, Director of Technology & Solutions Development, Biometrics Solutions Division, NEC.

About NEC Global Safety Division

NEC Global Safety Division, a business division within NEC Corporation, spearheads the company's public safety business globally. The Division is headquartered in Singapore and offers solutions in the following domains: Citizen Services & Immigration Control, Law Enforcement, Critical Infrastructure Management, Public Administration Services, Information Management, Emergency & Disaster Management and Inter-Agency Collaboration. Leveraging on its innovative solutions, the Division aims to help government and business make cities safer.

NEC Global Safety Division
Global Headquarters: 2 Fusionpolis Way, #07-01/02/03 Innovis, Singapore, 138634
For enquiries, please contact safety@gsd.jp.nec.com

nec.com/safety