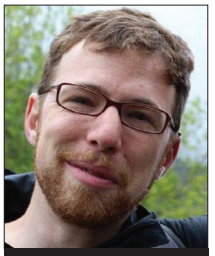
Can biometrics beat the developing world's challenges?



Daniel Storisteanu

Daniel M.L. Storisteanu, Toby L. Norman and Alexandra Grigore (Simprints Technology), and Alain B. Labrique (John Hopkins University)

The World Bank estimates that as many as 1.5bn people worldwide do not *officially* exist. This lack of formal identification is a key challenge across the developing world – without reliable, unique and persistent identifiers, governments and development organisations struggle to provide essential goods and services to the populations they serve. The problem is wide-ranging: the dynamic nature of subsistence or agricultural communities and largely dysfunctional civil registration systems, combined with rapid population growth, have led to communities which are uncountable and poorly censused. Paper-based identity systems are resource-intensive, fragile and easily manipulated.

Specifically, continuity of care in healthcare provision requires some mechanism of linking clients to their records over time. Lack of official identity documentation such as national ID cards or birth certificates obstructs people's access to rights and services. This can cost lives, waste resources (through inefficient distribution of limited resources), and prevent health, finance and other development organisations from reaching millions of beneficiaries, according to Gelb & Clark and other reports[1-4]. For example, systems that lack the critical 'backbone' to link records to individuals using unique identifiers may fail to recognise when pregnant women miss follow-up visits, which could prevent maternal and infant deaths, or when emerging entrepreneurs might be excluded from financial services.

As Alan Gelb, Director of Studies at the Center for Global Development, recently noted: "The identity gap is increasingly recognised as not only a symptom of underdevelopment, but a contributing factor." This problem is now recognised in the UN Sustainable Development Goals and by groups such as the World Bank's ID4D (ID for Development) and ID4Africa, which have been set up to tackle this challenge.

Identification is also essential to the gathering of accurate data, allowing the development community to better monitor the progress of programmes. Governments and international organisations currently rely on uncertain estimations for many progress indicators. For example, maternal mortality numbers in most countries are calculated on a regression model based on key predictors that puts maternal mortality in 2013 anywhere between 220,000 and 400,000 deaths[5], an arguably unacceptable level of uncertainty for a major development indicator.

"Systems which lack the critical 'backbone' to link records to individuals using unique identifiers may fail to recognise when pregnant women miss follow-up visits which could prevent maternal and infant deaths"

Programmes often try to use personal information such as names, dates of birth and postcodes to identify beneficiaries. But the problem is these identifiers are rarely unique and naming conventions vary dramatically across, and sometimes within, cultural groups. Individual names or family name combinations can repeat multiple times in a community (over 60% of males in some areas of Bangladesh use an honorific first name 'Mohammed', combined with a second name from a fairly small pool of options[6]). Names can be spelled (or unintentionally misspelled) in multiple ways, and many people do not know their exact date of birth.

Other challenges to paper-based ID systems, beyond the sheer logistics of capturing populations spread across large geographic areas, poor government infrastructure and record-keeping, also include the high costs of implementation and the frequency with which ID cards are lost or damaged.

Biometrics solution

Biometric identification can solve these intractable problems, providing a solution to help lift people out of poverty and even save lives. In much the same way as mobile phones have leapfrogged the need for landline phone infrastructure in the developing world, biometrics are on the verge of doing the same for the identification bottleneck. Biometrics include a wide range of biological measures which are considered sufficiently unique at a population level to allow individual identification with high rates of accuracy. Fingerprints, retina scans, voiceprints and facial feature recognition are some of the more commonly encountered biometrics, used to supplement or substitute formal paper-based identification.

Well over 1bn people in developing countries have now provided their biometrics across many hundreds of programmes spanning a wide range of organisations. For example, the UN High Commissioner for Refugees (UNHCR) is piloting fingerprint and iris enrolment of refugees. A government-owned hospital in Nepal is incorporating biometrics into an electronic health programme and the Unique Identification Authority of India is set to biometrically enrol the country's entire population of over 1.2bn people as part of its national registry.

A growing body of evidence demonstrates that biometrics can help build solid ID systems in short periods of time, with nearly immediate secondary benefits. A recent review of 160 biometric programmes in developing countries highlighted significant reductions in record-keeping errors, processing times and fraud (Gelb & Clark Working Paper cited above). With biometric IDs, previously 'invisible' residents may access rights and services that further efforts of inclusion and development goals like universal health coverage.

Current biometric failure

However, the current landscape of biometric projects is littered with pilots that have been

unable to scale through issues including low-accuracy performance, high costs and low interoperability between vendors. One problem is that, to date, no biometric system has been built specifically for use in the developing world, especially remote, rural settings where environmental conditions are harsher – high temperatures, pernicious dust and humidity, and worn or rough fingerprints can wreak havoc on sophisticated device performance and longevity. Again, an absence of interoperability standards and open systems creates insurmountable barriers to scale for many governments and development organisations, operating in parallel. Technology and systems turnover leads to rapid obsolescence, often accompanied by loss of support systems for the technologies invested in.

At a national scale, robust technologies are needed which can survive under difficult conditions for multiple years – with back-end data that remains compatible with future generations or advancements in biometric technology. Re-censusing hundreds of millions of people each time a shift in biometric technology occurs quickly is financially and logistically untenable. Here are the key issues to address:

1. Modalities

While most problems identified in this article can be tackled across a number of biometric modalities, here we focus on digital fingerprinting. This modality, by today's technical standards, is the least complex, least expensive and most consistently accurate (in its class of simplicity and cost) – all facets that increase the likelihood of its adoption and scale-up. As the use of mobile computing and communications technologies, like smartphones, continues to increase across government and development agencies, supporting biometrics with these devices may be an appropriate future strategy to cut device and implementation costs. Currently, smartphones with on-board fingerprinting capability are not accurate enough to perform 1:N matching and tend to be expensive. However, purpose-built accessory devices connected to a phone could utilise communication and connectivity functions for improved performance.

Other possible modalities that can be used with a smartphone include iris and voice recognition. Irises remain relatively stable over a person's lifetime, and their uniqueness allows for accurate identity matching when used with high-quality imaging technology[7]. However, a major problem is cost. Ideally, irises are imaged with expensive high resolution, near-infrared cameras, although the cost of these cameras has fallen and some are now available in select high-end smartphones. Acceptability may be another barrier to iris biometrics reaching higher levels of adoption – our field tests in Dhaka, Bangladesh found that many people were reluctant to have their photograph taken.

Voice recognition (aka speaker recognition) is another exciting biometric modality increasingly being used. Voice characteristics such as timbre, pitch and modulation are influenced by physiological traits such as the shape of one's vocal chords and nasal cavity, and behavioural traits that influence speech cadence and accent. At the time of writing, we are not aware of any high-accuracy voice recognition system that does not require server-level processing power. This in turn means systems have to maintain internet or phone connectivity to function – a problem in many international development contexts. Further research is also needed into whether illnesses or environmental factors that affect a person's voice preclude the reliable use of this biometric.

2. Systems must be human-centred

A major concern for a biometric ID system is the risk of exclusion; systems must be designed to reduce the proportion of people who are physically unable to enrol, and not punish people who cannot or choose not to enrol. Take the case of handling damaged fingerprints. Essentially all biometric systems in use today are designed for and by people in high income countries, and provide little focus on either sensing hardware or matching software that can deal with the considerable wear and scarring common in the developing world. Many people have been labouring with their hands their entire lives and display an above-average level of burns, scars and worn fingerprints. In our field tests with 217 Zambian manual farmers, 84% had some damage to their fingerprints.

In standard industry evaluations of system performance, error metrics are typically measured from biometric features captured in highly controlled laboratory settings from individuals employed in non-manual work. But typically in development applications, people are employed in manually intensive labour in challenging environmental conditions. We tested six commercial sensors reporting high accuracy levels by collecting over 125,000 fingerprint images from low-resource populations in Zambia, Benin, Nepal and Bangladesh. (This research was conducted in partnership with local NGOs and was approved by the University of Cambridge Judge Business School Ethical Review Committee. Informed consent was obtained from all participants.)

Many people have been labouring with their hands their entire lives and display an above-average level of worn fingerprints.

Every system tested failed to reach accuracy rates published in industry reports. The highest performing sensor was based on optical technology. Its superiority was most pronounced when imaging especially dry, damp (eg, sweaty) or worn fingers, which greatly challenged other technologies such as those based on capacitance, the technology used in most fingerprinting smartphones. However, optical technology failed most when sensors were exposed to direct sunlight during fingerprint capture. Overall, we found that fingerprinting can achieve high accuracy in difficult development contexts, but the sensor, extractor and matching software need to be tailored to this context.

3. Individuals who cannot be enrolled

Identification systems must prevent and mitigate errors that arise from false rejections (where someone cannot be matched to their previous fingerprint), which could lead to exclusion from services; or false positives (where the incorrect person is matched), which could, for example, lead to a patient being administered incorrect medication.

While tailoring hardware and software to international development contexts can reduce these errors, industry challenges remain in the fingerprint-identification of infants and individuals with notably worn prints. Biometric enrolment of infants, in particular, is in increasing demand for applications including tracking vaccination coverage and preventing misidentification in hospitals. Although there have yet to be any breakthroughs in this field, promising improvements for enrolment of infants as young as four weeks come from the work of Anil Jain et al at Michigan State University[8]. For many programmes, connecting an infant's record to the fingerprints of their legal guardians is a viable solution.

To prevent the individuals with especially damaged fingerprints from being excluded from services, enrolling multiple fingerprints or using multiple biometric modalities can significantly increase matching accuracy. In addition, alternatives must be available where individuals have extraordinarily worn fingerprints and cannot be

Optical technology proved the most accurate when imaging dry, damp or worn fingers.

enrolled, or choose not to give their biometrics.

In many applications, biometric systems will already need to be integrated with software platforms that use case management tools with searchable unique IDs such as names. In cases where individuals choose not to or cannot give fingerprints, the platform's current search system can still be used. Finally, when an individual is returned by the system as a match, it is critical that frontline workers are trained to always confirm a beneficiary's identity using secondary identifiers such as a photograph or name available already in the client database, to prevent the wrong goods or services from being administered.

4. Increasing usability through feedback loops

Ensuring that fingers are placed on the sensor consistently and properly is another significant factor contributing to system accuracy. This challenge is more pronounced with populations that have low lifetime exposure to technology. For example, many individuals in our Benin and Zambia cohorts intuitively tried to place their finger on the sensor as one might press a lift button, completely perpendicularly. To this end, hardware designed for ergonomics and ease-of-use can dramatically improve the accuracy of a system.

Including the intended users in product development can help to create systems that minimise finger placement errors and other adoption barriers. In contrast to traditional 'waterfall development' approaches, where every stage of R&D is mapped on to phases and rarely revisited once completed, adapting iterative and agile approaches in software and hardware development can be invaluable to producing a useable, intuitive system.

We worked with frontline workers interested in becoming users of biometric systems in Zambia, Benin, Bangladesh and Nepal to co-create and test sketches and moulds of casing concepts, prototypes, symbols and LED features for buttons and feedback features, and the design of the workflow. These exercises contributed significant suggestions to almost every facet of hardware design, including using a silicon rubber strap so users could confidently hold the scanner while operating other devices, and designing the casing so users can intuitively pinch the scanner to get the correct finger placement.

5. Technical considerations

Technologies created for developed countries frequently fail when transferred to global development contexts. This includes several stark examples of biometrics used for elections (Gelb & Clark Working Paper). These products often take for granted advanced infrastructure that allows consistent access to electricity and connectivity. To collect biometrics in the developing world, organisations require low-cost, rugged, high-accuracy systems that work independently of connectivity. Here are the main challenges

• **Mobility and connectivity**. In many programmes hindered by identification problems, frontline workers visit beneficiaries rather than the other way around. For example, community health workers make regular visits to pregnant women at their homes; micro-finance officers meet borrowers at community meetings in remote villages; and agricultural officers visit farmers on their land. If a frontline worker were to carry around a centralised identification station, they would need to bring a laptop and a wired scanner into the field and have constant access to the internet. Needless to say, this is neither practical nor feasible for these organisations, as constant connectivity is impossible. For this reason, a mobile scanner and device capable of running an automated fingerprint identification system (AFIS) is needed.

Simprints' design uses a mobile fingerprint scanner that connects via Bluetooth to a mobile phone.

In contrast, low-cost scanners are typically designed for desktop use. Without an on-board battery, Bluetooth and a rugged casing, they are useless for mobile field applications. Laptops are too expensive for many NGOs to provide to every frontline worker and too heavy to carry on field visits. Moreover, our interviews with organisations that have experimented with USB scanners report frequent breakdowns when used in harsh conditions.

The system that we are building, in a project between the University of Cambridge and the non-profit Simprints, uses a mobile fingerprint scanner that connects via Bluetooth to a device that frontline workers already frequently possess – a mobile phone[9]. This way, a frontline worker only has to sync their phone with a database, usually held online, before leaving for the field, and the scanner can pass a fingerprint template to the phone for offline matching. This is possible in the vast majority of use cases we have examined, where a database never needs to be larger than about 2,000 enrolees per device – which reflects the larger catchments covered by frontline workers and data enumerators.

Since internet connectivity is intermittent, it is crucial that these systems function offline. When there is internet connectivity, matching can run on the cloud. A cloud server can also be used to sync and back up data between different devices and act as a centralised verification station when required (eg, when a beneficiary moves into a catchment held by another database, or for de-duplication).

• **Cost** is often a primary concern for organisations working in international development. Budgets are extremely stretched and funding towards building technical infrastructure often comes directly at the expense of goods or services given to beneficiaries. Because users of biometric systems in systems in high-income countries often don't face the same cost constraints as organisations working in development, the cost of sales is frequently high. A second, related issue is over-specification. Because there is no incentive for stripped-down, lean biometric systems, most existing systems provide numerous costly features unnecessary for frontline workers in places like Bangladesh. There is a huge need in these places for lean systems developed with cost-reduction prioritised.

• **Robustness**. International development organisations often work in challenging environments. Frontline workers may have to hike up freezing high-altitude mountains in the Himalayas, or trek across dusty sand dunes in Saharan deserts. So the ideal scanner should

be shock-proof, water-resistant, dust-proof, and sustain a wide range of temperatures. One prototype we developed in the UK worked perfectly until we tested it in South Asia, where temperatures surpassed 40 degrees Celsius. A diode started leaking at these temperatures, triggering the circuit that starts up the CPU. As a result, the scanners turned on automatically whenever the weather became particularly hot, draining the battery. To troubleshoot this, our UK engineers used hair dryers to trigger the fault. Before deployment, hardware must be tested in a wide range of temperatures and humidity, and for ingress protection rating (eg, against dust and water ingression).

• **Interoperability** between biometric systems is a major consideration. Low interoperability arising from many customised, piecemeal solutions unable to talk to one another leads to redundancy and wasted effort, and may create complex technological barriers when trying to integrate systems. As more organisations adopt biometric systems, the ability to link beneficiaries between programmes, such as vocational training and micro-finance schemes, will be a powerful way to create holistic solutions to development challenges. For this to occur, programmes must adopt open ISO standards, such as NIST/ISO 19794-2 fingerprint templates which ensure fingerprint databases are interoperable with other open-standards systems. For example, the Indian Government's Aadhaar/UID scheme has enrolled over 1bn citizens with a unique biometric ID utilising 19794-2 fingerprint standards.

• **Open source**. Commercial extraction and matching algorithms are closed-source and proprietary. This makes them hard to upgrade or modify to meet project needs, limits the scope for collaboration, and makes the implementing organisation completely dependent on the vendor. If the supplier stops supporting a system, or goes out of business, the project fails. NGOs, social enterprises and particularly governments prefer working with providers of open source software because it doesn't lock them into a single supplier and allows them to take over ownership of the code if needed.

Given the success of open source digital platforms in international development, such a system in the biometrics sector is badly needed. Open source algorithms such as the NIST Biometric Image Software (NBIS) MINDTCT template extractor and Bosorth3 matcher, and Robert Vazan's SourceAFIS, are freely available for download. However their performance has yet to compete with proprietary systems. A high accuracy, fast and open extractor and matcher could be hugely beneficial for biometrics in development.

• **Security**. While we believe the benefits of biometrics potentially far outweigh the risks, it is the responsibility of all stakeholders to prioritise mechanisms that reduce these risks. Technical security measures are vital in systems used to handle personal data. For example, biometric data should be encrypted when not needed for authentication, and should be secured with SSL/TLS encryption when transmitted between devices. Images should be stored as encoded numeric byte-array templates. This means that in the unlikely event of unauthorised access, it is incredibly difficult to reverse-engineer the original image from an extracted template. Images should not be stored if templates are sufficient, and otherwise should be stored separately.

• **Privacy**. Biometric technology has made it easier to intrude on individual privacy on an unprecedented scale. Regardless of the security measures taken, history has shown that nothing is completely invulnerable to theft or abuse. And if someone's biometric data such as their fingerprint falls into the hands of an individual wishing to inflict harm, it is not possible to change, unlike a driver's licence or passport.

In many developing countries, privacy laws are often non-existent. However, it is imperative that privacy is viewed as a universal good to be protected and respected, and not as a process to satisfy bureaucratic requirements. It may be tempting to collect additional information or retain it longer than necessary, on the basis that it could become useful in the future. But doing so fails to recognise the dangers of data breaches or mission creep – where data is used for new purposes or shared with other organisations who use it for purposes outside the scope for which consent was originally given.

Only data essential to the delivery of goods or services should be taken. In the case of the maternal and child health projects we are involved in, this means taking biometric data stored as a template (the image is discarded), and in some cases coarse GPS data. We do not ask for individuals' names, dates of birth or other identifying information. An individual's template is contained in our databases with a randomly generated, numeric unique ID. This is used to link the information to a development organisation's database, which may contain other personal data. Therefore, if the biometric database is successfully attacked, sole access to encrypted templates and randomly generated UIDs make it impossible to connect to individuals.

• **Acceptability and consent**. The acceptance of a biometric system by individuals will vary widely depending on the specific use case and cultural context. For example, in Bangladesh we found that a large proportion of people were resistant to having their photograph taken, but consented to giving fingerprints. A large-scale CDC study showed that 94% of people approached in Kenya consented to fingerprint enrolment[10]. High levels of acceptance in developing countries have been attributed to the lack of criminal justice connotation that fingerprints have in the West[11]. Instead, biometric projects in developing countries have largely focused on fighting corruption, such as in elections, or giving access to services such as mobile money schemes (Gelb & Clark Working Paper).

When participants trust that programmes are designed to benefit them, they are much more likely to consent. But beyond the fact that informed consent is usually a legal requirement, it also plays a significant role in building trust with beneficiaries and the community. Perhaps most importantly, it is ethically imperative that people always have available the information that enables them to make the best decision for themselves.

However, in practice this may be difficult. Development organisations often work in communities with low levels of literacy, precluding written consent. Low levels of experience with technology may also make it difficult for people to understand why and how their data is being handled. Indeed, users taking biometric data need to be trained in order to be able to offer understandable answers, often through analogies, to such participants. In other cases, there is a tension between what legislation requires for consent, and what is culturally considered consent.

In one of our programmes where community health workers are fingerprinting their beneficiaries, the health workers behave in a professional, though informal, manner to help build a relationship with their beneficiaries – so reading out a consent notice written in legal jargon feels unwarranted, if not embarrassing. In practice, this means that health workers don't work towards gaining what, say, EU policy considers legal consent. They prefer to attain consent through unstructured discussion that explains why the fingerprints are being requested. In order to remain legally compliant, health workers can play an audio recording so that the legal jargon doesn't come directly from them.

• **Legal compliance**. Under European law, personal data such as biometrics can only be collected under strict conditions set out in Directive 95/46/EC – arguably the strictest, most comprehensive data protection legislation. The US takes a more decentralised approach, with legislation and regulation falling across different sectors. Regardless of legal requirements, it is ethically imperative that organisations collecting or using biometric data are proactive about security and privacy. The consequences of not doing so can be serious for the individuals involved. For example, biometric data taken for a health programme could fall into the hands of a micro-finance institution that decides to exclude individuals from financial services based on their health.

At the other extreme, there are nightmare scenarios where biometric data is used to determine an individual's ethnicity in violent campaigns. For this reason, we strongly recommend conducting privacy impact assessments for all projects. We also believe organisations deploying biometrics for international development should consider forming an independent oversight council composed of human rights lawyers, security experts and data protection specialists to regularly review privacy and security policies and offer advice.

Conclusion

While much can be done to improve biometrics for development, what is certain is that its usage will continue to grow exponentially. The identification gap and its impact on livelihoods is being increasingly recognised, and the pervasiveness and falling costs of biometric systems will make them more and more accessible to everyone, from grassroots NGOs to governments. But first we need to redesign systems with the people who use them in mind. Beneficiaries in developing countries are likelier to have worn, scarred, burned or otherwise damaged fingerprints that make biometric identification difficult unless systems are designed with this consideration in mind. Second, we must take into account the technical challenges of using biometrics for development. The lack of advanced infrastructure, intermittent connectivity, constrained budgets and other barriers must be incorporated into system design. Finally, the security and privacy of the beneficiary is paramount, and adherence to exemplary privacy and security principals beyond legislation militate against the risk of data abuse.

We have an opportunity to set the bar high in terms of the accuracy and transparency of biometric ID systems, and how to maximise the good they bring and minimise potential harm. The recommendations outlined here may not be easy to implement, but we believe they will go a long way toward improving and saving lives.

About the authors

Daniel Storisteanu is a Gates Scholar and Research Fellow at Darwin College, University of Cambridge. He is a co-founder of Simprints together with Toby Norman, who has a PhD in Management from Cambridge. Both are listed as Forbes 30 Under 30 Social Entrepreneurs. Alain Labrique is the founding executive director of Johns Hopkins University Global mHealth Initiative and Fellow at NIH mHealth Summer Institute. Alexandra Grigore is also a co-founder of Simprints and has a PhD in Nanoscience. She is among the top 200 Movers & Shakers in BioTech. The authors would like to thank Saving Lives at Birth: A Grand Challenge for Development for funding.

References

1. 'Identification for Development: The Biometrics Revolution – Working Paper 315'. Alan Gelb, Julia Clark. Center for Global Development, 28 January 2013. http://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315
2. 'Birth registration: Right from the start'. Marta Santos Pais. UNICEF Innocenti Digest No. 9, March 2002. https://www.unicef-irc.org/publications/pdf/digest9e.pdf
3. Labrique, Alain B et al. 'Pregnancy registration systems can enhance health systems, increase accountability and reduce mortality'. Reproductive Health Matters, Volume 20, Issue 39 (2012): Pages 113-117. http://www.rhm-elsevier.com/article/S0968-8080(12)39631-6/fulltext
4. 'The 'Rights' Start to Life: A statistical analysis of birth registration'. UNICEF, February 2005. http://www.unicef.org/publications/index_25248.html
5. 'The data revolution: finding the missing millions'. Elizabeth Stuart et al. Overseas Development Institute, April 2015. https://www.odi.org/publications/9476-data-revolution-finding-missing-millions
6. Norman, T, Prabhu, JC, Yunus, FM. 'Does Empathy Improve Marketing Performance? The Role of Cognitive versus Emotional Empathy in High Autonomy Sales Environments'. Cambridge, University of Cambridge Library, 2016.
7. Jain, Anil, Ross, Arun A, Nandakumar, Karthik. 'Introduction to Biometrics'. Springer US, 2011.
8. Jain, Anil et al. 'Giving Infants an Identity: Fingerprint Sensing and Recognition'. Michigan State University (2016): Pages 2-5. http://biometrics.cse.msu.edu/Publications/Fingerprint/Jainetal_GivingInfantsanIdentity_ICTD2016.pdf
9. Storisteanu, Daniel et al. 'Biometric Fingerprint System to Enable Rapid and Accurate Identification of Beneficiaries'. Global Health: Science and Practice, Volume 3, Issue 1 (2015): Pages135-137. http://dx.doi.org/10.9745/GHSP-D-15-00010
10. 'Fingerprinting Individuals in the KEMRI/CDC Health and Demographic Surveillance System (HDSS), Western Kenya, 2010'. V Were et al. INDEPTH Network, 2011. http://www.indepth-network.org/ISC%202011/presentations/Tuesday/HDSS%20FINGERPRINTING%20PRESENTATION_Victor%20Were.pdf
11. 'Perception and Acceptance of Fingerprint Biometric Technology'. Rosa R Heckle, Andrew S Patrick, Ant Ozok. Symposium On Usable Privacy and Security, 2007. http://cups.cs.cmu.edu/soups/2007/posters/p153_heckle.

How the biometrics industry can help stop child abuse


Tim Ring

Tim Ring, BTT

October's 'Biometrics 2016' conference in London featured an extraordinary session where experts in child protection (see box) appealed for help from the biometrics profession to combat child sexual abuse. The disturbing scale of the task was set out by special agent Jim Cole, head of the US Department of Homeland Security (DHS) victim identification programme, who told the conference that a staggering 185,000,000 child abuse images and videos have been seized in the US since 2002, with around 5,000 new files found every week. "It's a shocking number that most people are unaware of," he says.

The material is also shocking. "We're talking about brutal sexual assaults of infants, toddlers, by and large pre-pubescent children," Cole says. These images are being shared by offenders who increasingly use 'anonymised' technology: the DHS has identified over 50 Darknet boards whose sole purpose is to