GAME CHANGER?

5G is going to radically change the way we think about digital services, access and security.
Delighted to be back

We are delighted – and excited – to be at Mobile World Congress for another edition. Many of the big themes at MWC are already reflected in our articles in this issue of The Review. Our cover feature considers the transformational effect of 5G – for providers and customers – and the new security challenges that this will bring.

In ‘Connected Consumers’, we explore the possibilities that could open up for users when 5G meets the eSIM. Experts predict that this could “power an explosion of efficient, robust and affordable” connected devices. Mass adoption, however, will depend on usability and security.

Biometric security continues to be an important part of our offering, so we’re pleased to have been able to speak to Isabelle Moeller, the Chief Executive of the Biometrics Institute, for this issue. Read our profile of Isabelle to find out how the Institute is providing leadership in an emerging sector.

With the increasing adoption of biometrics, regulators have brought this data under the remit of new EU General Data Protection Regulation. Read our article on the consequences of data breaches under this new regime and how you can make your organizations more robust against attacks.

Many of you will have heard that in December 2017 Thales put in a bid to acquire our company, which was unanimously recommended by our Board of Directors. We believe that this offer is in the best interests of Gemalto, the sustainable success of our business, clients, employees, shareholders and other stakeholders. We expect the deal to close in the second half of 2018. Until then, Gemalto will maintain business as usual – delivering best-in-class digital security solutions.

I hope you find plenty in this issue to help you continue to build technologically advanced and secure organisations.

Enjoy the read.

Philippe Vallée
CEO
Gemalto

Contributors
Nicholas Booth
Nicholas worked in IT support within the health, financial services and public sectors before becoming an IT journalist.

Adam Oxford
South Africa-based Adam has been a technology journalist for the past 15 years, writing for titles across the world.

Tim Green
Tim was a senior analyst at Screen Digest before launching B2B title Mobile Entertainment in 2005.

Susan Anthony
After more than 25 years as an equity analyst following technology stocks, Susan is now a freelance commentator and blogger.

David Howell
David reports on technology and computing. He also works as a consultant to small businesses moving online.

Tamsin Oxford
A journalist and editor for nearly 20 years, Tamsin specializes in IT and has edited titles such as PC World.

James Hayes
James is a former Senior Editor of the flagship magazine of the Institution of Engineering and Technology.

Adam Oxford
South Africa-based Adam has been a technology journalist for the past 15 years, writing for titles across the world.

Tim Green
Tim was a senior analyst at Screen Digest before launching B2B title Mobile Entertainment in 2005.

Susan Anthony
After more than 25 years as an equity analyst following technology stocks, Susan is now a freelance commentator and blogger.

David Howell
David reports on technology and computing. He also works as a consultant to small businesses moving online.

Tamsin Oxford
A journalist and editor for nearly 20 years, Tamsin specializes in IT and has edited titles such as PC World.

James Hayes
James is a former Senior Editor of the flagship magazine of the Institution of Engineering and Technology.
In this issue...

4 DIGITAL DIGEST
National cryptocurrencies, driverless taxis, paying with wearables, plus more

8 INNOVATION
The gigabit society
5G will cause a major paradigm shift for mobile network operators, and change how services are delivered

14 SOCIETY
How biometrics strengthens the hand of law enforcement
To stay one step ahead of the criminals, supporting infrastructures will need to keep up with biometrics technology itself

18 INNOVATION
Software is a service
How the traditional pathways to technology solutions have changed

20 FIRST PERSON
The perfect fit
Isabelle Moeller, Chief Executive of the Biometrics Institute, on providing leadership in a developing sector

24 SOCIETY
In safe hands
The EU’s incoming eIDAS regulations will provide secure digital identities for consumers and ease cross-border trade for businesses

27 INSPIRATION
Securing the mobile revolution
The mobile banking sector is booming in Africa, but could certain phone technologies be putting consumers at risk?

30 DIGITAL PLANET
The world’s smartest cities
A 760mph/1225kph train and an electric car-sharing scheme are enabling smarter city living

32 SOCIETY
Getting ready for GDPR
Will a new EU data protection regulation fortify the safeguards around personal data?

34 INNOVATION
Connected consumers
Pairing the eSIM with 5G could trigger a revolution in standalone connected devices

38 EARLY ADOPTERS
Digitally driven
Early results from a digital driver’s license pilot suggest the eDocument has been a big hit with users

Read more online

› For more on the latest trends in technology and digital security, visit The Review’s online partner, /review, at gemalto.com/review
For us, virtualization and the new architecture that is designed around it is the major revolutionary aspect of 5G, which is otherwise more evolutionary“

MICHELE ZARRI, TECHNICAL DIRECTOR, GSMA

Read more on page 8

China’s digital social security card

China’s government is joining forces with WeChat operator Tencent to digitize social security cards on the mobile messaging, social media and payments platform.

Citizens will be able to use their electronic social security cards to supply official identification information to authorities and companies when making online enquiries about benefits and insurance coverage. They will also be able to apply for government services or even check into hotels without having to carry a physical ID card.

Future plans for the eID include introducing a payment function so that users can pay their medical bills quickly and efficiently by scanning a QR code at payment terminals.

Facial recognition technology will be used to verify the identity of applicants before their virtual ID cards are authorized. China’s government hopes the initiative will deter online identity theft.

WeChat currently has 980 million monthly active users in China. Chan Ka-keung, a professor at the Hong Kong University of Science and Technology, said in a recent industry forum that Chinese consumers have enthusiastically embraced new technology and have had no issues about sharing relevant data with trusted service providers, such as those in online search, eCommerce and social media.

The digital social security card initiative is currently being trialled in 26 cities across China, including tech capital and home of Tencent, Shenzhen.

Source: scmp.com

2018’S TOP 10 TECH PREDICTIONS

Amazon and Facebook will bid for sporting rights
The tech giants will enter the bidding war for the rights to stream English Premier League matches.

Social payments will be available to the masses
Apple and Facebook will drive the market for social media transfer of money to a person or business.

Blockchain will power fintech and insurance solutions
The tech will be used in new areas such as money transfer and payments, insurance and ID verification.

Edge computing will fast track the IoT
Edge computing will help IoT providers deliver bigger, better, faster services.

Facial recognition applications will surge
Shoppers’ sex and age will be determined to target them with recommendations from available inventory.

The rise of robo-advisers and app-based investments
With AI-influenced fintech services, investors might just wave goodbye to their financial planner.

Verifying your identity
Machine learning and smartphone connectivity will create and verify your digital identity.

Chinese eCards and wallets achieve scale in the West
China’s eCard and wallet providers will partner with European and US firms to cater for Chinese tourists.

Smart toys will educate the masses
Educationally-focused toys, with an emphasis on coding, will hit the mainstream.

Wireless charging market moves up a gear
In a two-speed market, Qi will be used for wearables, small devices and smartphones, and AirFuel for large devices.

Source: juniperresearch.com
Paying with wearables

Netherlands-based ABN AMRO is to roll out an initiative to test new wearables as a payment method to 500 of the bank’s clients. During the four-month pilot, those clients selected will be provided with a ring, watch, bracelet or keyring that comes embedded with contactless payment technology.

Clients will share feedback on their experience of using the wearables through the bank’s online app so that improvements can be continuously made while the pilot scheme is running. ABN is the first bank to enable worldwide payment with a wearable that’s linked to a current account.

“As much as 50% of all payments in the Netherlands are contactless, but the rise of contactless payment doesn’t stop at bank cards and mobile phones,” says Yvonne Duits, Product Owner, Payments at ABN AMRO. “More and more products have payment through Near Field Communication, so naturally we’re eager to test this method with our clients. The current project involves a range of wearables. We care about making things convenient for consumers and offering everyone a payment method that suits their preferences.”

Source: abnamro.com

---

Retirement village gets driverless taxis

Residents of America’s largest retirement village, based in Florida, will see the world’s biggest fleet of self-driving taxis introduced onto its roads next year.

Inhabitants of The Villages will need a smartphone to summon a self-driving car, using a mobile app. The vehicles will be operated by US firm Voyage, which already runs a handful of driverless taxis in a retirement village in San José, California – one of 20 US states that have approved the use of autonomous vehicles on their roads.

Voyage is predicting “high demand” from The Villages’ 125,000 residents and has reportedly given an equity stake in the company to the owners of the retirement estate.

But if car research firm Kelley Blue Book’s figures are anything to go by, the taxis may not be a hit. It found that only 9% of those aged 51–64 said they felt confident enough to travel in a fully driverless vehicle. That age group cited safety concerns related to testing and accidents as one reason for their reluctance to use autonomous vehicles.

Source: bbc.co.uk
Biometrics has its weaknesses and so multi-factor authentication is certainly, in most cases, the way to go.”

ISABELLE MOELLER, CHIEF EXECUTIVE, BIOMETRICS INSTITUTE

Read more on page 20

Central banks ponder cryptocurrencies

The Bank of Israel is thinking of issuing a digital currency to create a faster, fee-free, payments system, according to press reports. The move would be an attempt to reduce the amount of cash in the Israeli economy, in a bid to combat the ‘black economy’, estimated to be worth 22% of the country’s national output.

As Bitcoin and other cryptocurrencies, such as Ripple and Ethereum, become more well known, economists are predicting that the technology could one day be used across a wide range of countries, where centralized banks would issue the digital currencies. This is expected to increase the scrutiny of cryptocurrencies by regulatory authorities.

However, the Bank of England (BoE) says it has put its cryptocurrency plans on hold amid fears that it could adversely impact traditional banks if consumers decided to stop using commercial bank accounts, in favor of buying goods with BoE-issued digital money. A flurry of cash withdrawals from banks in favor of a cryptocurrency is also a concern. A slowdown in cash flow could make it more difficult for high street banks to pay out loans and interest payments, and ultimately lead to collapse, creating turbulence in the wider economy, the BoE said.

Sources: reuters.com; ftadviser.com

Alipay payments at all-time high

New figures from Chinese eCommerce giant Alibaba show that 82% of transactions on its platform in 2017 were made through mobile devices. This ratio is at an all-time high, the firm says.

Around 520 million people - 37% of China’s population - use Alibaba’s payment platform, Alipay, which allows payments through computers and mobile devices.

Users in the northern province of Shanxi and the south-western province of Guizhou appear to be most reliant on the app, with mobile payments accounting for 92% of their transactions over the past year.

The growth in mobile payments has been made easier by an advance in mobile network technology. Figures from China’s Ministry of Industry and Information Technology show that 4G users account for 70% of China’s cellphone users, up from 55% as of the end of 2016. Mobile payments can also be made through 3G.

Physical cash is taking a hit from the mobile payments boom in China. Last year, Alibaba reported that the number of searches for wallets on its online shopping platform had seen a decline for the first time.

Source: ecns.cn
US trust in biometric authentication rises

Could the days of PINs and passwords in the US be over? A survey of 1,000 Americans, conducted in December 2017 and commissioned by Visa, shows that US consumers have a strong interest in the use of biometrics to protect their personal data.

In the survey, 86% of respondents said they were interested in biometrics to verify identity or make payments, while 46% believed biometrics are more secure than passwords and PINs.

“For financial institutions, the time has never been better to integrate biometric technology into banking apps and payment experiences for customers,” says Mark Nelsen, Senior Vice President of Risk and Authentication Products at Visa.

“Advances in mobile device features are increasing the accuracy and speed of biometrics, such that they can be used for financial transactions. At the same time, consumers are widely familiar and comfortable with using biometrics for more than just unlocking their phones.”

Source: visa.com

### Event calendar

Gemalto regularly participates in trade shows, seminars and events around the world. Here’s a list of those taking place in the next few months.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Sector</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 26-Mar 1</td>
<td>Mobile World Congress</td>
<td>Mobile Services &amp; IoT</td>
<td>Barcelona, Spain</td>
</tr>
<tr>
<td>Feb 27-Mar 1</td>
<td>Embedded World 2018</td>
<td>Mobile Services &amp; IoT</td>
<td>Nuremberg, Germany</td>
</tr>
<tr>
<td>Mar 13-14</td>
<td>Seamless Australasia</td>
<td>Biometrics Payments</td>
<td>Sydney, Australia</td>
</tr>
<tr>
<td>Mar 20-21</td>
<td>Telecoms Fraud &amp; Revenue Assurance</td>
<td>Mobile Services &amp; IoT</td>
<td>London, UK</td>
</tr>
<tr>
<td>Mar 20-22</td>
<td>Passenger Terminal Expo</td>
<td>Government</td>
<td>Stockholm, Sweden</td>
</tr>
<tr>
<td>Mar 21-23</td>
<td>Security Printers by Intergraf</td>
<td>Government</td>
<td>Dublin, Ireland</td>
</tr>
<tr>
<td>Mar 26-29</td>
<td>SCA Payment Summit</td>
<td>Banking &amp; Payments</td>
<td>Orlando, USA</td>
</tr>
<tr>
<td>Apr 16-20</td>
<td>RSA Conference 2018</td>
<td>Enterprise &amp; Cybersecurity</td>
<td>San Francisco, USA</td>
</tr>
<tr>
<td>Apr 18-19</td>
<td>ID at the Borders</td>
<td>Government</td>
<td>Brussels, Belgium</td>
</tr>
<tr>
<td>Apr 24-26</td>
<td>ID4Africa</td>
<td>Government</td>
<td>Abuja, Nigeria</td>
</tr>
<tr>
<td>Apr 30-May 2</td>
<td>connect:ID</td>
<td>Government</td>
<td>Washington, USA</td>
</tr>
<tr>
<td>Apr 30-May 2</td>
<td>Cardware</td>
<td>Banking &amp; Payments</td>
<td>Niagara Falls, USA</td>
</tr>
<tr>
<td>May 7-9</td>
<td>Source Media Card Forum Expo</td>
<td>Banking &amp; Payments</td>
<td>Miami, USA</td>
</tr>
<tr>
<td>May 14-17</td>
<td>AAMVA Region I Conference</td>
<td>Government</td>
<td>Wilmington, USA</td>
</tr>
<tr>
<td>Jun 3-6</td>
<td>CCMTA</td>
<td>Government</td>
<td>Quebec City, Canada</td>
</tr>
<tr>
<td>Jun 4-6</td>
<td>Money2020 Europe</td>
<td>Banking &amp; Payments</td>
<td>Amsterdam, The Netherlands</td>
</tr>
<tr>
<td>Jun 4-7</td>
<td>Gartner Security &amp; Risk Management Summit</td>
<td>Enterprise &amp; Cybersecurity</td>
<td>National Harbour, USA</td>
</tr>
<tr>
<td>Jun 5-9</td>
<td>Computex, Taipei</td>
<td>Mobile Services &amp; IoT</td>
<td>Taipei, Taiwan</td>
</tr>
<tr>
<td>Jun 6-7</td>
<td>TU Automotive</td>
<td>IoT &amp; Automotive</td>
<td>Nov, USA</td>
</tr>
<tr>
<td>Jun 18-21</td>
<td>AAMVA Region II Conference</td>
<td>Government</td>
<td>Myrtle Beach, USA</td>
</tr>
<tr>
<td>Jun 27-29</td>
<td>Mobile World Congress Shanghai</td>
<td>Mobile Services &amp; IoT</td>
<td>Shanghai, China</td>
</tr>
<tr>
<td>Aug 4-9</td>
<td>Black Hat</td>
<td>Enterprise &amp; Cybersecurity</td>
<td>Las Vegas, USA</td>
</tr>
<tr>
<td>Aug 21-23</td>
<td>AAMVA International Conference</td>
<td>Government</td>
<td>Philadelphia, USA</td>
</tr>
<tr>
<td>Aug 26-30</td>
<td>VMworld</td>
<td>Enterprise &amp; Cybersecurity</td>
<td>Las Vegas, USA</td>
</tr>
<tr>
<td>Sep 7-12</td>
<td>AAMVA Region IV</td>
<td>Government</td>
<td>Big Sky, USA</td>
</tr>
</tbody>
</table>
5G will radically alter how next-generation mobile data services are delivered, fundamentally changing our thinking about service access, security and how data is managed and distributed.

THE GIGABIT SOCIETY

Last year, Netflix alone was responsible for over a third of all the downstream traffic over the internet across all of North America, according to figures compiled by statistics portal Statista. It’s evidence, if any were needed, that data, and the ability to move vast quantities of it to and from digital devices, is now defining what mobile networks need to be of service their customers.

As networks have developed from 2G (launched in Finland in 1991) to 4G (launched in the US in 2010), the focus has been on the ability to handle increasing amounts of data and delivery speed. When 5G arrives in 2020, better performance will be part of what it will deliver. However, it will also usher in bigger changes to how and where data is stored, and how this is delivered to customers and the countless number of devices that will be connected using this network.

Operators will see a shift in their role from providers of voice services to hosts for not only vast quantities of data, but also the applications that rely upon this information. The rapidly expanding autonomous vehicle industry will be one of the first to exploit 5G networks. Entertainment services will also see rapid expansion, and the digital infrastructure of cities will enable them to deliver advanced services to their inhabitants. And as machine learning and artificial intelligence (AI) expands in every sector from healthcare to retail, 5G is vital to ensure these new applications have the network capacity they need.

For example, 5G will enable the realization of the smart city vision, in which multiple types of data are collected about things such as air quality and the number of cars and pedestrians on the road. Then, AI and machine learning is used to automate decisions to improve the quality of life for residents – for example, redirecting the traffic flow of autonomous vehicles to avoid polluted and congested areas.

5G will of course deliver faster networks, but also the development of intelligent networks that are increasingly decentralized and able to react to the needs of individual users. 5G is a completely new way to securely manage access to data over multi-access edge networks. These networks feature multiple cloud-based IT environments that exist at the edge of a cellular network, and which allow mobile network operators to deliver services closer to their customers, reducing network congestion and improving the performance of applications. As 5G networks proliferate, the channels for potential attack will also expand. 5G and its operators will enter a new age of data and network security, which will need new approaches to ensure the network infrastructure and the data it carries is secure.

The Next Generation Mobile Networks (NGMN) Alliance defines 5G as “an end-to-end ecosystem to enable a fully mobile and connected society. It empowers value creation toward customers and partners, through existing and emerging use cases, delivered with consistent experience, and enabled by sustainable business models.” 5G is not being built as a standalone radio network technology, but rather as an open platform enabling digital transformation.
It does this by providing ubiquitous connectivity in converging licensed and unlicensed radio technologies such as LTE, NB-IoT, and Wi-Fi with its new high-speed cellular radio options.

**A FLATTER NETWORK**

The current network infrastructure is extremely hierarchical, with devices connected to content that can often reside in distant servers, resulting in slow connections and high latency. 5G moves away from this to create a flatter network that can deliver advanced and integrated user experiences. In addition, functionality shifts from hardware to software. This means that many of today’s hardware servers will be replaced with virtual servers that can be thought of as building blocks that can be grouped together to deliver specific services.

In addition, these virtual servers can be used with Software Defined Networks (SDN) to create ‘network slicing’. Network slicing creates virtual ‘slices’ within a single physical network. When it comes to levels of data being used and the speed at which that data is required, users have different needs. Network slicing allows operators to cater for those different needs via different slices within the same network. Put simply, it delivers highly flexible and agile networks that can adapt to users’ needs and data demands.

Paul Bradley, Head of 5G Strategy and Partnerships at Gemalto, explains: “The fundamental component of 5G is the virtualization of the network. That means in practice that the current physical servers that the telcos have been deploying to make up a network service move to virtual functions that can be run on generic server boxes. The other main component of 5G is that the virtualized functions making up a network service will exist in centralized data centers and, more importantly, will also exist on the edge of the network. What this means in practice is that services that require low latency, such as gaming and autonomous vehicle tracking, will be possible and will have excellent performance because the network and its data is localized.”

Michele Zarri, Technical Director of GSMA, the global trade body for mobile network operators, agrees that the critical development will be in virtualization and the ability to do network slicing, because this allows mobile operators to generate multiple types of networks from the same infrastructure and support multiple types of businesses associated with them.

“For us,” says Zarri, “virtualization and the new architecture that is designed around it is the major revolutionary aspect of 5G, which is otherwise more evolutionary. Virtualization and network slicing will help to deliver value across a wide range of verticals, such as automotive, energy and finance. Each vertical will have its own independent network, which is customized according to its needs. For example, an IoT sensor in a package delivered by a courier company may indicate where the package is until it is delivered and then trigger an alert once it’s opened. The amount of data and frequency needed for this would not be high, nor would the latency requirement be an important consideration. However, an autonomous vehicle would need to be alerted in real time about an accident ahead so that it can anticipate the appropriate emergency stopping time. This will require a medium amount of data bandwidth and low latency.

The multi-layered approach to networks is at the heart of what 5G will deliver. Ericsson and DoCoMo, for instance, have already shown how network slicing...
can support augmented reality applications, as well as voice and data exchange across the same network.

5G will need a new approach to how networks are constructed. This Slice-aaaS (Slice-as-a-Service) was discussed at the GSMA’s Mobile World Congress Americas in San Francisco in September 2017. Speaking at the Future Networks Seminar, Doug Eng, Technical Architect of Wireless Network Architecture and Design at AT&T, explained: “At AT&T, we’ve been selling around 4,000 different business packages with 3G and 4G. When 5G arrives, we think we can drastically reduce that number.”

Developing the 5G network is being driven by key use cases. There will be three phases to the rollout of 5G. The first is to meet the core use cases, to enhance mobile broadband. This is clearly the focus for the entire industry, as more efficient data delivery is being driven by consumer need. The second phase is the ultra-reliable and low latency services needed by autonomous vehicles and networks for the emergency services. The last phase is to support the Internet of Things (IoT). This is last because the IoT already has a number of communications platforms that can service it, so it’s not a priority for 5G development.

DATA ON THE EDGE

The decentralization of data is already happening as customer demand and behavior changes. The US is witnessing the creation of ‘edge data centers’ that are designed to extend the reach of centralized data centers, to improve overall performance and delivery of services to customers outside of large urban areas.

Whereas the main data concentrations today are in cities such as New York or San Francisco, which have continued to push to improve bandwidth, in a 5G environment, the ‘edge’ becomes the focus for data delivery to end users who don’t live in large cities that have well developed broadband and cellular connections.

Companies including Google (YouTube), Netflix, Akamai, Facebook, Apple, Amazon and Microsoft together represent 80% of all internet traffic.

It’s a fundamental concept that 5G will be as inclusive as possible and support the UN’s Sustainable Development Goals

PERVASIVE SECURITY

The arrival of 5G will enable new innovations in the automotive and healthcare sectors, with many industries leveraging the IoT to deliver new products and services. But how secure will they be?

Gemalto’s Paul Bradley, Head of 5G Strategy and Partnerships, says: “With 5G, the security landscape changes. The move to edge data centers will require a different approach to security.”

As a core component of the networks forming the foundation of 5G is open flexibility based on Software Defined Networks and Network Function Virtualization, the security these networks require must evolve. With more use of virtualization in particular, security protocols will have to improve. They must detect anomalies, stop malware and include intelligent DNS to prevent incidents such as the Mirai botnet attacks last year. With the IoT exponentially increasing the potential access points for malicious code to enter networks, secure connections become vital.

In its 5G security whitepaper, mobile operator Ericsson explains: "A multi-stakeholder approach involving operators, vendors, regulators, policymakers and representatives of 5G users ... is fundamental to the security baseline of trustworthy, cost-efficient and manageable 5G networks. Pre-standardization consensus building, such as joint research by the different stakeholders, will be important.”

Clearly, the threat landscape is about to radically change. The open and integrated nature of 5G requires a new kind of dynamic security that reacts second-to-second as the network is accessed by users and devices.

“Mobile operators cannot afford to let security weaknesses undermine the compelling benefits of 5G and virtualized networks,” says Bradley. "We are partnering with a major industry player to provide actors deploying cloud-based virtualized networks with all the tools necessary to address the dangers posed by network disruption or data breaches in the next phase of our connected world.”

Source: Ericsson

tinyurl.com/Ericsson-5G

According to research from Quartz. It’s plain to see how a more reactive and dynamic network is essential to maintain and expand the services these companies offer to their customers.

One of the first tangible tests of 5G – managed by Korea Telecom (KT) – was at the recent Winter Olympics in South Korea. The Games used pre-standard network infrastructure. 3GPP – a collaboration of telecommunications providers – isn’t scheduled to release the first incarnation of 5G until June 2018, which was too late for implementation at the 2018 Winter Olympics. However, the Games did
Network slicing will give businesses access to highly customized networks tailored to their very specific requirements in a cost effective, timely and efficient way.”

MICHELE ZARRI, TECHNICAL DIRECTOR, GSMA

- act as a test bed for the new platform, with 5G radio using the available LTE core network.

The current 3G/4G network is estimated to reach 59% of the global population, according to the GSMA. It’s a fundamental concept that 5G will be as inclusive as possible and support the UN’s Sustainable Development Goals. The date set for 5G to become widely available is 2020. Already, Verizon and AT&T in the USA, Japan’s NTT DoCoMo, Etisalat in the UAE, China Mobile, and KT and SK Telecom in South Korea have announced plans to support 5G with a wide range of services. 5Groningen has also established a testing area in North Groningen, Netherlands, for various 5G-related projects, from autonomous vehicles and smart ambulances to smart agriculture.

The ability to develop new network architectures is the foundation on which 5G will be built. Critical systems and communications, together with new security protocols, will converge to create a new network that can serve all its users. Gemalto calls these ‘secure chains of trust’, which ensure that each slice of the 5G network is isolated and secured for the use case. As the customer or device switches between services, they may also switch network slices. Security in a 5G environment needs to be agile and dynamic to authenticate each customer, connected device or object as their tasks change.

Simply delivering more efficient access to data will also transform many industries. Smart medicine and personalized healthcare is increasingly becoming a data-based industry. 5G will enhance many of the services already on offer, but will also create many more opportunities as services get fast and efficient access to the information they need. GlaxoSmithKline, for instance, is developing an implant that could treat arthritis and diabetes. Technologies to treat and relieve the symptoms of dementia are based on available data and need networks with the performance, reliability and availability that 5G can deliver.

Industry will be able to advance the concepts of Industry 4.0, which can become a reality with 5G networks. The 5G-Enabled Manufacturing (5GEM) project aims to explore the possibilities that 5G could deliver to industry. Funded by Vinnova, the innovation agency within the Swedish Government, Chalmers, Ericsson and SKF aim to demonstrate the powerful influence 5G can have on all areas of industry and manufacturing to realize the vision of the IIoT (Industrial Internet of Things).

Sergio Falletti, Technology Partner and Head of Mobile Specialism at DigitasLBi, says 5G’s most significant impact will come from its support for the IoT. “The rapid growth of low-power communication technologies like LoRa shows that there is already significant demand for IoT connectivity. While the standardization process is already in progress, 5G will be its culmination, acting as an enabler for IoT adoption across agriculture, transport, logistics, health and more.”

Agriculture is one of the most interesting industries that will be transformed by access to 5G networks. Vodafone already provides drone connectivity across
its 4G network. This can be used for precision farming that will be linked to other machinery, such as harvesters, that can take drone data and couple it with GPS to give farmers an unprecedented overview. 5G will make these connections more robust, more reliable and faster.

The burgeoning autonomous vehicle industry will be one of the first mass-market examples of 5G in action. In Germany, Vodafone is testing vehicle-to-vehicle communications along the A9 between Munich and Ingolstadt. The test currently uses 4G, but will see major enhancements once 5G becomes widely available. Autonomous vehicle development is a focus of the transport industry, but 5G offers the ability to create communications networks that become dynamic, reacting to changing driving conditions. If you add AI to further analyze the information available, predictive systems then become a reality for all drivers, enhancing their journeys.

**OMNIPRESENT CONNECTIVITY**

The GSMA expects 5G connections to reach 1.2 billion, some 12% of total mobile connections, by 2025 and overall operator revenues to grow at a CAGR of 2.5% to reach US$1.3 trillion in the same year. The GSMA’s aspiration is for 5G to drive annual growth to 5%. The greater affordability of smartphone handsets, all of which are mobile broadband capable, will further drive the expansion of the 5G network.

Whether you’re supporting entertainment streaming services, which show no sign of slowing their growth, or new products and services that require fast and localized data centers, or whether you’re doing something else, 5G is a new way of thinking about the data that needs to be exchanged. When 5G networks are considered, they are highly modular. The use of CDNs (Content Distribution Networks) is well understood. However, under 5G, the concept of localizing content access goes much further.

GSMA’s Zarri says: “Network slicing will give businesses access to highly customized networks tailored to their very specific requirements in a cost effective, timely and efficient way. It will mean that they can also have the potential to optimize their current services and create new offers that otherwise wouldn’t have been possible. Businesses need to get ready to take advantage of these opportunities.”

The Winter Olympics in 2018 were the first major test of pre-standardized 5G technologies. At the moment, apart from the initial phase of ‘early drop’ releases to enable limited scale pilots based on some existing core network infrastructure, standards have not yet been clearly defined and accepted. Many of the incumbents in the telecoms sector are pushing forward with their own trials. The promise of 5G needs to be met with realistic targets for spectrum allocation and the need for an integrated approach to how the underlying network that 5G represents is commissioned, and then implemented. The usage scenarios will drive the initial rollout of 5G.

The expectations for 5G are high. Pre-standard testing is already under way, with formal specifications commercialized from 2019. 5G isn’t just the evolution of 4G. Several technologies are being developed in parallel to deliver the high performance at low latency that 5G demands. The 4G radio interface (LTE-Advanced Pro) is likely to be used to provide a coverage layer via macro cells, with a new cellular radio interface being developed by 3GPP to deliver the high data rates needed based on their initial Release 15 specification. The agility 5G will deliver marks a watershed moment for mobile communications, across multiple industries from transport to healthcare.
Biometrics are helping law enforcers to keep one step ahead of increasingly sophisticated criminals. To retain this upper hand, supporting infrastructure will need to advance as fast as the technology itself.

**HOW BIOMETRICS STRENGTHEN THE HAND OF LAW ENFORCEMENT**

When the world’s populations mostly lived in rural communities, there were no official police forces. There was still crime, but since everyone knew each other, identification was less of a problem. The Industrial Revolution changed the nature of society and had strangers living alongside each other in an urban world. Police forces emerged as a necessity and they faced a challenge in identifying citizens. Amazingly, more than two centuries later, police are still facing the same challenge, but it has been exacerbated by the anonymity of the online world.

The unique characteristics of each person’s body have long been recognized as a potential identity provider. The Chinese first identified the palmprint as a form of unique identifier 3,000 years ago. In 1858 Sir William Herschel, a British Civil Servant working in India, conceived the first systematic capture of hand images for identification purposes. This invention led to the fingerprint principles that are still used today. However, it was shunned for several decades in favor of an anthropometrics system, which identified people by detailed records of their body measurements, physical descriptions and photographs. This system, whose foundation logic was that no two people have the same body measurements, was later discredited in an incident involving twins. This highlights the challenges of biometrics: the invention of options for verification and, equally crucially, the creation of the systems to support these incredible inventions.

Today, there is a plethora of biometric techniques used for identification. There are many aspects of humanity that are unique to each individual and there are now machines that can identify faces, gaits, gestures, irises, veins, signatures and voices. Analysis of DNA is also a crucial biometric for crime detection, but not for crime prevention. Yet. The key to mass adoption is the storage and management of the data that describes each unique human characteristic.

**DETECTION AND DETERRENT**

The effect of the rollout of finger detection and management systems in San Francisco, California exemplifies this. In the 1980s, the volume of fingerprints being taken had grown to exceed the storage capacity of these millions of physical records. In December 1983, the Federal Bureau of Investigation (FBI) awarded a contract to create an IT management system that could automate the process of comparing a fingerprint from a crime scene with the millions of records on a database. The Automation Fingerprint Identification System (AFIS) was born.
When this system was bedded in and began to work to its fullest efficiency, the impact on crime detection was immediate. As word spread among criminals, it had a dramatic deterrent effect too.

A statistical study of AFIS positive identifications against burglaries in San Francisco, for the period 1984 to 1988, showed that there was a 10-fold increase in latent print identifications in 1984. As a result, the local district attorney demanded and got five new positions to prosecute the AFIS cases. The knock-on effect of this was that the conviction rate in AFIS-generated burglary cases was three times higher than in burglary cases without this type of evidence.

As conviction rates went up, the number of burglaries in San Francisco fell dramatically. FBI figures show a steady decrease from 6,700 in six months up to December 1984, to 4,500 by December 1987. Overall, there was a 26% decrease in the number of burglaries over four years.

Biometric-based crime detection techniques continue to be refined into more effective evidence-gathering systems. In 2008, the Urban Institute’s Justice Policy Center in the US found that analyzing DNA evidence from property crime scenes helped identify suspects in twice as many cases, yielded twice as many arrests and led to twice the number of convictions.
successful prosecutions compared with cases built on traditional eyewitness identification and fingerprints. Processing a case with DNA evidence costs less too.

**BIG DATA CHALLENGE**
Managing biometrics is a big data problem that typically involves high volume, large databases and high accuracy, says Simon Pei, head of biometrics product management for Gemalto. This means managing and mining millions of data records at top speed and with high accuracy.

There is also constant pressure to improve the quality control of the systems. For prints, for example, quality control is ensured during capture by examining the quality of fingerprint images and prompting operators to retake them in real time.

“Using multiple records per subject, and using both rolled fingerprints and flat fingerprints, can increase the potential latent search accuracy,” says Pei.

It’s one thing to match prints from a suspect against the database, but a different matter to take a “scene of crime” partial mark, says Quocirca security analyst Rob Bamforth, who helped integrate automated fingerprint recognition systems for London’s Metropolitan Police in the late 1980s and 90s.

With joined-up data, more could be done. This is where big data will play a bigger role. More data will be fed into an evidence database and this will increase the scope for other non-static biometrics such as facial recognition and gait analysis (which judges us by our posture and walking style) to be used in conjunction with “scene of crime” data.

**A HISTORY OF BIOMETRICS IN LAW ENFORCEMENT**

- **1858**
  First systematic capture of hand images for identification

- **1903**
  New York State Prisons begin using fingerprints

- **1969**
  FBI pushes to make fingerprint recognition an automated process
For more on how biometrics is helping law enforcement officers, visit tinyurl.com/Paraguay-murder-case

HURDLES AHEAD
Moving toward such integration will not be without its difficulties. One of the emerging challenges of the biometric security age is how to manage the masses of data created by all these records. Given the complexity of the information recorded on each measurement taken of a person’s biometrics – fingerprint data must be able to accurately reproduce a model with ridges and bifurcations – it follows that each record is sizeable. And given that agencies will have tens of millions of records, there will be considerable storage, management and integration challenges. The US entry-exit system, for example, captures over 200,000 fingerprints on a daily basis to check against 200 million existing records. In addition to fingerprints, there will be DNA records, iris scans, signature and gait measurements stored.

In light of this, compromises and choices about the way that data is stored and managed will inevitably have to be made. “Costs are still big constraints for government agencies,” says Pei. An entire sub-sector of the security software industry has evolved to rationalize the cost by constantly fine-tuning the processes of the vast machinery that must support all this big data processing.

The makers of these systems must also adapt to national agencies’ desire to share information and embrace fast-changing standards, says Pei. These will be specified not just by national standards bodies such as the US National Institute of Standards and Technology, but also by the specifications from national agencies such as the FBI or Canada’s Royal Canadian Mounted Police or the European Union-wide “Prüm Convention” for sharing biometrics information across multiple national police forces.

And then there are new data protection laws on the horizon to consider. The EU General Data Protection Regulation (GDPR), which comes into force on 25 May 2018, will require data breaches to be reported to a national supervisory authority and to the individuals affected within 72 hours of the breach detection. All organizations holding or processing data on EU citizens must comply with GDPR and failure to do so could result in fines of up to €20 million (see page 32 for more).

As companies wrestle with these and other considerable networking, processing and storage management challenges, the evolution of biometrics continues apace. In the near future we will be protected by even greater levels of authentication, created by new multi-modal systems that can cohesively fuse different disciplines, such as facial recognition and surveillance. Data encryption will bring an added layer of security to these vast and growing databases. And inputs into the security database will be more frequent, with the emergence of more user-friendly systems using touchless fingerprint scanners and mobile biometric devices.

Society is getting more complicated now too, says Bamforth. “In the old days, crimes were normally committed within a known locale and with fixed modus operandi.” As criminality and biometrics get more advanced, for the latter to keep the upper hand, its supporting infrastructures must retain their ability to handle high-volume, large databases with high accuracy.

CASE STUDY
PARAGUAY NATIONAL POLICE FORCE
In an extraordinary case in Paraguay, a killer was identified solely through a picture of his palm, not even a palmprint. The case involved the inexplicable murder of two men, aged 20 and 22, who were shot dead in the city of San Estanislao. Officers recovered a cell phone belonging to one of the victims and forensic experts began listing all his phone calls. One of the photos on a popular messaging app showed a quantity of marijuana held in an open hand. Police guessed the drug dealer must have sent the picture to prove he had the “merchandise”. Incredibly, the National Police’s Human Identity Division in the capital, Asunción, managed to zoom in on the picture and obtain an image of the dealer’s prints. When entered into a Gemalto Cogent AFIS (Automated Fingerprint Identification System), which holds seven million records, a positive identification was achieved in minutes.

Using multiple records per subject, and using both rolled fingerprints and flat fingerprints, can increase the potential latent search accuracy.”

SIMON PEI, HEAD OF BIOMETRICS PRODUCT MANAGEMENT, GEMALTO
Technology solutions have undergone a metamorphosis, from product to software to as-a-Service

SOFTWARE IS A SERVICE

The solid weight of the product that used to land heavily on business desks, especially within the business-to-business (B2B) environment, has evolved into an elegant ecosystem of as-a-Service (aaS) models and solutions. The Software-as-a-Service (SaaS) market has seen steady growth over the past few years. The IDC FutureScape: Worldwide Software Business Models and Monetization 2017 Top 10 Predictions report states that, by 2019, more than 50% of all industries will price and package their offerings as services with flexible subscription or consumption-based pricing models. The traditional pathways to product and technology have changed, and the benefits to the business in terms of accessibility, flexibility and cost indicate that this trend is not going anywhere anytime soon.

These significant changes have been driven by innovation, says Mervin Miemoukanda, Senior Research Analyst, Software and Market Intelligence at International Data
Corporation. “This has led businesses to develop completely different software architectures and user interfaces. From an aaS perspective, software development has undergone a range of changes, from new tools to techniques and languages. In a sense, the cloud is a way to automate the deployment phase of software development.”

**MIMICKING THE CUSTOMER EXPERIENCE**

The consumer world played no small part in the change from the use of tangible product to the on-demand flexibility of aaS. The ubiquity of the smartphone and consumer adoption of the tools it enables, and the access it provides, has triggered the demand for solutions that can be accessed anywhere at any time.

“Hind shift in how the world engages with software took place around 10 years ago,” says Ariella Shoham, Senior Director of Marketing for Software Monetization at Gemalto. “The business world started to mimic the customer experience, taking the enterprise application from on-premise solution to the connected cloud, driven by workforce demands for better connectivity, engagement and interaction.”

The ability to work from anywhere not only boosts productivity and puts the employee online 24/7, it also allows for the organization to fine-tune capacity and spend. It takes away the reliance on the hardware requirements within the enterprise, as the applications that used to depend on a specific machine in order to operate are now sitting in the cloud and can be used on any device. The operating expenditure advantages of the aaS model far outweigh having hardware on site.

“SaaS as a delivery model has allowed more businesses, be they small or large, to save money on the acquisition of hardware such as servers and storage,” adds Miemoukanda. “Before the advent of SaaS, businesses would have to purchase software from specific vendors and pay annual licensing and maintenance fees. With the SaaS model, companies acquire software on a per-user basis or as a subscription model. Another key benefit is the ability to use the service a business needs any time and anywhere.”

**BUSINESS DEVELOPMENT OPPORTUNITIES**

The ways in which people are consuming software are not just redefining how software is used, but also creating more opportunities for businesses to develop different routes for the consumption of software. For the seller, the “once done” approach to dropping off a box has transformed into the “always connected” approach. Instead of calling once every two years to renew a license, the seller can use data and insights around SaaS to provide advice and support. What is the business using the most? What is it using less? Which people and departments are more inclined to use specific solutions versus others? Within this approach to customer service, there lies the ability to develop new revenue streams and drive richer engagement.

"SaaS reduces the initial cost barriers to entry, especially for smaller organizations that can now deploy and use many of the advanced features and products that would have previously been overly complex and costly for them to deploy,” adds George Amoils, Cloud Advisor at Cloud Essentials, global cloud migration specialists. “The other factor to consider is the pace at which technology is changing; organizations need to be in a position to change and keep up to date. SaaS allows the organization to be way more flexible and able to adapt to change.”

There is also a move toward a relationship mentality, as opposed to a ‘sold once’ mentality, which benefits both the business and the customer. For the user, there is immediate access. They don’t want to wait to have their software enabled; they want what they need, right now. And they’re happy to pay for the convenience.

“We live in the age of instant gratification for the consumer and the business,” says Shoham. “This means that the ways in which software is monetized and managed have to change. The business user wants to pay per consumption and the software provider has to create models that allow for this.”

**SOFTWARE’S FOUR PILLARS**

Software licensing still drives the SaaS model, but it can’t adhere to rigid forms that end up alienating the customer and impacting the budget. The protection that software licensing provides is important; it’s just not everything. Instead, it needs to be seen as a way to maximize value and overall profitability. The new way of looking at software places it on four pillars – security, packaging, management and tracking. These tools allow you to seamlessly create new packaging to reach new market segments, to manage back office functionality with greater efficiency and accuracy, and to use data to optimize product roadmaps and business strategies.

With SaaS, technology solutions providers can create value where it hasn’t existed before. They can develop new ways of meeting client demand, on demand, and fundamentally change the ways in which solutions and services are consumed.  ■
Isabelle Moeller’s background in marketing and events has been invaluable in helping the Biometrics Institute raise its profile and provide leadership in this growing sector.
When Isabelle Moeller applied for a job to lead the Biometrics Institute, preparing for the interview was tricky. It was 2002 and Googling 'biometrics' didn’t get you very far. Today, thanks to ePassports and smartphones that unlock using fingerprint and voice recognition technology, everyone is increasingly familiar with the world of biometrics.

In that time, Moeller has moved from General Manager to Chief Executive, growing the Institute from 10 founding member organizations to over 230 and making it “the place to go to learn and know about biometrics”. Last October, the Security Industry Association recognized Moeller’s contribution to the sector by naming her one of five winners of the 2017 Women in Biometrics Awards. The global awards annually honor the work of female leaders helping to drive the biometric identity and security industry forward.

For the uninitiated, she certainly makes the technology sound exciting. “Biometrics are quite cool,” she says. “They’re a bit magical, in a way. A door might open if you put your fingerprint on it.”

SERVING A NEED
The Biometrics Institute was set up in 2001 in Australia, which, at the time, was experiencing a tourist boom. As visitor numbers increased, the Australian government began looking for ways to easily manage passenger flows in and out of the country’s airports. Biometrics was one solution, but there was a need to better understand how this technology worked and could be tested.

“The founder of the Biometrics Institute, Dr Ted Dunstone, had the foresight to realize that there was a need for this very new industry to have a place to come together,” says Moeller. “He was able to secure funding through the Australian government to establish this organization to provide a platform for the industry to learn and share knowledge and experience about what was quite a new technology.”

The Institute’s founding members were government agencies, such as immigration and customs services, the police and some suppliers of biometrics technology. Today, the Institute has grown into an international membership body that has expanded to include businesses from financial services, the aviation industry and the privacy community, as well as academics involved in research and development in biometrics.

Throughout this time, the Institute’s objective – to promote the responsible use of biometrics through guidance and best practice – has remained constant. “Often, legislation can’t keep up,” says Moeller. “The technology is moving so fast that it’s very difficult to provide the right framework in time. Standards take a long time to develop, so in the meantime there’s a need to help organizations understand how we implement this technology. What does it mean if we collect people’s data? How do we store that information securely? What else do we need to consider? These are the types of questions we’re seeking to answer on a day-to-day basis.”

LEADING THE WAY
With a background in marketing and events, Moeller might seem like an unusual choice to run an industry body for the technology sector. But she was actually the perfect fit for an institute that was just starting out and in need of a leader who could recruit members, organize meetings and training courses, and keep a growing and diverse membership updated with the latest news and developments about the body.

Having previously worked in an events sector that was focused on eCommerce and mobile, she wasn’t a complete stranger to the tech world, but she admits that getting to grips with biometrics was a steep learning curve and one made all the more difficult by a lack of information and public suspicion about this emerging technology.

RÉSUMÉ: ISABELLE MOELLER

2017 Named one of five winners of the global 2017 Women in Biometrics Awards, held by the Security Industry Association

2011 Appointed Chief Executive of the Biometrics Institute; relocates to London, UK

2002 Joins the Biometrics Institute as General Manager, based in Sydney, Australia

1998 Appointed Senior Conference Manager for The Economist Conferences in London, UK

1996 Joins AIC Conferences (now Terrapinn) in Frankfurt, Germany and London, UK as Conference Producer
The third area of focus is on the use of biometrics in developing nations, where citizens lack official identity documents, such as birth certificates, and need to find ways to access government services. The Institute is still considering exactly what role it has to play in these regions, but disseminating best practice in the use of biometrics is likely to be a key part of that.

CURRENT PRIORITIES
Biometrics is fast-expanding and it’s impossible to monitor all developments closely, so the Institute currently has three priority areas: government, the consumer sector and developing nations.

The first task is to service the existing membership, which has a strong leaning toward government agencies involved in border security, law enforcement and managing civil identities.

“We are also seeing a second area emerge around the consumer space,” says Moeller. “Mobile phone companies are introducing biometrics now and financial institutions are looking at this technology to help deliver services. This is a new area that needs more development of standards and certification.”

HOW BIOMETRICS ARE BEING USED AROUND THE WORLD

SOUTH AMERICA
The challenge: Combating fraud

The solution: Companies are increasingly using biometrics to allow customers to securely access products and services such as cash from ATMs and car hire from car rental firms

AFRICA, ASIA AND THE MIDDLE EAST
The challenge: Lack of official documentation, such as birth certificates, makes it difficult for people to access services by proving their identities

The solution: Biometrics are a secure way to prove your identity to gain access to sensitive services such as opening a bank account or applying for a passport

EUROPE, NORTH AMERICA, AUSTRALASIA
The challenge: Protecting privacy and combating identity fraud, data breaches and terrorism, particularly when traveling

The solution: Increased use of biometrics in border security to identify potential terrorists and in online transactions to combat identity fraud

“There was very little information at the time about biometrics,” Moeller remembers. “And we were faced with challenges around biometrics being very new and people having concerns in the form of ’Big Brother is watching me’, and what does this technology actually do? So there were a lot of questions that needed to be addressed and the answers weren’t readily available.”

As Chief Executive, Moeller’s role has been to implement the strategy set by the board of directors, but on a day-to-day basis, she describes herself as a “connector”. “I’m going out there, finding everyone who is involved in this community, and who should be involved in this community, to make it all happen,” she says.
Mobile phone companies and financial institutions are introducing biometrics now. This is a new area that needs more development of standards and certification.

ISABELLE MOELLER, CHIEF EXECUTIVE, BIOMETRICS INSTITUTE

The Institute also has several working groups that focus on understanding and developing information and guidance on specific aspects of biometrics. Two of the longstanding working groups focus on privacy and technology innovation, while newer ones are looking at border management and digital services.

The Border User Group is currently conducting an internal survey of border agencies across the world to gain an understanding of how biometrics are being used throughout the border management process. That will lead to a set of high-level recommendations for the use of biometrics in border management. The work is timely. The use of biometrics in border management is one of the biggest trends in the sector right now, according to the Institute’s annual Industry Tracker – a survey that takes the pulse of the biometrics industry.

“That’s where the largest applications are happening and the biggest procurement contracts are taking place,” says Moeller.

The Digital Services Committee focuses on how organizations can use biometrics to verify the identity of customers transacting on digital devices – something that Moeller says is also currently a “very hot topic”. The Industry Tracker has uncovered an increase in the use of biometrics in financial services transactions, followed closely by mobile commerce payments.

Across all of these areas, the key message to any organization using biometrics is to look at whether the technology actually has a place, says Moeller. Organizations need to ask themselves whether biometrics are the right choice, how they should be implemented and how privacy issues should be addressed. “Biometrics are exciting, they offer a great solution, but they also have their challenges,” Moeller points out. “It’s all about making an informed decision, and we are there to help guide organizations along that path.”

MULTIPLE CHALLENGES

The challenges posed by biometrics are multiple but a key one is vulnerability to hacking by criminals using stolen biometrics to pose as someone else. Moeller points out the graphic, but not entirely unrealistic, possibility that criminals could steal a user’s fingerprint, either by force, by drugging the individual or even by severing their finger from their hand. The industry is well aware of users’ concerns and has developed technologies such as “liveness detection” in response. Liveness detection establishes whether a biometric sample comes from a genuine living user, or not.

Another concern is that biometric data being amassed could be breached. The Institute’s Industry Tracker often flags concerns about privacy as one of the main factors holding the industry back.

“One of the main things that we hear is a concern about loss of control over your biometric data and a potential lack of trust in organizations managing your biometrics,” says Moeller. “That’s where the Institute comes into play. There is already legislation in many countries that, even now, includes definitions of biometrics, but the Biometrics Institute has developed privacy guidelines providing a set of principles at a very high level that outline how biometrics and privacy should be managed.”

The guidelines cover how to collect information, how to store it, and how to ensure it’s not being used for something else. There are also principles around informed consent so that the person understands why their biometrics are being collected.

Bearing in mind the vulnerabilities around hacking and privacy, biometrics are clearly not the answer to all our digital security problems. But used as part of a layered approach, they are the best answer we have right now. How many layers of security you use, however, is up for debate.

There is a place for using just one biometric, but you need to assess the risk of doing so, says Moeller. “I may be comfortable accessing my phone using just my fingerprint because there is nothing valuable on it, but would I want to transact £50,000 using just a fingerprint? Probably not. Biometrics has its weaknesses and so multi-factor authentication is certainly, in most cases, the better way to go.”

Two of the Institute’s longstanding working groups focus on privacy and technology innovation, while newer ones are looking at border management and digital services.
The EU’s incoming eIDAS regulation is meant to ensure that our burgeoning digital identities can access services and products across borders, but it will also serve as a business enabler that facilitates closer commercial exchanges and boosts trade.

Our interactions with people and businesses are increasingly through digital channels that are largely oblivious of national frontiers and of the statutory powers those frontiers mark the boundaries of. Across multiple aspects of international public policy, aging laws sometimes struggle to stay relevant to technological change; in the European Union (EU) particularly, unaligned member state legal frameworks have long been recognized as an inhibitor to cross-border business growth, administrative efficiency and citizen entitlements.

While digital authenticators like electronic signatures have achieved some cross-border recognition, the need for up-to-date, internationally admissible standards of digital identity, and trust verification and validation, is now being met by the EU electronic identification, authentication and trust services (eIDAS) regulation.

Trust is the driving factor here. The bodies behind eIDAS believe lack of trust in online product and service provision holds back economic potential for consumers and suppliers. When it becomes fully operational from 29 September 2018, each EU citizen with a notified national identification scheme (for example, a national identity card) can use it to identify and/or authenticate themselves to access public services available in other EU countries where similar eIDs exist.

In a pilot project that has now ended, Germany, Austria and the Netherlands successfully connected their electronic identification and authentication infrastructure, making it possible to use Austrian and German eIDs to access Dutch online public services. For example, an Austrian driver fined for speeding in the Netherlands could use their eID to access...
Many EU countries have already deployed eID schemes and can leverage on chip-enabled identity or resident permit cards to allow for secure identification.”

YOLANDA VARUHAKI, MARKETING DIRECTOR, ID & HEALTH CARE IN GOVERNMENT PROGRAMS, GEMALTO

detailed information about their penalty in their native language, and choose to pay or challenge the fine.

In a separate pilot project currently under way, citizens in Finland and Spain can access each other’s eGovernment services – including registering for web services and making payments – using a single username and password. Mobile phones can be used for second-factor PIN authentication for extra security.

In this and other ways, eIDAS is set to give new life to practice standards around several areas of trust management and eID for electronic transactions and certifications within the European Digital Single Market. Its remit will be achieved partly by supersedence of cross-border barriers to digital trade, and by the establishment of a standards framework that legalizes reciprocal recognition of public digital identification and authentication systems between EU states.

States must mutually recognize approved eID and trust services, with national legal frameworks statutorily required to permit and facilitate EU citizens’ intent to use their national eID with public and commercial services across frontiers. For the first time within the EU, qualified eSignatures, electronic seals, time stamps, electronic registered delivery services, and website authentication certificates will hold legal status parity with traditional paper-based equivalents, although eIDAS does not affect the validity of existing formats; nor does it specify technical standards for the eID and trust services technology. Suppliers of products and services that comply with eIDAS regulations have, however, to be approved as Trust Service Providers (TSPs) by their respective national supervisory bodies.

BUSINESS BENEFITS
For businesses that already have partners and customers within the EU, the benefits eIDAS brings should prove compelling. Simplified procedures for international deals should result in reduced costs, as contractual arrangements between two or more parties in disparate EU states require less form-filling. There should be faster processing of contracts, delivery documents, and payments due to commonly admissible approvals signoff.

Applications to trade in other EU markets are expected to be made easier, leaving business more agile in response to business opportunities. Such improvements will naturally be good news for SMEs that have been beset by red tape as they have expanded beyond their home countries.

Moreover, eIDAS can boost customer acquisition by making it more straightforward to validate the identity of EU citizens, thereby shrinking administrative overheads for new account set-ups, and (in theory) making credit rating checks more simple. This is likely to benefit sectors such as fintech, where making the opening of new accounts easier is a vital differentiator to traditional banks, for example. By the same token, eIDAS’s provision for qualified certificates for website authentication, once established, will bolster consumer confidence when purchasing products and services from online traders registered to foreign EU states.

Businesses across Europe are investing heavily in ‘digitalization’ – the use of digital technologies to change business models and provide new revenue – and value-producing opportunities. Gartner’s 2017 CIO Agenda Survey notes how, as digitalization matures, enterprises find themselves part of a ‘digital ecosystem’ – a group of competitive enterprises, customers, regulators and other stakeholders that exchange information and interact entirely electronically. As a piece of pro-digitalization law, eIDAS aids economic growth with its endorsement of sustained investment in information technologies, and thus provides supportive context for enterprise IT spend proposals.

STANDARDS CONTINUITY CHALLENGES

eIDAS – which came into force in September 2014, and has been applied in phases since July 2016 – addresses a range of use cases and procedures, some of which date from the Electronic Signatures Directive, which eIDAS repealed. This directive was the cause of some befuddlement in electronic authentication and eID sectors due to the fact that, as a directive rather than a regulation, it was open to variations of interpretation by EU states at a time when the technology evolved rapidly.

However, according to Gemalto’s Marketing Director for ID and Health Care in Government Programs, Yolanda Varuhaki, that technological evolution is ongoing, which could represent a challenge for this aspect of eIDAS’s reach. ‘Gemalto fully supports the eIDAS regulation, as it creates the foundation for boosting cross-border business opportunities and developing trust services,” Varuhaki says. “Many EU countries have already deployed eID schemes and can leverage chip-enabled identity or resident permit cards to allow for secure identification and digital signatures for public and private transactions, while protecting their sensitive

LEGALLY BINDING eSIGNATURES
The eIDAS regulation recognizes three different levels of eSignatures as legally binding across EU member states:

Electronic Signature (eSignature): Basic signatures in electronic form, eSignatures cannot be denied legal acceptance just because they are digital.

Advanced Electronic Signature (AdES): AdESs require a higher level of security, typically met with certificate-based digital IDs. An AdES must be uniquely linked to the signatory, be capable of identifying the signee, be used under the sole control of the signer, and enable the verification of the integrity of the signed agreement.

Qualified Electronic Signature (QES): QESs must also be uniquely linked to the signatory, but are further required to be based on qualified certificates. Qualified certificates can only be issued by a Certificate Authority and are needed for the qualified signature, but there is no obligation to store them in the hardware security module. To create a QES, a Qualified Signature Creation Device (QSCD) is mandatory. A QSCD can be hardware- [a smart card] or software-based [a server solution], but it has to be certified. In order to provide qualified eSignature services, a Trust Service Provider (TSP) must be given qualified status.
is authorized to provide and preserve digital certificates
to create and validate eSignatures, and to authenticate
their signatories, as well as websites.

TSP take-up is still in play, but the opportunity
could exist for organizations like mobile network
operators, professional bodies and trade associations,
for example, to provide trust services to their own
subscribers, members and business-to-business
affiliates. (There’s also the prospect of TSP status
serving as a means to discover prospective pan-
European customers and partners.)

As it rolls out, eIDAS will join a range of other
eID trends that are profoundly transforming the
relationship between citizen and service provider,
and that, cumulatively, will call upon us to pay greater
attention to the way the eID ethos shapes how our
lives are lived. As eIDAS regulation allows for the
co-existence of multiple identification schemes with
different or equivalent assurance levels within the same
country (countries can notify as many schemes as they
wish), there may be more eID types heading our way.

Mentioned earlier was the fact that the promotion
of trust as an enabler of organizational and individual
rights is at the heart of eIDAS, and savvy citizens will
also know that our eIDs exist in digital domains where
levels of identity theft increase year on year.

“Increased awareness of the risks involved talks
in favor of solutions that leverage on field-proven
security standards and innovation technology, in order
to minimize exposure to eID misappropriation,” says
Varuhaki. “Greater commitment to increase usage of
secure solutions will help reduce the risk.”

WHEN TRUST IS A MUST

Vendors of eIDAS-ready products must ensure that
those products have been evaluated against the
necessary technical compliances, principally the
Common Criteria for Information Technology Security
Evaluation, the international standard for security
certification. Those entities interested in certification
as a TSP also need to be assessed for eIDAS compliance
by their country’s eIDAS supervisory body. As an
example, a certified TSP, which can be recognized
through the EU trust mark designed for this purpose,
Mobile banking is booming in Africa, but what risks does financial inclusion bring with it?

SECURING THE MOBILE REVOLUTION

Cast your mind back and remember how mobile banking services looked 15 years ago. Just like today, there was a split between the few technology-enabled 'haves' in certain parts of the world, and the vast majority of 'have-nots' in the rest. The lucky ones could open their state-of-the-art phone menu screen and begin transacting from wherever they might be, while the rest still saw banking from a desktop browser as cutting edge.

Except that 15 years ago, the future of banking tech wasn’t in the hands and pockets of rich consumers in developed economies: it was countries like South Africa that led the way with experimentation on mobile devices for their decidedly middle-earning customers. Addressing the needs of large ‘unbanked’ populations, low internet penetration and poor access to branch services, they innovated in ways that countries with well-established cultures of financial inclusion simply didn’t need to in the pre-smartphone era.

It wasn’t just the South African banks either: nationwide mobile-to-mobile payment systems originated in Kenya, with the launch of mobile
Whatever the driving forces have been, the mobile phone has been key. According to the latest figures from mobile network operators industry body GSMA, there are around 178 million registered bank accounts in Africa. The same report calculates the number of mobile payment accounts at 277 million.

The difference between Africa and the rest of the world is stark. In 2014, 12% of adults on the continent had a mobile money account, compared to just 2% of the population in the rest of the world. That number is rapidly growing: half of all mobile money services in use today are based somewhere in Africa.

Mobile banking is different to mobile payment accounts, which may be used purely for retail transacting and have no interest-bearing capacity. The two are on a clear path of convergence, however.

A paper published in the Review of Development Finance

Traditional banking infrastructure failed to meet the needs of African economies so they invented their own

operator Safaricom’s M-PESA in 2007. That’s almost a decade before brands such as Venmo, Facebook Messenger payments and WeChat Pay were available.

This story, of how traditional banking infrastructure failed to meet the demands of African economies so they invented their own, has been told often. Today, African firms still stand out as innovators in the world of fintech – Nigerian payment gateway Flutterwave is a graduate of the prestigious Y Combinator programme and South African media giant Naspers owns a third of WeChat Pay parent Tencent.

Despite the early leadership in fintech for development, it’s clear that some of the challenges that drove early adoption of mobile banking and payments in Africa haven’t gone away, and they still create unique circumstances for unique solutions, including those around security.

GROWTH FACTORS

The most common explanation for the way African technology has evolved is that the continent is “not mobile first, it’s mobile only” when it comes to internet access. Payment services such as M-PESA developed in Kenya because the vast majority of the population had no easy way to send money to one another via traditional banks or the internet, but they did have mobile phones.

There have been other factors at play. A concentrated drive by stakeholders such as the World Bank, US AID, the UK Department for International Development (DfiD) and private philanthropists such as the Bill and Melinda Gates Foundation saw US$34 billion in aid money invested in financial inclusion projects between 2008 and 2015.

While wider availability of smartphones can make mobile banking safer, the challenges don’t end there, warns Sanjay Vaid, Practice Director at Wipro. Low cost, rarely updated phones are more likely to be vulnerable to security flaws. For example, high data prices have helped to drive the provision of municipal sponsored free WiFi in many cities – there’s a strong probability that many low cost phones won’t be updated to protect against recently discovered weaknesses in the WPA2 protocol, which is almost universally used for Wi-Fi security.

THE SMARTPHONE SOLUTION

While wider availability of smartphones can make mobile banking safer, the challenges don’t end there, warns Sanjay Vaid, Practice Director at Wipro. Low cost, rarely updated phones are more likely to be vulnerable to security flaws. For example, high data prices have helped to drive the provision of municipal sponsored free WiFi in many cities – there’s a strong probability that many low cost phones won’t be updated to protect against recently discovered weaknesses in the WPA2 protocol, which is almost universally used for Wi-Fi security.
in June 2017 showed direct progression from use of mobile payments to formal financial inclusion and the opening of savings accounts.

For mobile payments in Africa, the risks are unique. Safaricom has reported in the past that the incidence of fraud on the M-PESA platform is much lower than that of credit cards. Just 0.002% of M-PESA transactions are bogus, Safaricom says, compared to between 0.05% and 0.1% for credit cards around the world. This is partly a result of investments made by the operator around security, and partly the fact that M-PESA customers aren’t high value targets for thieves.

Far more at risk are the agents, who convert digital cash into physical currency and vice versa. Because they carry cash, agents are at higher risk of crime than end users, and recent efforts to protect them include insistence on photo identification of customers at the point of exchange.

**SECURITY AND MOBILE BANKING**

Mobile banking carries different risks and solutions.

For customers who are banking online with smartphones and apps, says Sanjay Vaid, a Practice Director for cyber risk security at consultancy firm Wipro, the security concerns in Africa are the same as anywhere else in the world. Cell phone theft, password breaches, malware breaches and phishing attacks are the main worries for customers with an iPhone whether they are in Nairobi or New York.

“To a certain extent, security needs are universal,” says Vaid. “There’s always the need for encryption, strong identity authentication and multi-factor tokens.”

What’s different in Africa’s emerging consumers, Vaid explains, are the types of cell phones that have to be secured against an ever more dangerous threat landscape. Smartphones are far from ubiquitous. According to Pew Research Centre, 37% of South Africans own a smartphone, as do 28% of Nigerian, 26% of Kenyans and 24% of Ghanaians. Other African countries lag behind significantly.

Feature phones are used for mobile banking and payments all over the continent, but as Vaid points out, the key technologies used – SMS and USSD – have known security weaknesses that could be exploited to intercept transactions.

“SIM-swap” fraud, for example, is a form of identity theft that has long been an issue in Africa and is filtering to the rest of the world as mobile banking becomes more popular. It involves convincing a mobile operator that you are a customer who has purchased a new SIM card or lost their old one, and need a number transferring. Once fraudsters have access to the victim’s mobile number, they target bank accounts and request new login details, allowing them to gain control of mobile bank accounts. Banks and telecoms operators need strong, secure processes in place to verify end users’ identity, alongside risk engines that detect and prevent suspicious behavior from a customer’s account.

To improve security in general, says Vaid, we need to increase the use of smartphones that support fully encrypted, app-based transacting – this is happening organically as the cost of a new smartphone is almost the same as a feature phone today.

Once smartphones are available, apps become popular fast. A survey by IT vendor Avaya found that the app was the preferred banking channel for 30% of South Africans – that’s more than three quarters of all those who have access to mobile apps.

James Fowle of FNB, a bank that operates in eight African countries, says that nine out of 10 of his customers use mobile banking in some form or another. Where smartphone penetration is higher, the bank encourages customers to switch from USSD access to the more secure app as soon as possible, by incentivizing its use with reward points.

But what of the future? Jaco Botha, of South African cyber security firm Parsec, says as advances in artificial intelligence and machine learning improve, criminals are using these technologies to launch ever more sophisticated and convincing phishing attacks on bank customers. In areas where digital literacy is low but uptake of mobile banking high, helping people understand digital risks as they enter the formal banking system for the first time will be the most critical defence against attacks.
 Residents of the Eindhoven district of Strijp-S will soon be able to book electric vehicles from a car-sharing scheme, ride on electric buses and use energy produced during the clean-up of contaminated land. The district is taking part in the EU-funded Triangulum initiative, which aims to demonstrate smart city solutions.

A district-wide system of complex hardware and software will allow the residents to access all kinds of infrastructure, with the intention of helping them to use energy and transport in a more sustainable way. It will monitor and control street lighting, mobility, houses and offices. It will also enable an app for parking management and a smart charging station.

Eindhoven is one of three cities taking part in the initiative; the others are Manchester, in the UK, and Stavanger, in Norway.

Source: tinyurl.com/SmartTriangulum

2.4%

Montevideo, in Uruguay, plans to harness technology to encourage the use of bicycles. Currently, only 2.4% of journeys are made using bicycles, but, with support from the Inter-American Development Bank (IDB), the city hopes to increase this dramatically by 2020.

Several teams participated in a recent workshop and presented applications that could improve cycling in the city. One, Pedaleapp, received a US$5,000 prize from the bank and a further US$5,000 to incubate its technology. The solution will be supported by improvements to bicisendas (bike lanes).

IDB’s Morgan Doyle said: “We believe that it is possible to have more human, livable, modern and less polluted cities.”

Source: https://tinyurl.com/MontevideoBikes

2,400

Smart streetlights in the Californian city of San Diego will form a connected digital network that will improve parking and traffic management, enhance public safety and track air quality.

The city has partnered with General Electric to upgrade the streetlights in a project that will see 3,200 smart sensors deployed, making it the largest city-based deployment of an Internet of Things platform in the world. The sensors will use real-time data to do things such as direct drivers to available parking spaces, help the emergency services, track carbon emissions and identify intersections that could be improved for pedestrians and cyclists.

The information can be used to support San Diego’s Vision Zero strategy to eliminate fatal road accidents and severe injuries. Installation of the new streetlights is expected to be completed by the fall.

Source: tinyurl.com/Road-Lighting

0.5m

IDB’s Morgan Doyle hopes to see Montevideo’s residents make half-a-million bike trips a day

Source: https://tinyurl.com/MontevideoBikes

THE WORLD’S SMARTEST CITIES

In every region of the globe, new technologies and intelligent design are making city living easier and cleaner

AUTHOR ANDREW STRANGE
US$35bn

Just over an hour from Seoul, a new International Business District is rising on land reclaimed from the sea in the city of Songdo. The US$35 billion construction project is remarkable because the district will be an exemplar of smart city living.

Started in 2002 and due for completion in 2020, it features mass public transport systems, so residents don’t have to drive. And the city has been designed to ensure that schools, hospitals, offices and shops are all within walking distance.

There is a huge cycle network, more than 100 buildings are Leadership in Energy and Environmental Design (LEED)-certified (a globally recognized green rating system), and an innovative underground waste management system will suck waste to a central recycling facility. It is estimated that Songdo will produce a third fewer greenhouse gases than other cities of the same size.

But so far only 70,000 people work in Songdo, which is far fewer than the 300,000 envisaged.

Source: tinyurl.com/SongdoSmartCity

760mph/1225kph

A train that can travel up to 760mph/1225kph is expected to cut the journey time between Dubai and Abu Dhabi from 90 minutes to under 12. The Hyperloop – an idea first proposed by Tesla CEO Elon Musk – is based on magnetic levitation, which removes friction between the train and the rails, and allows much faster speeds.

The train, which will travel along vacuum-sealed tubes at almost supersonic speeds, is due to go into service in 2020 and is part of Dubai’s efforts to become one of the world’s smartest cities. Initial designs include virtual windows so that passengers will be able to see where they are.

Hyperloop technology will help to ensure that 25% of commutes in the UAE are made in autonomous vehicles by 2030.

Sources: tinyurl.com/HyperloopDesign, tinyurl.com/DubaiToFujairah, tinyurl.com/SmartDubai

US$7bn

Singapore is a clean, organized, technological city, but it faces a huge challenge because of a lack of drinking water, which must be imported from Malaysia. The city has, however, turned this problem to its advantage by using policies that support innovation to address the water shortage.

As a result, it now has more than 100 companies generating US$370 million in annual revenue from selling rainwater collection and water recycling technologies around the world. In fact, since 2006, Singapore’s water tech sector has generated more than US$7 billion from international projects.

The use of public policy tools to crowdsource solutions is one of the key characteristics of smart cities.

Source: tinyurl.com/SingaporePolicies
New EU data protection rules present organizations with the perfect opportunity to embrace security by design and offer customers a superior service.

One date that should be firmly in the calendar of all organizations holding information on individuals in the EU is 25 May 2018 – the day that the General Data Protection Regulation (GDPR) comes into force.

The EU has had data privacy mandates in place since 1995 – the Data Protection Directive, which was designed to protect EU citizens’ privacy and restrict the distribution of sensitive personal data outside the EU. Since then, there has been a massive rise in incidents of data breaches – according to Gemalto’s Breach Level Index, 1.4 billion records were breached in 2016, increasing to over 1.9 billion in the first half of 2017 alone. More executives now recognize that it is a question of when, not if, their organization will be hacked, and the scale of the potential reputational and financial damage that such incidents can cause.

Executives now recognize that it is a question of when, not if, their organization will be hacked, and the scale of the potential damage.

FORTIFYING SAFEGUARDS
The introduction of the GDPR is designed to fortify the safeguards around personal data – encompassing the right to be forgotten as well as clear and affirmative consent – and to standardize data protection requirements across the EU. The GDPR will affect
all organizations, regardless of size, industry or location, if they hold or process personal data on EU citizens.

A key aspect of the GDPR is the requirement to report a data breach to the national supervisory authority and to the individuals affected within 72 hours of its detection. Sanctions for failing to do so can involve a fine of up to 4% of global turnover or a maximum €20 million, whichever is higher. However, if an organization can demonstrate that its data was protected by encryption (unlike 95% of the 2016 data breaches) or anonymized, it is absolved from reporting the breach to the affected people, while if it can prove it had tried hard to protect the data, the regulatory authority may treat the incident more leniently.

Although the GDPR was formally adopted by the EU in April 2015, the response of organizations has been mixed: some have a strategy and may even have started to implement it, but many others are still unprepared. Getting ready for the GDPR is not an overnight process and organizations will not be expected to have everything in place on 25 May 2018, but they could be subject to an audit and must still comply with the breach reporting requirements after the GDPR becomes effective.

**IN-BUILT SECURITY**

Many organizations respond to the need for increased security by applying patches to an existing system (a big challenge), but GDPR compliance implies security by design – a system that has been designed with security in mind from the outset, rather than simply as an afterthought. This is in line with Gemalto’s recommended compliance infrastructure approach, which covers key aspects that organizations will need to address, providing a cost efficient and effective way to meet existing and future compliance obligations (see box above, right).

**BUILDING A COMPLIANCE INFRASTRUCTURE**

- Establish a central point of control and visibility for managing encryption technologies, keys, policies, logging and audits
- Make sure only the right people can access private information and data can be managed without being altered, with layered access controls based on strong, multi-factor authentication solutions and hardware security modules (HSMs)
- Ensure an authentication management platform is in place that enables the central management of authentication devices and policies
- Develop a data protection privacy policy that makes sense to the administrator and to those who enforce it
- Establish the centralized, efficient and secure management of cryptographic keys and policies
- Ensure secure cryptographic key management involving robust HSMs
- Safeguard regulated data across all applications and systems through encryption, so even if an organization’s initial defenses are breached, sensitive data is still protected

With only a few months until the GDPR comes into force, it is now critical for organizations that have done little so far to start preparing. Industry experts suggest a six-step approach to achieving GDPR compliance by controlling access to personal data (remembering that people are, and will remain, the biggest risk), encrypting that data (even if not mandated by the GDPR) and securing and managing the keys (see box below, left).

Adopting a positive attitude will be key to developing successful GDPR compliance, as it offers an excellent opportunity to understand how personal data is handled and to improve communications with customers. Security by design is a way to provide a superior service to customers and to ensure that an organization moves with the times. Biometrics, for example, are becoming increasingly relevant as technology improves and hacking becomes even more widespread; as Verizon suggests in its 2017 Data Breach Investigations Report, organizations are not doing enough “if a username and password is the only barrier to escalating privilege or compromising the next device”.

**SIX STEPS TO GDPR COMPLIANCE**

1. Understand the legal framework
2. Create a data register
3. Classify the data
4. Start with the top priorities
5. Assess and document additional risks and processes
6. Revise and repeat

For more from Gemalto on GDPR, visit tinyurl.com/Gemalto-GDPR
Bringing the eSIM and 5G together will trigger a connected device revolution, but are consumers ready for it? Maybe, with a little help from their smart assistant.

In 2012 Stephen Wolfram published a very long and detailed blog about the 300,000 emails he’d sent since 1989. He had entered every bit of data manually inside a spreadsheet. The blog even featured a heat map showing the time he’d spent on every email.

The blog attracted a lot of attention. It revealed Wolfram as the uber nerd of the ‘quantified self’ movement – a collection of people who record every aspect of their lives, and whose motto is ‘self knowledge through numbers’.

Wolfram’s obsessive email auditing may have been eccentric when he started it in the 1980s. But by the time he published his results, not so much. Why? Because by then technology had made it possible for anyone to quantify themselves. You didn’t need a spreadsheet and lots of spare time. You could just buy a Fitbit, a Jawbone or a Misfit.

This new generation of wearables moved the idea of the fully connected consumer closer to the mainstream. By pairing a wristband with an app, anyone could measure their sleep patterns, heart rate, calorie consumption, footsteps.

When Apple launched its own smart watch in 2015, experts believed the connected revolution was imminent. They predicted a huge new market.

The truth is, it has yet to arrive. In 2017, a report from digital research firm eMarketer revealed 75% of adults had never purchased any kind of smart clothing or wearable device. Meanwhile, among those who had bought one, 83% said it was for fitness and health tracking.

LIMITLESS POTENTIAL

Of course, wearables only represent one facet of the connected device world. Nick Turner, Partner of the Consumer and Industrial Products division at Deloitte, says, “In the longer term, ‘connected device’ will be a potentially limitless term, as it becomes possible to attach internet-connected sensors to almost anything.”

Indeed, Gartner estimates that, by 2022, the average household “could contain several hundred smart objects”.

What could make this happen? Well, one important catalyst could be a new kind of SIM card, the eSIM, which can be soldered in place and programmed to connect to a chosen carrier remotely. The eSIM gives a smart device independent connectivity. It’s more practical than a traditional SIM card, which has to be removed and replaced. And it is more flexible than a Wi-Fi connection.

In 2017, the Samsung Gear S3 watch became the first device to ship with an eSIM. Since then there
have been more, including the Microsoft’s Surface Pro and the Apple Watch Series 3.

So, can the eSIM move beyond watches and PCs and make pretty much anything ‘connectable’? Emmanuel Legros, Head of Marketing for Consumer IoT at Gemalto, thinks so. “There are a lot of devices out there, like smart doorbells for example, that currently rely on Wi-Fi to connect,” he says. “But they can be out of range of the router or the connection can drop. I’ve spoken to these manufacturers and they are very interested in eSIMs because they provide a permanent connection that works almost anywhere.”

PARTNERING WITH 5G

The eSIM should therefore make it easier for a diverse range of products to connect; even more so when paired with next generation 5G networks. 5G is not just faster than LTE, it also offers 100x better latency, up to 100x more connected devices per unit area and a 90% reduction in energy usage. It will roll out in selected regions later this year.

The combination of eSIM and 5G should power an explosion of efficient, robust and affordable connected devices. But will the public buy them? Market watcher CCS Insight admits it’s taking a while for the mass market to catch on. Indeed its most recent survey focused on early adopters as its previous attempts to question a cross section of the public about connected devices proved so challenging.

“We found it hard to get meaningful results from talking to the general public because so few of them use these devices,” says analyst George Jijiashvili. “We decided to question tech enthusiasts to get better insights.”

What emerged was a very high level of satisfaction. For example, 85% of respondents said they used their smart speaker (Amazon Echo or Google Home) every day or most days, while 40% said they used it more than when they first bought it.

This could be significant as smart assistants like Echo, Google Home and others have proved to be the most successful of the new generation of connected devices. In fact, these voice-controlled devices could play a key role in accelerating the connected future by solving the user interface issue.

Here’s the argument: many consumers are enthusiastic about smart gadgets such as lights, thermostats, locks and alarms, but have been put off
by the difficulty of controlling them from one location. At first there were apps. But this solution proved unwieldy. Telling Echo/Alexa to "turn down the heating" is a far more elegant form of management.

Jijaishvili says: "It’s obvious that the giant tech firms see the smart speaker as the next big frontier. They’re investing heavily in the space. And our research shows that people love these devices."

**SOLVING CHALLENGES**

If eSIMs and 5G look set to make devices cheap and reliable, and voice acts as the user interface for controlling them, what is left to solve? Legros has a simple answer: the business model. He says: "How will people pay for all these new connected services? We can’t expect people to add a new subscription whenever they want to add a new device – especially as a lot of smart devices are gifts."

Happily, many carriers already recognize this. Verizon, for example, offers its subscribers a flat monthly data fee with the option to add any connected device for $5 per month.

The other obvious barriers center on security and privacy. Connected devices are constantly in communication, and therefore vulnerable at multiple points. They can spread malware fast. Hackers can use these weaknesses to steal financial information and inflict sabotage.

Solving this will be tough, especially as many connected devices are made by companies with no history of security. Lighting companies, for example, have spent decades focusing on illumination, not data encryption.

The evidence suggests many of these companies lack the skills or the desire to build security in. In 2014, HP’s Fortify software unit tested Internet of Things (IoT) devices like lawn sprinklers, alarms and thermostats. On average, each device contained 25 security holes.

A related question is how to patch these devices? Can consumers be expected to update the firmware in dozens of connected gadgets as if these devices were iPhones? Would they know how?

One possible solution is to make the processing inside the devices more secure. The industry is working on this. For example, in 2017 chip specialist ARM unveiled its Platform Security Architecture (PSA) – open-source code that should, in theory, help device makers build products that are harder to hack.

**PROTECTING PRIVACY**

Related to the security question is the privacy issue. A world of connected devices gives manufacturers the opportunity to track and surveil users. In fact, they already do. This issue threw up one of the more unlikely stories of 2017, when sex toy maker We-Vibe agreed to pay customers up to $10,000
FORMAT WARS
Whenever a transformative new technology comes along, there is usually a format war: VHS and Betamax; Blu-Ray and HD DVD; GSM and CDMA.
The world of IoT and connected devices is, regrettably, no different.
For all the hype, this market is still at its formative stage. And as such, its dominant technical standard has yet to be agreed.

Clearly, connected devices need to communicate with each other. To do so, they must share networking protocols. However, with multiple companies competing for supremacy, there is still no universal consensus.
The three main competitors are Google’s Thread, The Allseen Alliance’s AllJoyn and the Open Connectivity Foundation’s IoTivity. All three have open sourced their technology to encourage third-party manufacturers to adopt their standards.

But some manufacturers still believe they can establish their own standards. Apple has HomeKit, which gives device makers a platform through which to connect objects to apps. Meanwhile Amazon Echo and Google Home do the same via their smart speakers.
Samsung and LG, meanwhile, are developing SmartThings and SmartThinQ respectively.
In the United States, the four states of Colorado, Idaho, Maryland and Washington D.C. are piloting the concept of a digital driver’s license (DDL). The goal is to create and implement a solution that taps into the ubiquity and large-scale adoption of the smartphone to deliver a secure identity verification tool, with multiple applications and use cases.

The DDL is an incredibly secure version of a physical driver’s license stored on a smartphone and it is used to supplement existing licensing and identification documents. It has been designed to be as user-friendly as possible, while allowing for a comprehensive and secure ecosystem that grants users access to a variety of services and solutions.

Throughout the pilot, 98% of participants carried their DDLs with them and used them frequently and 56% were willing to pay for the solution should it move forward into mainstream adoption. The situations that they were most likely to use the DDL for were airports and travel, 62% for hotels, 44% for purchasing alcohol, 43% for age-restricted venues and 41% for the doctor or the pharmacy.

The researchers also found that many use cases for the DDL presented themselves throughout the trial that nobody had originally considered, and this versatility was highly favored by the users.

The first phase of the DDL pilot underscored the multiple benefits to the individual: identify yourself online; sign documents electronically; rent cars; book airline tickets; organize driving services; and so much more.

Currently, as the project moves toward the second phase, it is looking to integrate with additional services. There are also plans to explore the use of the DDL in payments and digital wallets to make them faster and even more secure.

The four states are also working with key organizations to ensure that global and national standardization and specifications are in place. These include the NIST Trusted Identity Group on digital authentication guidelines and privacy, ISO WG10 TF14 for worldwide standardization, and AAMVA mDL Working Group for standardization in North America, alongside functional requirements and guidelines. What happens next will depend on the successes within phase two, but so far the responses have been overwhelmingly positive and the potential is extraordinary. Welcome to digital identity on demand.

For the latest technology news, check out the Gemalto blog at blog.gemalto.com
We are delighted – and excited – to be at Mobile World Congress for another edition. Many of the big themes at MWC are already reflected in our articles in this issue of The Review. Our cover feature considers the transformational effect of 5G – for providers and customers – and the new security challenges that this will bring.

In ‘Connected Consumers’, we explore the possibilities that could open up for users when 5G meets the eSIM. Experts predict that this could ‘power an explosion of efficient, robust and affordable’ connected devices. Mass adoption, however, will depend on usability and security.

Biometric security continues to be an important part of our offering, so we’re pleased to have been able to speak to Isabelle Moeller, the Chief Executive of the Biometrics Institute, for this issue. Read our profile of Isabelle to find out how the Institute is providing leadership in an emerging sector.

With the increasing adoption of biometrics, regulators have brought this data under the remit of new EU General Data Protection Regulation. Read our article on the consequences of data breaches under this new regime and how you can make your organizations more robust against attacks.

Many of you will have heard that in December 2017 Thales put in a bid to acquire our company, which was unanimously recommended by our Board of Directors. We believe that this offer is in the best interests of Gemalto, the sustainable success of our business, clients, employees, shareholders and other stakeholders. We expect the deal to close in the second half of 2018. Until then, Gemalto will maintain business as usual – delivering best-in-class digital security solutions.

I hope you find plenty in this issue to help you continue to build technologically advanced and secure organisations. Enjoy the read.

Philippe Vallée
CEO
Gemalto

gemalto.com  @gemalto  LinkedIn.com/company/gemalto

The Review is produced for Gemalto by Wardour, Drury House, 36-38 Russell Street, London WC2B 5HA, United Kingdom +44 20 7010 0999  wardour.co.uk
COMMUNICATIONS MANAGER, GEMALTO
Laurence Manouelides
EDITOR-IN-CHIEF
Eila Madden
GROUP ART DIRECTOR
Steven Gibbon
PRODUCTION DIRECTOR
Jack Morgan
PRODUCTION DIRECTOR: Angela Chedlow-/Dave
SENIOR ACCOUNT MANAGER: Matt Govecky
CLIENT SERVICES DIRECTOR: Egan Anker
CREATIVE DIRECTOR: Dara Barnett
MANAGING EDITOR: Claire O’Dwyer
CEO: Martin MacConnol

Delighted to be back

Contributors

Nicholas Booth
Nicholas worked in IT support within the health, financial services and public sectors before becoming an IT journalist.

Adam Oxford
South Africa-based Adam has been a technology journalist for the past 15 years, writing for titles across the world.

Tim Green
Tim was a senior analyst at Screen Digest before launching B2B title Mobile Entertainment in 2005.

Susan Antony
After more than 20 years as an equity analyst following technology stocks, Susan is now a freelance commentator and blogger.

David Howell
David reports on technology and computing. He also works as a consultant to small businesses moving online.

Tamsin Oxford
A journalist and editor for nearly 20 years, Tamsin specializes in IT and has edited titles such as PC World.

James Hayes
James is a former Senior Editor of the flagship magazine of the Institution of Engineering and Technology.

The Review is produced for Gemalto by Wardour, Drury House, 36-38 Russell Street, London WC2B 5HA, United Kingdom +44 20 7010 0999  wardour.co.uk
COMMUNICATIONS MANAGER, GEMALTO
Laurence Manouelides
EDITOR-IN-CHIEF
Eila Madden
GROUP ART DIRECTOR
Steven Gibbon
PRODUCTION DIRECTOR
Jack Morgan
PRODUCTION DIRECTOR: Angela Chedlow-/Dave
SENIOR ACCOUNT MANAGER: Matt Govecky
CLIENT SERVICES DIRECTOR: Egan Anker
CREATIVE DIRECTOR: Dara Barnett
MANAGING EDITOR: Claire O’Dwyer
CEO: Martin MacConnol

The Review is published by Gemalto Corporate Communications – www.gemalto.com
© 2018 Gemalto - www.gemalto.com. All rights reserved. Gemalto, the Gemalto logo and product and/or service names are trademarks and service marks of Gemalto NV and are registered in certain countries. The views, expressions, contributions and correspondents are their own. Reproduction in whole or in part without written permission is strictly prohibited. Editorial opinions expressed in this magazine are not necessarily those of Gemalto or the publisher. Neither the publisher nor Gemalto accepts responsibility for advertising content. For further information on The Review, please email: laurence.manouelides@gemalto.com

The Review is printed on Carbon Life 80 paper. Certified as an FSC mixed sources product, CO3 544 TS 002 is printed with 58% recycled paper and 42% from well managed forests, together with 50% FSC-certified virgin paper from well-managed forests.

amdocs digital eSIM manager
breaking the barriers to consumer IoT
5G is going to radically change the way we think about digital services, access and security.