



BIOMETRIC SUMMIT LONDON 2018

Innovation in biometric technology

powered by 



Platinum sponsor

STIFEL

Hospitality sponsor



Silver sponsors



Sponsors



Media partners



Goode Intelligence

Goode Intelligence is a leading cyber security research, analysis and consulting organisation founded in 2007 and based in London. We work internationally with technology vendors and service providers to **inform, educate and influence**. Our services are used by a range of clients, from established super-brands right through to hot, emerging start-ups and market disrupters.

www.goodeintelligence.com



RANT Events

RANT Events is a well-established events company operating in the information security industry with the largest community of senior end-user only information security professionals in the UK. It was established to provide uniquely relaxed and open networking events where members can discuss and debate challenging industry topics, while receiving educational content and CPE credits.

www.rantevents.com



A very warm welcome to the inaugural Goode Intelligence Biometric Summit London 2018.



We're witnessing explosive growth with the use of biometric technology for a wide range of applications across all sectors.

Biometric technology is incredibly versatile; breaking out of its traditional applications, law enforcement, defence and border control, biometrics is being used to secure mobile devices, authenticate consumers into banking apps, identify new customers for digital onboarding and detect fraudsters attempting to social engineer contact centre workers.

In recent years we've even seen biometrics break out of the security world with facial recognition being leveraged to detect emotion to support advertising and online education courses. It is even being used to detect whether a car driver or occupant is attentive as a method to prevent accidents.

We are only just starting to scratch the surface of what biometric technology can offer and I believe it will fundamentally change the way that we interact with the Internet – blurring the lines between physical and cyber worlds.

Today's summit brings investors and business leaders together to hear about the latest innovation in biometric technology from some of the brightest minds in the industry representing some of the fastest growing companies in technology.

The summit kicks off with an entertaining presentation from the executive editor at Wired Magazine UK, Jeremy White, who will be bringing his skills in identifying emerging trends and technological shifts that will affect both consumers and businesses to a presentation on how Artificial Intelligence (AI) and Biometrics are being harnessed by businesses to gain a competitive advantage.

These themes are further explored in the Showcasing UK Biometrics panel bringing together three leading UK-based biometric vendors. The UK is starting to incubate potential leaders in the biometric and identity industry and our panel includes B-Secur with its cutting-edge heartbeat (ECG) technology, AI-powered facial recognition from iProov and identity and authentication platform providers SmilePass.

The consumer biometric revolution was started by Apple with the arrival of Touch ID fingerprint authentication on the iPhone 5S in 2013. Since that leap, billions of smartphones get shipped every year with touch fingerprint sensors as standard. Torgny Hellström, Chairman of Precise Biometrics will be sharing his views on market trends in fingerprint biometrics and will include the latest on the potentially explosive growth of biometric payment cards.

Biometrics offers a way in which the password can finally be relegated to the technology scrap heap but biometrics on their own do not provide the answer for a password-less world. Nok Nok Labs is a California-based authentication vendor that has been instrumental in setting up the FIDO Alliance – a group of leading technology companies and global businesses with a mission to standardise authentication and to make it simple for users. In the session Accelerate Digital Transformation with Biometrics in an era of PSD2 and GDPR, Nok Nok's Michelle Salway, Senior Director of Sales, EMEA will be providing insight in how they are able to transform business with their FIDO biometric authentication solutions.

Biometrics can operate in both passive (without direct interaction from a user) and active (where the user directly presents their biometric - fingerprint, face or heartbeat) modes. Behavioural biometrics is a passive biometric technology that learns how users interact with technology and creates unique profiles that can detect normal or abnormal behaviour. One of the leading behavioural biometric specialists is Sweden's BehavioSec and we are delighted to welcome Mark Gent, Director, Worldwide Sales Engineering at BehavioSec who is presenting The Human Factor as an Asset.

And finally, GDPR has been all over the news recently with the EU data protection becoming law on 25 May across the European Union. Biometric data is one of our most personal pieces of data and in our final session of the day, I'll be moderating a panel representing the views of a data protection officer (Emma Butler from Yoti), a lawyer (David Cook from Eversheds Sutherland) and a technology provider (Andrew Bud from iProov). You can expect some lively debate from the panellists on a vitally important part of biometrics!

I hope you enjoy this summit and look forward to speaking with you throughout the afternoon.

Thank you

Alan

Agenda

13:00 - 13:30	Registration and light refreshments
13:30 - 13:35	Opening Welcome: Alan Goode, CEO and Chief Analyst, Goode Intelligence
13:35 - 13:50	Presentation from Stifel
13:50 - 14:30	<p>Keynote Address: Jeremy White, Executive Editor, WIRED Magazine UK</p> <p>AI & Bio: harnessing technology for competitive advantage With the rise of biometrics, voice recognition and digital assistants, most think we are now living in the AI age. The truth is that this is only the beginning of this era. However, already companies are working on ways to gain advantage over their competitors using these new technologies. Also, the rise of robotics, autonomous vehicles, health tech and increase in computer processing power is matched by the rapid reduction in cost of technology. The resulting ever closer collaboration between humans and machines is set to transform businesses in currently unimaginable ways.</p>
14:30 - 15:15	<i>Showcasing UK Biometrics:</i> Presentations by three leading UK-based vendors – B-Secur, iProov and SmilePass – followed by a panel moderated by Steve Cook, expert biometrics and fintech consultant.
15:15 - 15:35	Break
15:35 - 16:00	<p><i>Market trends in fingerprint biometrics, Torgny Hellström, Chairman, Precise Biometrics</i></p> <p>Fingerprint biometrics is growing rapidly and is well on its way to replacing passwords for identity authentication. Still, we have just seen the beginning of this development. Biometrics will introduce smarter payments that increase convenience and security, further personalise our homes and introduce new means of interaction with our cars. With this context in mind, Torgny will provide an overview of the current market trends in fingerprint biometrics.</p>
16:00 - 16:25	<p><i>Accelerate Digital Transformation with Biometrics in an era of PSD2 and GDPR, Phil Dunkelberger, CEO, Nok Nok Labs and Michelle Salway, Senior Director of Sales EMEA, Nok Nok Labs</i></p> <p>Learn about the latest innovations and emerging Web Authentication standards that help you deploy biometrics for improved user experience and security without compromising user privacy for PSD2 and GDPR compliance.</p> <p>Find out how innovative financial services and other organisations are leveraging authentication as a cornerstone of their digital transformation strategy to increase customer engagement with frictionless biometrics, mitigate phishing attacks and reduce transaction fraud.</p>
16:25 - 16:50	<p><i>The human factor as an asset, Mark Gent, Director Worldwide Sales Engineering, BehavioSec</i></p> <p>Proving who you are as an end user online is onerous, to say the least. Equally, organisations struggle to find the right balance between convenience and security for their customers: BehavioSec's patented technologies deliver a behavioral biometric solution that helps millions of users to authenticate securely, while keeping a great UX.</p>
16:50 - 17:30	<i>Privacy & Biometrics – The impact of GDPR on Biometrics:</i> Moderated panel by Alan Goode with Andrew Bud, CEO, iProov, Emma Butler, DPO, Yoti and David Cook, Solicitor Advocate, Eversheds Sutherland.
17:30 - 19:00	Drinks Reception & Networking Session

Welcome from Stifel

Welcome to Stifel. We're delighted to be hosting the Goode Intelligence Biometric Summit London 2018, bringing together the very best cybersecurity experts, practitioners and investors from all over the globe, for this afternoon of insight into the latest innovation in biometric security.

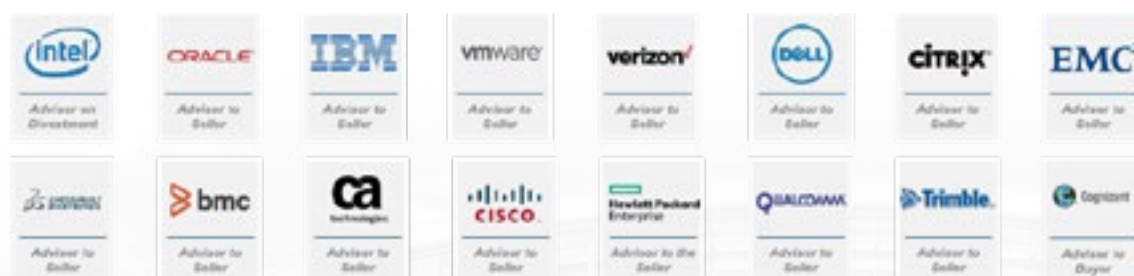
For over 125 years, meeting and exceeding the objectives of our clients has positioned our Firm for success. We believe that by placing our clients' interests first, they prosper. We focus on deeply understanding where our clients want to go so we can help them get there. In doing so, we also gain unique insights into the next trends and are able to connect the best companies with the right investors and acquirers at the right time.

Stifel is a global investment bank listed on NYSE with a multi-sector full-service offering focused on the mid-market including corporate broking, capital-raising (equity/debt/convertibles) and mergers & acquisitions. We have been in London since 2005 and employ 280 people here and 8,000 globally.

In Q1 2018, we raised £1.4bn for clients on the London Stock Exchange which represents about 20 percent of all capital raised on the Exchange and a fivefold increase on Q1 2017.

We also have one of the largest global technology investment banking teams with a 45+ year heritage and strong track-record.

Interacting with Key Strategies in Technology



Working with Relevant Private Equity Firms



We're looking forward to meeting you and hearing your story during the Summit today – please come and say hello.

STIFEL

Biometrics: Are they becoming the nirvana of personal security?

By 2020, nearly all smart devices including mobile phones, tablets and wearables will have some form of biometric security enablement. By the same time, personal banking through mobile apps will likely overtake online banking in the UK.

In 2017, over 22 million people managed their current account on their phone, according to a report by CACI. By 2023, they have predicted that around 35 million people or 72 percent of the UK adult population will bank in the future via a phone app.

The combination of mobile banking and biometric security in our smart devices will enable consumers to have more confidence regarding their personal security and will be far safer than it has ever been. Digital identity and proving who you are has become important for all kinds of remote banking.

Combining both physical and behavioural biometric technologies together will play a central role and a key component of the customer journey and user experience. Besides it also has the convenience over having to remember complex passwords or PINs.

However, even though we know that biometric technology is not perfect, it is certainly a better security method than traditional user names and passwords, which can be hacked or stolen because there have been a large number of high profile data breaches in the past few years.

Behavioural biometrics is the fastest growing of all the biometric sciences and there are many new Fintech and start-up companies offering different types of solutions. Sometimes known as passive biometrics, they usually

require the user to just carry on with what they are normally doing. Behavioural biometrics provides an analytical tool to moderate risk. It actually monitors user behaviour during the duration of the visit and detects anomalous

activity. There are some 2,000 parameters that behavioural biometrics depends on that give a clear indication of someone's unique identity. These range from monitoring human motion gestures and patterns to keystroke dynamics, and factors such as speed, flow, touch, sensitive pressure and even signature formats. It also uses machine learning and AI as a continuous form of authentication. This technology can detect bot attacks and synthetic account openings too. A number of prominent banks have already deployed behavioural biometrics as part of their remote customer on-boarding strategies.

Regulators have aimed for more competition in the sector through the system of Open Banking, which allows customers access to specific new services through their old account. New regulations in the form of the revised EU Payment Services Directive (PSD2) and the General Protection Data Regulation (GDPR) are having a serious impact on banking services. Both regulations require tighter security measures over payments and personal data.

As part of PSD2, Strong Customer Authentication (SCA) will come into force later next year. This means banks and other commercial enterprises must be compliant with a minimum of Two-Factor Authentication regarding online and mobile payments, with certain low risk exemptions. However the large majority of payments will require a task to prove your





identity, and in some cases it will require a step-up process too. This means combining something you have in your possession such as your smart device or bank card and something you know such as knowledge based answers, with a biometric component such as a selfie or fingerprint.

Privacy has become an issue too. In GDPR, biometrics is now subject to explicit consent given by the user as it is considered that biometric templates cannot be regarded as non-sensitive data under the Article 29 guidelines. They may contain a more limited amount of personal information than the biometric data themselves and in a coded form, but that extract serves as a pre-processed format for matching and is capable of providing unique identification in an automated matching process. The special power of biometric data is their capacity to serve as a universal identifier allowing information about the same person to be linked across different information sources.

2018 has seen biometrics come of age. Many consumers are already using a biometric method to unlock their smartphones; features such as a fingerprint scanner in Android phones, or TouchID/FaceID in IOS phones, for example. Many UK banks have introduced face or voice recognition as an alternative to passwords for log-ins or transaction verification, and in some cases, it's both. It also suits consumers who prefer a choice. With other biometric technologies such as iris, palm, vein, heartbeat and even DNA methods coming in the future, our human

characteristics, whether they are physical or behavioural, are the unique ways to identify us.

Now that biometrics are being used in many verticals such as education, healthcare, aviation, automation, IoTs (Internet of Things) and financial services, consumers are already becoming familiar with the idea that biometrics are a fundamental part of the mobile banking landscape. Biometrics are now ubiquitous!

Our Speakers



Andrew Bud, CEO, iProov

Andrew Bud is founder and CEO of iProov, the world's leading provider of online face verification. Previously, he was the founder, CEO and then Executive Chairman of mBlox Inc., which grew to become the world's largest provider of enterprise-to-consumer SMS services and payments, processing six billion transactions a year when it was sold

for \$117m in 2016. His earlier experience includes the role of Marketing Director of Azlan, Europe's largest distributor of Cisco, and the founding CTO of Omnitel Pronto Italia (now Vodafone Italia), and the founder of Europe's first wireless LAN business. He has a degree in Engineering from the University of Cambridge.



Emma Butler, Data Protection Officer, Yoti

Emma Butler is the DPO for Yoti, a digital biometric identity platform. Before joining Yoti in 2016 she spent four years in the Privacy team at RELX Group, also acting as the UK DPO for the LexisNexis Legal and LexisNexis Risk businesses. Before joining the private sector, Emma spent seven years leading the international policy team at the ICO

where her role included working with other regulators and the Article 29 Working Party. She has a degree in French, Italian and linguistics, an LLM in Information Rights Law and Practice, an ISEB data protection certificate, CIPP/E and CIPP/M and is also an IAPP Fellow in Information Privacy.



Ben Carter, Commercial Director, B-Secur

Ben Carter is the Chief Commercial Officer at B-Secur. Ben's experience spans a number of local and global leadership roles in major technology players including Microsoft, Nokia, Pace and Sony.

Specialising in the mobile industry, with experience across global and European operator, retail and distribution channels, Ben manages commercial strategy and GTM, building strong customer relationships.



David Cook, Solicitor Advocate, Eversheds Sutherland

David is a solicitor at Eversheds Sutherland in Manchester specialising in privacy and cyber security compliance and litigation. He advises on a range of cyber security and data protection related legal issues, including the following:

- General Data Protection Regulation: advising clients on how to approach their compliance journey for this new law and its various and onerous obligations.
- Pre-incident readiness: assisting clients in assessing their current ability to respond to cyber incidents or data loss in a compliant manner, providing workshops and advising C-suite stakeholders on their legal responsibilities and liabilities, and then supporting organisations with respect to maintaining an incident response process that will withstand regulatory consideration or customer scrutiny.

- Incident response: advising clients on their legal response to a cyber incident or data loss and translating the technical forensic outcomes to boardroom approach to regulatory engagement, customer notification and/or seeking law enforcement assistance.
- Cyber security compliance: advising and assisting clients on the numerous (and often competing) cyber security laws and regulations that businesses operate within, such as the GDPR, the Computer Misuse Act 1990, the Regulation of Investigatory Powers Act 2002 and the Communications Act 2003.

David also advises on the cyber security impact of the various new laws being introduced across Europe, such as the General Data Protection Regulation and the Network and Information Security Regulations 2018. He regularly provides seminars to academia, law enforcement, lawyers and those in the information security industry.



Steve Cook, expert biometrics and fintech consultant

Steve Cook has previously worked with organisations such as Daon and Facebanx as a sales consultant. He now advises banks, fintech start-ups and investor groups in the area of biometrics. Steve has a strong background in providing guidance in financial services and a good understanding of the latest market trends in the biometrics industry. He also has a wealth of knowledge in the areas of

regulations such as PSD2 and Strong Customer Authentication. Steve is a regular speaker at conferences and the owner of "Biometrics for eCommerce", a LinkedIn business community group with more than 23,000 members. Read more about Steve at

www.bioecom.com



Torgny Hellström, Chairman, Precise Biometrics

Having spent more than 30 years in the global tech industry, Torgny Hellström today is a management consultant and non-executive board member for several companies. He is the chairman of Precise

Biometrics and currently Executive Chairman awaiting the newly recruited CEO's arrival in August.

**Grant Crow, CEO, SmilePass**

Grant is a very experienced, entrepreneurial software (SaaS) CEO with international experience and a track record of leading rapid sales growth in UK based Enterprise SaaS businesses ranging in size from start up to \$40m ARR. Grant has led SaaS businesses in Talent

Management and Strategy Execution and has three successful exits including an IPO behind him. His passion is building great teams who achieve outstanding results.

**Khalil Dimachkie, CTO, SmilePass**

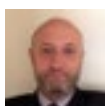
Khalil is a CTO with a difference. In addition to possessing the expected technical qualities and experience in mobile, agile and emerging technologies, he is a commercial entrepreneur. He also writes

and blogs regularly and is a highly regarded speaker at events on emerging technologies and their practical applications.

**Phil Dunkelberger, President and Chief Executive Officer, Nok Nok Labs**

Phil has broad experience resulting from more than 30 years in technology. Prior to leading Nok Nok Labs, he served for eight years as co-founder and CEO of PGP Corporation, the leader in the Enterprise Data Protection market, until acquired by Symantec in 2010. He has significant experience in SaaS infrastructure and enterprise software, having served as Entrepreneur-in-Residence at Doll Capital Management (DCM), President and CEO of Embark, and COO of Vantive Corporation. He has also held senior management positions

with Symantec, Apple Computer and Xerox Corporation. Phil has served on several boards of directors, and currently serves on the Advisory Board of Ionic Security. He is a founding board member of the Cyber Security Industry Alliance (CSIA) and is Chairman Emeritus of TechAmerica's CxO Council. He holds a B.A. in Political Science from Westmont College and is a member of the school's President's Advisory Board.

**Mark Gent, Director Worldwide Sales Engineering, BehavioSec**

Mark Gent is the Director of Worldwide Sales Engineering at BehavioSec AB, a leading provider of AI driven Behavioral Biometric solutions. He has 30 years' experience in the IT industry, in both technical and

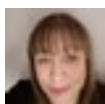
managerial roles, and draws on this to deliver insights into the role of technology in delivering benefits to both business and the public.

**Alan Goode, CEO, Chief Analyst and Founder, Goode Intelligence**

Alan Goode is the CEO, Chief Analyst and Founder of Goode Intelligence – the UK's leading cybersecurity research and consulting company.

With 13 years of research and analysis experience and prior to that, 17 years of senior management and technology consultancy including strategy and deployment, Alan is an expert in biometrics, authentication/identity, fraud management and cyber security. His previous roles include Head of Information Security at T-Mobile UK,

Security Practice Manager at Atos Origin, Head of Digital Security at De La Rue Identity Systems (including biometric passports) and Security analyst for Citibank (Payments). Alan is a frequent speaker and industry awards judge including GSMA Global Mobile Awards for the past seven consecutive years, speaker on biometrics at Connect ID, Biometrics & Identity Conference 2015, MoneyConf 2016 and Lendit Europe 2017.

**Michelle Salway, Senior Director of Sales EMEA, Nok Nok Labs**

Michelle has over 30 years experience in the IT industry with the last 16 years focused on Information Security in high tech sales and products. Before joining Nok Nok Labs, Michelle spent the previous five years as sales and product specialist in Identity and Authentication services for Symantec, and has managed sales organisations in EMEA for PGP TrustCenter and Betrusted. Before moving to the UK, Michelle was GM of Sales and Consultancy at 90East, a Managed Security Services

company in Australia that was acquired by Betrusted. She left her native New Zealand in 2000 after working in senior management roles with both Systems Integrators and Network Services Providers there. She has extensive experience working with Business, Industry and Government implementing strong secure solutions which enhance client experience and deliver value.

**Jeremy White, Executive Editor, WIRED UK**

Jeremy White is Executive Editor of WIRED UK, a monthly magazine that focuses on how emerging technologies affect culture, the economy, and politics. Prior to this role, he was WIRED's Product Editor in charge of all product coverage for WIRED UK, both print and digital - finding the best-looking and top-performing products that are truly WIRED and at the very cutting edge of innovation and design, covering automotive, interior design, technology, sound & vision and watches - plus much more. He also edited WIRED's GEAR section, which highlights and tests the very best in "WIRED" products from smartphones to wearables, nano drones to supercars, interiors to architecture.

His expansive knowledge of the product world and forecasting design and tech trends has seen him be commissioned for consultancy services to some of the world's largest consumer brands on industrial design and user experience.

Jeremy appears regularly on the BBC and Sky News representing the magazine. He has been writing about technology and design for more than 10 years and is also currently the technology expert for Telegraph Luxury and Harrods.

Our thanks to all our wonderful sponsors

Platinum sponsor

STIFEL

Silver sponsors



BehavioSec passively verifies and confirms a user's identity by monitoring how they naturally interact with their device through behavioral biometrics. Clients use BehavioSec to enable risk-based authentication throughout a customer journey. BehavioSec has secured billions of transactions using its transparent approach to identity verification for customers in North America, Europe, and Asia – all without degrading user experience.



Nok Nok Labs is a leading provider of authentication solutions targeting consumer-facing mobile and web applications. It is designed for enterprises seeking to deploy simple, secure and scalable authentication leveraging biometrics and privacy-preserving decentralised authentication and supports emerging FIDO and Web Authentication standards.

Nok Nok S3 Authentication Suite provides an out-of-the-box, FIDO-certified authentication server along with SDKs for mobile clients, authenticators and IoT devices. The majority of its customers are in North America, Europe and Japan, across telecom, financial services and retail verticals. Nok Nok Labs is one of the founders of the FIDO Alliance and author of its primary standards.

PRECISETM

BIOMETRICS

Precise Biometrics is a market-leading supplier of solutions for convenient and secure authentication of people's identity. We develop and sell fingerprint software that provides the market's best user experience and security. Our solutions are used hundreds of millions of times every day by people all over the world and are marketed together with strong business partners. For more information, please visit www.precisebiometrics.com

Hospitality sponsor



Sponsors



B-Secur want to make the world a safer place with ECG biometrics, securing human and technology interaction at its heart.

Our mission is to empower our partners to protect their customers' digital identities and physical lives.



iProov is the world's leading provider of online face verification. It delivers unrivalled spoof detection ("liveness", PAD) using its unique Flashmark technology, on which ten patents have been granted. iProov has been procured by customers such as the US Department of Homeland Security and ING for authentication of users against their photo ID portrait to identity check them for KYC and immigration purposes, and by HMRC for strong customer authentication for repeat authentication. The technology has been recognised by numerous awards from bodies including the NCSC, SINET and Citi. All iProov's technology has been developed by its staff at its base in London, where it has been trading since 2013.



SmilePass uses ground-breaking biometric solutions to manage identification and authentication across the customer journey – controlling the impact of fraud, social engineering and theft.

Launched in 2018, SmilePass is based in London. Our flexible platform works with companies all over the world to build secure and trusted communities. For more information visit www.smile-pass.com



ACUMIN CONSULTING HAVE HIT A MILESTONE:

20 YEARS OF PROVIDING RECRUITMENT SERVICES TO THE CYBER SECURITY INDUSTRY.

Cyber security, information risk management, business protection. The terminology may change but Acumin remains a constant; a trusted industry partner in permanent and contract recruitment, and global executive search. Acumin are a first choice cyber security specific recruitment consultancy for some of the world's leading brands, because when it comes to security there can be no compromise.

We support requirements in many professional areas including technical security, application security, security architecture, penetration testing and digital forensics, counter fraud, information and risk assurance, governance risk and compliance and CISO's and executive management. Our highly trained consultants are subject matter experts, who provide an advisory service tailored to your needs.

**Interested in a new role or a team member?
Contact one of our expert consultants today.**



Contact Us:

email: info@acumin.co.uk

web: www.acumin.co.uk

call: 020 3119 3333

Securing Billions Of Transactions Globally

We believe that great user experiences should never come with risk. BehavioSec has created the new model for strong, multi-layered customer security. Now you can stop fraud, prevent attacks, and authenticate your customers — all without burdening them. We call it behavioural biometrics, and it uses continuous authentication powered by machine learning to verify users. Based not on what they know or do, but how they uniquely engage with their web and mobile apps.

BehavioSec's patented approach can verify who someone is based on how they interact naturally with their apps and deliver instant identity verification alongside continuous authentication. No special sensors. No extra hardware. Enterprises solely have to integrate BehavioSec's Behavioural Biometrics platform to enable their apps to intelligently authenticate their users continuously and protect their online transactions from malware, fraud and theft.

Behavioural Biometrics – a machine learning based approach used to continuously and transparently authenticate the identity of a person based on how they interact with mobile and web apps – has grown in acceptance as part of a multi-layered authentication approach across large-scale production deployments. This evolution in the market has been driven principally by digital transformation initiatives in Fintech throughout apps that support billions of high value transactions across millions of users.

With high profile fraud, theft and cyber security incidents being reported almost every day, security and risk management experts are declaring that passwords and tokens are outdated. Enterprise security practitioners, digital transformation leaders and lines of businesses are conscious of the shortcomings that traditional authentication technologies pose to the digital experiences of their users. At the same time, consumers are demanding a seamless, high quality experience across their mobile and web apps, not endless passwords and tokens that introduce complexity and frustration. So, it is essential that enterprises delivering mobile and web apps provide a means of authentication that does not infringe on user experience. This is where Behavioral Biometrics comes in.

While the initial demand for behavioral biometrics surfaced for Fintech related apps, there is an emerging requirement in other industries where there is a combination of fraud and theft risks associated with apps that put both consumers and enterprises at risk. Looking to the future, any scenario where a user interacts regularly or for extended periods with mobile and/or web apps provides an opportunity to deliver continuous user authentication with behavioral biometrics without burdening user experience. Behavioural biometrics is the future of continuous user authentication in the digital transformation era.



"The first time I was shown behavioral biometrics it astonished me; even working with it full time now, I still enjoy that moment of realisation when you demo it to someone unfamiliar with its capabilities."

Mark Gent, Director Worldwide Sales Engineering, BehavioSec



BehavioSec

The token you can't forget

We transform your behavior
into an extra layer of security.

behaviosec.com



We caught up with Phil Dunkelberger, President and CEO of Nok Nok Labs and, one of the legends from Cyber Security, to ask a few questions about the state of biometrics now and what the future likely has in store for us.



Tell us about how your business has grown and evolved over the past years.

There's been a lot happening! From 2012-2014 we set out a vision to transform the way authentication works, we invented the concept for FIDO, we recruited allies, created the FIDO Alliance and shipped the first versions of our product. Then as our vision was embraced, we created the first secure fingerprint sensor based FIDO authenticator with Validity/Synaptics, Samsung and Qualcomm. We proved that FIDO could work at scale by deploying at scale with PayPal, Docomo and AliPay. Now we're the market leaders in shipping FIDO standards based solutions, with market leading customers including four of the largest banks and four of the largest telcos in the world. And we've doubled our revenue year over year.

We've evolved the FIDO standards with Google and Microsoft, co-authoring FIDO2 to bring FIDO to browsers and operating systems and launched partnerships with Fujitsu, Hitachi, Threatmetrix and others to be announced soon who are taking our products to market.

What's the most exciting innovation you have seen in biometric technology?

We monitor developments in biometrics on three fronts: sensing technology; form factors/usability and security. We're pleased to see all three going through an explosive growth period and we expect to see more biometrics, in more factors than ever before. FIDO of course allows these biometrics and tokens to be used for more than just opening your phone, it allows for secure online and privacy-respecting authentication.

Current biometrics implementations already prevent scalable attacks nicely. We're particularly excited by continuing improvements in the underlying security architecture for biometrics to prevent spoofing and other targeted (nonscalable) attacks. Apple and Samsung have both demonstrated careful attention to detail here using both hardware and software to innovate beyond previous limitations and to raise the bar for attackers.

Where are you seeing the greatest demand for biometrics?

By far it's in reshaping customer experience and enhancing user journeys for customer satisfaction, lowered costs of interaction, greater customisation and increased profit through reduced friction.

The mobile phone has been the most popular device for consumer biometrics to date – what do you see coming next?

Mobile phones and communicators of all kinds will remain the most intense area of innovation and change. We predict changes in the form factor as battery life and radio technology get better and "unbundling" of phone features (e.g. into a data brick in your bag or a smart ear-bud you wear). In the future, biometrics will be everywhere as the "gesture" to authorise and activate these interactions.

How do you think Machine Learning (ML) and Artificial Intelligence (AI) will be used in biometrics?

Spoofing and detection of attacks is one area, more accurate template matching is another. Algorithmic techniques complemented by ML can enhance effectiveness; the challenge is doing it with minimal battery drain and to keep getting better with more use.

For those thinking about developing biometric technology, what one piece of advice would you give to them?

Keep in mind that the journey from working in the lab or limited environments to working in a commercial setting at a hundreds of millions of user scale is a long one. We've seen companies fail to integrate into required form factors, miss the quality goals, fail usability and be broken or defeated trivially in a way that would prevent any kind of mass deployment. The reason why fingerprint sensors got as good as it is, is because it took 20+ years of R&D and over a billion dollars of capital went into the sector.

And for those looking to deploy biometric technology in their organisation, what are the key things that you would advise them to consider?

Start with technologies that consumers are familiar with and whose technology performance and security characteristics are well known. Make sure you create a threat model and understand the security and privacy model of your biometrics implementation. Consider using FIDO as a shortcut to get the security, quality and privacy implementation of biometrics vs. "rolling your own".

nok nok



Strong Customer Authentication Made Easy

Phishing Resistant | Decentralised | Privacy Ready

The UK Government reports on its website that “technology businesses are at the heart of the UK economy and are playing an important role in driving growth across the country, from financial services and high-value manufacturing to retail and agriculture”. It attributes the UK’s “outstanding environment” to the following factors:

- a strong start-up culture bolstered by technology clusters all over the UK
- a ranking of fifth best place in the world in the Global Innovation Index in 2016
- 4 of the world’s top 10 universities, plus educational providers that develop our technology workforce

But what does all this mean for UK biometrics businesses? We spoke to the CEOs of three leading UK-based vendors – B-Secur, iProov and SmilePass – to find out.

What are the benefits and barriers of building a technology company in the UK?

Andrew Bud, CEO, iProov: “The UK is in most respects a wonderful place to build a technology company. Establishing and administering a company are simple and low cost processes, and skilled Board members are not deterred by excess risk. InnovateUK has proved to be an outstanding supporter of innovative technology SMEs with its grants, which enable companies to cut the financing demands of addressing hard technological challenges.

“The tax regime is very supportive: R&D tax refunds represent a very meaningful source of funding, EIS encourages investors to support growth companies on their way up, the Patent Box enhances business returns and EMI is a great way to provide options to the key staff needed to build a technology company. Labour law is flexible enough to recruit good people and exit poor performers without excessive damage, and the legal environment is transparent, comprehensible and not corrupt. Our universities produce staff trained to think as well as to know, but competition for good staff is becoming intense and salary costs are spiralling dangerously, especially in London.

“If there is a real weakness, it is the absence of an effective mid-cap equity market for high growth technology firms competitive with, for example, Sweden’s Nasdaq Nordic, to provide crucial liquidity options for UK technology companies.”

Grant Crow, CEO, SmilePass: “On the benefits side, we have access to a wide pool of talent, including talent with an international mindset and linguistic capability. And there are generous taxation allowances for compliant management incentive schemes. Over the past five years, VC and related funding has become more widely available and competitive. For the barriers, there is still significant distrust of cloud security among tier one enterprise. It’s also a highly regulated environment and this raises costs and takes time.”

Alan Foreman, CEO, B-Secur: “The UK, and especially Northern Ireland has an amazing talent pool of engineers who are helping amazing companies do amazing things and it has been a real benefit to us of setting up in Belfast. One of the things that I would say is a barrier, is that the level of investment into tech companies in the UK is still nowhere near that of the US. It probably means we will have to expand our investment search into the US during our next investment round.”



Andrew Bud
CEO
iProov



Grant Crow
CEO
SmilePass



Alan Foreman
CEO
B-Secur

What's the impact of machine learning and AI on biometric technology?

Alan Foreman: "We are using machine learning techniques and AI to help us learn more about a User every time they authenticate to get into their device. This allows us to build up a profile that can enhance our security and prevent spoofing but can also enable us to go beyond authentication and look at whether a user is stressed, fatigued or potentially unwell when they access their device."

Andrew Bud: "Machine learning has changed everything in biometrics. Previous biometric solutions based on statistics and algorithms had found limits to their performance, limits which imposed often unacceptable constraints on the user context, behaviour and experience. Deep neural networks, if trained on large data sets and tuned correctly to specific use cases, outperform the old methods by orders of magnitude. This is a qualitative change, making some real-world solutions feasible and attractive for the first time."

"However machine learning and AI are also potent tools for attackers, enabling the creation of utterly credible fakes if given the chance. For the first time, biometric scores have become lethal attack vectors, enabling adversarial AI attacks to produce beautiful forgeries that outperform real humans if given the chance. Biometrics will become an arms race between the AI on both sides, won by whoever can protect their methods better."

Grant Crow: "The impact has been massive. Advances in these applied technologies are mainly what is responsible for making biometric modalities like face recognition fast and usable. The old approach to face recognition software was not very accurate and extremely dependent on aligning your face correctly and having the right lighting. Machine learning and AI techniques have allowed the development of very robust and adaptable algorithms."

"However it is important to note that there have not really been any major theoretical/mathematical breakthroughs in AI since the 1970s. It is just the hardware that is now cheap and powerful and has enabled the application of techniques that used to be purely theoretical."

What is the impact of biometrics on identity and authentication?

Grant Crow: "Biometrics has the ability to both simplify and increase the security of authentication at the same time. The simplification comes from having a modality/factor that allows the person to verify themselves without having to know or have anything."

So, device vs cloud – what's the best model for biometrics?

Alan Foreman: "Every use-case will have benefits and drawbacks of both solutions; either cloud-based or device-based or both. We work with our clients who integrate our technology to ensure that we deploy our algorithms in the most valuable and secure way."

Andrew Bud: "Devices and cloud must work in tandem, each with their own role to play. Biometric data collection is the job of the device, as it becomes ever more richly endowed with sensors. But biometric analysis must be done exclusively in the cloud. In a world of AI-based attacks, reverse engineering becomes fast and horribly effective. Handing the biometric matcher and/or spoof detection system, in a device, to an attacker will enable the rapid and inevitable development of totally effective, scalable and low cost attack methods. Protection against fakes becomes critical, so it is essential that the biometric analysis processes be done in the cloud and not on the device."

"Keeping the biometric template itself secret is necessary but less crucial for security because biometric systems are not shared secret systems – at least, not when the biometric is public to begin with, like the face. Possession of a device is one great factor in authentication: beyond that, device-based biometrics certainly provide great convenience, but they don't provide much additional security. Instead, cloud-based biometrics are the future of strong authentication."

Finally, when you look beyond authentication, what other non-authentication use cases and applications will be transformed by biometrics?

Grant Crow: "Retail and occupier analytics is a major one. The technology exists to track how people use retail or office space through facial recognition while still maintaining anonymity. This data can be used to compile very powerful insights into the usage of physical space and footfall."

Andrew Bud: "Authentication is such a rich seam to mine, as it addresses the fundamental issue of trust in the online ecosystem. Biometric authentication can assure persistence of an online persona, by confirming it's always the same human behind each successive interaction, even if their real-world identity is forever unknown. Conversely, it can link a real-world identity to an online identity, by confirming that a person is the genuine owner of a trusted identity credential. This is already a fast-growing use for biometrics in remote, online ID matching for onboarding KYC and remote border control, where biometrics can far outperform even humans in matching a selfie to a passport photo. In a future ever more polluted by bots, fake identities and synthetic imagery, trusted biometrics will be one of the few defences separating truth from lies."

Alan Foreman: "We are currently using ECG biometrics to determine a user's stress, fatigue, drowsiness, atrial fibrillation, respiration rate, medical grade heart rate and more. This allows us to build many more use-cases using our data than just a challenge and response authentication. We are seeing lots of traction for these use-cases within vital-signs monitoring in the automotive industry and within healthcare data in wearables."



Biometrics for eCommerce is the largest active biometric community news group on LinkedIn with more than 23,000 members. It specialises in biometrics being deployed with mobile devices, payments, authentication and digital on-boarding, mainly within the financial services sector. Members regularly post general articles of interest and group discussions. You are welcome to join.



BiometricUpdate.com is the leading news property that publishes breaking news, analysis and research about the global biometrics market.



FindBiometrics is your leading industry resource for all information on biometric identification and identity verification systems and solutions. We have the latest daily news from the global biometric and identity management business community, a comprehensive vendor list, informative articles, interviews with industry leaders, exclusive videos, links to biometric associations and a calendar for the most important and current industry events and conferences.

For more than a decade we have brought you the top industry news, answering all of your questions, and have remained an integral player in the biometrics community. Now, here in the industry's most rapid growth period, we are here to keep you more connected, knowledgeable, and up-to-date on the latest identity management news than ever before. FindBiometrics is also a proud member and longtime supporter of the International Biometric and Identification Association (IBIA).

FindBiometrics is a division of TopickZ Inc. TopickZ is a progressive electronic information resource company, led by a team of experienced and award winning professionals. With a proud history, and bright future, TopickZ has a passion for informing and educating by embracing all of the opportunities created by the rapid growth of technology, digital media, and mobile. The company is privately held and does not trade on equity markets.



With more than 38 years of combined experience in the industry, our dedicated editorial leadership team has lived and breathed biometrics as the sector has rapidly evolved. Every day of the week, our editorial team analyses, interprets and disseminates breaking biometric news on market trends, new technologies, government policies, privacy issues and more.

Our readership has grown exponentially since our launch in 2010 and today Planet Biometrics is seen as the critical news resource for biometrics industry professionals.



With over 30 years' experience in the global tech industry and, as the Chairman of an evolving company, which over the past three years has grown to around 50 employees with over 30 customers in different geographical regions across the world,

including market leaders and vendors with new technologies, Torgny Hellström has an acute understanding of the Biometrics market. And he's clear about how to grasp the opportunities and face the challenges in order to be successful, particularly for any new entrants into the market. "Be clear. Put the users first and ask 'how can their everyday life become easier by using biometrics?' Then bring a product fast to the market."

Of course, as with any market, it also takes a careful balance of time,



resource and innovation to be successful. It's a big challenge to ensure both a high level of biometric performance and a good user experience of sensor technologies. Torgny explains that "fingerprint sensing under the smartphone's display is a very exciting innovation. The demand for sensors that can be placed beneath the screen or the glass is being driven by the new smartphone designs with edge-to-edge displays. Our experience shows that optical and ultrasound sensors work best as they provide a better user experience and simplify the mobile phone production process. We have over 20 years of research in fingerprint biometrics at Precise Biometrics, and we're now leveraging this knowhow to optimise our fingerprint software for these sensor technologies, making sure that our customers' solutions provide a great user experience and are easily integrated in smartphones."

Biometric smart cards – a more convenient and secure alternative to PIN code-based payment cards

- Biometrics open up the opportunity to lift or raise purchase caps on contactless payments, making it more convenient for cardholders while also complying with card issuer security
- Fingerprint biometrics provide a high level of security and prevent fraud – a concern for many contactless payment cards users
- Retailers can benefit from higher in-store throughput without making additional investments
- Banks and payment providers can reduce payment card fraud
- Consumers are ready to engage as they are used to the convenience of using fingerprint authentication instead of PIN codes through their smartphones

So what are the key market trends that are most important for Precise Biometrics at the moment?

"The greatest demand is from mobile, where we are seeing continued growth of fingerprint technology. This year, we expect to see close to 900 million smartphones with fingerprint biometrics – that's a 20 percent year-on-year growth. The market for fingerprint technology in mobile phones continues to change at a rapid pace and we've seen the start of a technological shift in the sensor market from capacitive sensors to optical and ultrasound sensors. During the first few months of this year, a number of mobile phones featuring these technologies have been launched, and the market is showing an increasing interest.

"Another key trend is the emergence of biometric smart cards and this is expected to grow significantly in the coming years. The first market trials



of biometric payment cards were initiated in 2017 and this year, several commercial pilots of contactless biometric cards have started across the globe – in Europe, Japan, Middle East and the USA. Put simply, Biometric payment cards provide a more convenient and secure alternative to PIN code-based payment cards and are set to gain widespread acceptance.

"Looking ahead, privacy and the protection of individuals' data is becoming more and more important, you just have to look at the advent of GDPR. Biometrics can further increase the protection of data and people's identity,

as it offers improved security compared to pins and passwords. We also think that machine learning and AI will be used more. For many years already, fingerprint biometrics have been using machine learning and that area is still evolving. Advanced (or heavier) biometrics such as face require dedicated AI engines to give an acceptable user experience. Likely other modalities will be able to use these techniques too to become more secure and user friendly."

What GDPR means for Biometrics

It's just been a matter of weeks since the General Data Protection Regulation (GDPR) was introduced. While there is no single over-arching piece of legislation that covers the collection and use of biometric data, there are a number of different laws that cover the area of privacy around biometrics, including the GDPR. As Emma Butler, Data Protection Officer for Yoti explains, "In the UK there is no specific biometric legislation but biometric data used to identify an individual is classed as 'sensitive data' under data protection law. This means it is subject to particular rules and safeguards and its use is more restricted. In addition, the US has specific biometric legislation in several states". David Cook, Solicitor Advocate at Eversheds Sutherland adds, "What we have is a patchwork of different laws that go some way in covering the area in relation to the holding and use of this material by the state, by employers and by commercial organisations." These laws include:

- Data protection law in the form of elements of the General Data Protection Regulation and the Data Protection Act 2018
- Human rights laws with respect to the right to private life under Article 8 of the European Convention on Human Rights and Schedule 1 of the Human Rights Act 1998
- Oversight on the use of biometrics by the government, through the Commissioner for the Retention and Use of Biometric Material, a role that they are obliged to fill by Section 20 of the Protection of Freedoms Act 2012

The newly introduced GDPR covers the use of personal data by organisations and "sets out quite onerous obligations around what they do with personal data, with a sub-category of personal data which has additional safeguards, says David.

"The main impact is the change in classification from 'ordinary data' to 'sensitive data', says Emma. "This means that in certain circumstances the lawful basis an organisation used before 25 May now needs to be supplemented by an additional lawful basis for sensitive data. In the UK, national law has retained the fraud prevention lawful basis for processing sensitive data, which is often the purpose of biometric data processing. However, this does not exist in other EU countries' national law, making it more difficult for organisations wanting to operate across the EU. GDPR allows for Member States to introduce additional lawful bases for sensitive data, but so far, to my knowledge, only the Netherlands and Croatia have done this for biometric data.

"Many organisations may now need to use explicit consent as their lawful basis instead and so need to provide for that consent to be withdrawn, as well as the additional rights attached to using consent as a lawful basis. Where organisations offer online services to children that involve biometrics (children are defined differently in different Member States) and they use consent as their lawful basis, they will need to age gate and get parental consent.

"In addition, there is a particular difficulty for employers using biometric access controls for increased security reasons, given consent in this employment context would not be considered valid.

"Finally, organisations collecting and using biometric data on a large scale will now be legally obliged to carry out a privacy impact assessment."

David continues, "The GDPR sets out very stringent requirements on organisations to demonstrate why they need to process biometric data. The ongoing compliance with the GDPR after that point is also an issue: a breach of the GDPR in relation to biometric data will be seen as a significant breach. The Information Commissioner's Office (ICO) has previously stated that a security breach around sensitive data affecting even a single data subject could be considered serious enough to warrant a monetary penalty."

So, what should an organisation be considering when it collects and uses biometric data? In Emma's opinion the same basic considerations apply to any proposed collection and use of personal information: "Why you are collecting it; what you will do with it; where you will store it; who will have access; and how you will secure it. It becomes more important with sensitive data like biometrics to have suitable security and access controls and to consider if your collection and use is ethical, fair, proportionate and justifiable. The lawful basis you use will also dictate other obligations and requirements."

The processing conditions set out with respect to the GDPR demonstrate the scale of the task. An organisation considering the use of biometric techniques also needs to consider the GDPR principle of Data Protection by Design and by Default. "The use of new technology like biometric techniques, on a large scale and using automated processing, leads to an obligation to undertake a Data Protection Impact Assessment (DPIA)" says David. "If the DPIA established that the proposed use of biometrics presented a high risk to the rights and freedoms of individuals, then the organisation should consult with the regulator before proceeding. In certain circumstances, the organisation should also consult with the individuals likely to be affected. These are seriously rigorous safeguards to ensure that the use of biometric data is only ever carried out in limited circumstances and, even then, with the risk to those affected kept absolutely minimal."

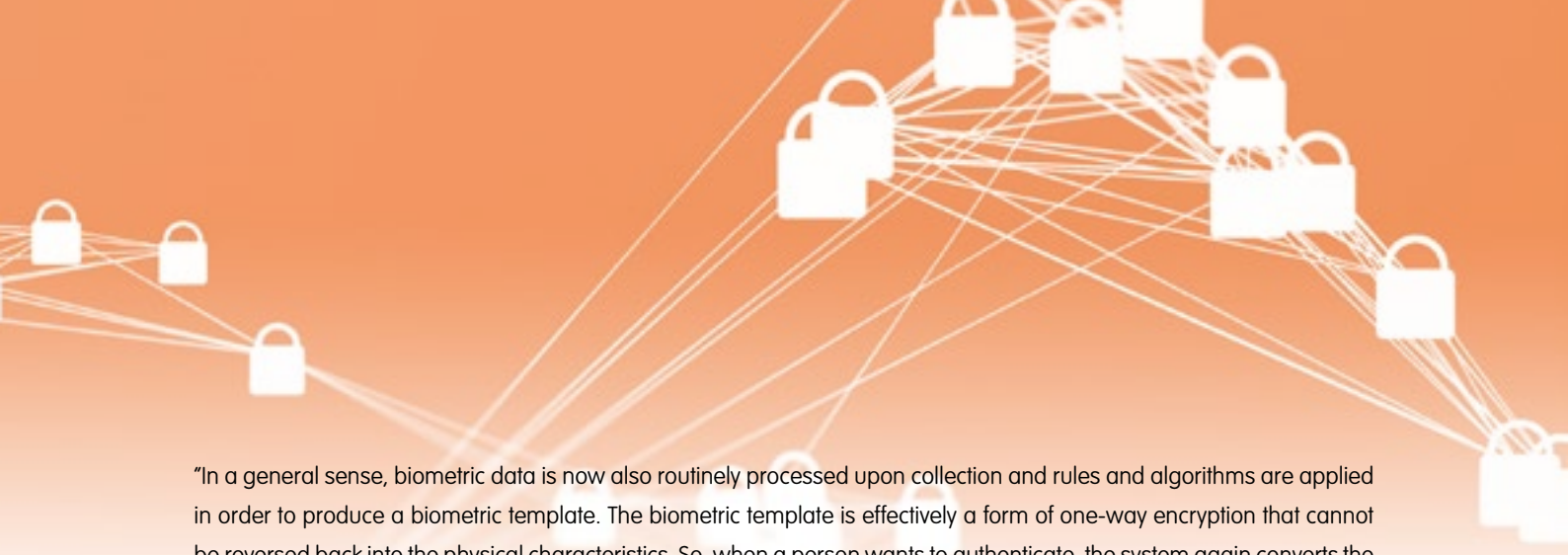
Making sure that biometric data isn't stolen or re-used is critical so it's important to have the right technology controls in place. According to David, fairly sophisticated security approaches are being deployed to meet this need. "A good example is the iPhone which routinely deploys fingerprint scanning technology to authenticate the user. The use of the biometric data is limited to authentication protocol and no more. Biometric data is stored within the Apple Secure Enclave security chip on the phone and is not stored on Apple servers or via the iCloud.



David Cook
Solicitor Advocate
Eversheds Sutherland



Emma Butler
DPO
Yoti



"In a general sense, biometric data is now also routinely processed upon collection and rules and algorithms are applied in order to produce a biometric template. The biometric template is effectively a form of one-way encryption that cannot be reversed back into the physical characteristics. So, when a person wants to authenticate, the system again converts the biometric characteristics by this process and it is the conversion data that is compared against the template. The biometric characteristics are not stored; just the template.

"This process is broadly similar to how systems authenticate passwords: a user types in their plain text password, which is processed by a security algorithm and might be hashed and salted and it is the product of that process that is compared against what is stored – the plain text password is not stored and the risk to individuals is minimal if the stored password 'template' is lost.

"Having said that, there will be circumstances in which biometric data is lost by organisations. In order to prevent it from being re-used to allow access to information and devices that should not be allowed, we are now seeing the increased use of multi-factor and multi-modal authentication: the biometric data is not the only data to be provided and the person must still use another form of verification in order to authenticate."

Using Artificial Intelligence (AI) alongside biometric data is another key area for consideration. Emma says "There are certain countermeasures to prevent exposure of private information when training on sensitive biometric data. Privacy-preserving machine learning is a research line that focuses on developing countermeasures against attacks which try to reverse engineer a trained machine learning model. These countermeasures can be roughly categorised into two groups: those that work to prevent the model relying too much on the data of any specific individual during training; and those that deliberately add noise to the training data."

In David's opinion, the combination of artificial intelligence and biometric data is one that might be expected to be high risk and therefore something for which the regulator must be consulted about. "The GDPR sets out that a DPIA should be carried out for the use of new technology and the ICO has issued guidelines that state that it expects a formal assessment for the use of artificial intelligence." Explaining this further, David says "The GDPR seeks to cover the use of behavioural characteristics such as biometric data and the determination and definition of those characteristics by an artificial intelligence platform is a prospect that most people would find alarming. The GDPR sets out to tumble such an idea through a set of cogs and mechanisms and deliver a compliant product at the end of it through the organisation: processing only in specific and limited circumstances, being transparent around what is proposed; implementing Data Protection by Design and by Default; completing a DPIA and consulting with the regulator and data subjects as necessary and, complying with the onerous terms of the GDPR regarding sensitive data."

It's not clear yet how this all works in practice however David is certain that 'novel and new technological advances are going to occur and are going to test the terms of the GDPR. What data subjects find acceptable will also shift over time. It's clear however that the GDPR enforcement regime can be unforgiving and organisations that want to conduct such practices will need to be squeaky clean from a data protection or privacy perspective in order to manage the commercial risk."

We are a leading cyber security research, analysis and consulting organisation founded in 2007 and based in London. We work internationally with technology vendors and service providers to inform, educate and influence. Our services are used by a range of clients, from established super-brands through to hot, emerging start-ups and market disrupters.

Inform – keeping you up-to-date on the latest market trends in cyber security through our primary research, analyst reports, market intelligence and surveys. Our proven qualitative and quantitative research is matched to your specific needs to help you make informed business decisions.

Educate – through our integrated go-to-market services, we can help you create understanding about your brand or a new product – targeting your customers, investors or partners – to show why your offering is applicable and relevant.

Influence – once people know about and understand your product or service, we'll help you win over and inspire the market, driving your sales. Our strong success in influencing stakeholders draws on our robust foundation of primary research and data, supporting company brands and products to show how you add value.

Research and Analysis

- Off-the-shelf research including:
 - Analyst and market forecast reports
 - Market surveys
 - Insight reports
 - Monthly Market Intelligence reports
- Custom Research

Visit our website:
www.goodeintelligence.com

Custom Research

- White Papers
- Product evaluation reports
- Webinars
- Analyst-led events

Consultancy

- Technology vendor strategy and advisory
- End-user consulting
- Investor services
- Security awareness and engagement



Goode Intelligence Biometrics for Banking – Market and Technology Analysis, Adoption Strategies and Forecasts 2018-2023 – Second Edition

This report is the first in a three-part series – Biometrics for Financial Services – and investigates the current global adoption with market analysis including key drivers

and barriers for adoption, interviews with leading stakeholders, technology analysis with review of key biometric technologies and profiles of companies supplying biometric systems to banks. It also includes regional and global market forecasts for users and revenue for the six-year period from 2018 to 2023.

Biometrics for Banking is available at US\$5,000.00 for an Enterprise licence.

Author: Alan Goode
Publication Date: June 2018
Number of Pages: 253



Goode Intelligence Biometrics for the Connected Car – Automotive Biometrics Market Analysis & Forecasts 2018-2023

The Goode Intelligence Analyst Report Biometrics for the Connected Car is the first report in its IoT series and covers market analysis and forecasts for the adoption of

biometrics for the automotive industry.

This report is available at US\$5,000.00 for an Enterprise license.

Author: Alan Goode
Publication Date: Nov 2017
Number of Pages: 163



Goode Intelligence Mobile & Wearable Biometric Authentication Market Analysis and Forecasts 2017-2022

The fourth edition of Goode Intelligence's highly influential market analyst report provides an investigation into the use of biometrics for authentication on smart

mobile and wearable devices. The updated report includes impact analysis on Apple Face ID and new sections and forecasts on facial recognition hardware.

The Mobile & Wearable Biometric Authentication report is available at \$5,000.00 for an Enterprise license.

Author: Alan Goode
Publication Date: Sep 2017
Number of Pages: 188

BIOMETRICS FOR THE CONNECTED CAR



Seven Key Applications for Automotive Biometrics

Goode Intelligence

- 1 VEHICLE ENTRY**
You protect a \$500 smartphone with a biometric but not a \$50,000 car. Digital keys on smartphones unlocked by biometrics will become a dominant method of accessing your vehicle.
- 2 ENGINE START**
Either through a biometric sensor integrated into a car or via your smart mobile or smart wearable device.
- 3 CAR PERSONALISATION**
Supports both owned and ride-sharing models. Biometric identity allows a car to be personalised for each driver.
- 4 IN-CAR PAYMENTS**
The car as a payment method for road tolls, drive-through restaurants, petrol and electricity re-charge. Biometrics to support convenient payment authorisation.
- 5 INSURANCE**
Supporting 'Black Box' telematics by knowing exactly who is in the car.
- 6 HEALTH, WELLNESS & WELLBEING (HWW)**
Continuous monitoring of drivers for tiredness, illness and intoxication through face, ocular, ECG and even EEG biometrics.
- 7 VEHICLE TO HOME AUTOMATION**
The connected car meets the connected home.



Information taken from the Goode Intelligence analyst report "Biometrics for the Connected Car - Automotive Biometrics Market Analysis & Forecasts 2018-2023"

Notes

