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."