validsoft
Voice. Identity. Guaranteed.

# The Beginning or the Beginning of the end for Behavioural Biometrics?

## How Artificial Intelligence Will Determine the Future of the User Interface and User Authentication

As advances in and uses of Artificial Intelligence (AI) continue to grow and expand, a recent article in a journal suggesting that behavioural biometrics are the future of user authentication raises a number of questions around the veracity of the claim and, more importantly, the very future of behavioural biometrics as a viable means of authentication.

By way of background, behavioural biometrics are based on measurable patterns in human activities and, in the context of authentication solutions, include keystroke, mouse and even signature analysis.

**"The future Human User Interface will determine the method of User Authentication".**

Physiological biometrics, on the other hand, are based on physical human characteristics such as face, voice, fingerprint, and iris recognition, amongst others.

Behavioural biometrics were originally used in the second world war to determine who was sending a morse code, by examining the rhythm of the code. In today's world, the communication mediums for behavioural biometrics is no longer the telegraph but the keypad, mouse and touchscreen. So rather than the rhythm of the operating tapping out the code, the dynamics of today include seek and hold times of keys, use of left or right shift keys, speed of typing, common spelling errors and corrections, mouse pressure and angle of movement and even the angle at which a device is held.

This raises the first issue on the aforementioned claim on the future of user authentication being behavioural biometrics. What if the future of User Interfaces isn't based on keyboards, mouse pads or pointing devices? What if it's based on an interface that isn't actually measurable by any behavioural dynamic? Or, and most likely, it will be a combination of channels comprising those that enable behavioural biometrics and those that don't. The ability to leverage behavioural analytics will be driven by the channel and interaction the user is performing. As we move towards the unification of customer engagement this disparity in the authentication of users will ultimately cause it to fail.

**"Natural Language Understanding (NLU) is driving the change in interaction".**

That is exactly what is happening today and, in an article published within the same journal, the author opines that voice is the next User Interface. This is an opinion shared by many, including Facebook, Amazon, Microsoft, Google, and Apple, and is based on the fact that AI chatbots and the improvement in Natural Language Understanding (NLU) is driving the change to how we will increasingly interact with organisations and machines in the future. All of the aforementioned organisations, and others, are actively developing their AI capabilities in the area of NLU as keyboards, mousepads, touch screens and pointers don't exist in their vision of the migration to the human user interface. We are, in fact, already using voice as a human user interface with personal assistants on our phones and tablets, our home speakers and even our cars. The natural progression, and one that has already commenced, is the replacement of today's structured web-based forms with interactive NLU-based interactions.

Secondly, and as alluded to previously, the concept of the omni-channel customer experience is also at odds with behavioural biometrics being the future of user authentication. In our dealings with human agents and AI chatbots in organisations' contact centres, there is no interface that supports behavioural

biometrics. The interface, once again, is voice and it is a physiological biometric that seamlessly and invisibly authenticates this, i.e. voice biometrics.

Voice biometrics is in fact the future of user authentication because the method of biometric, or human authentication must align with the human user interface. Only voice authentication can authenticate voice commands or conversations, whether over contact centre channels, web browsers, which already obviously accept audio commands, apps, smart speakers, automobiles or IoT devices. Measurable human activities based on physical movements of humans or hardware devices will not be applicable when those hardware devices are no longer the common UI. Furthermore, selecting an authentication model intrinsically tied to a specific UI is, in effect, creating a security model that cannot support a true, evolving omni-channel engagement strategy.

**"Measurable behavioural analytics do not exist in a voice UI".**

The other major concern with behavioural biometrics becoming the future of user authentication is to do with AI itself, and in particular the advances in machine learning. There are many machine learning tools, one example being Generative Adversarial Networks (GANs), which are particularly adept at producing audio and video deepfakes, based on genuine datasets, i.e., recordings, photos and videos of real people, used to train the system.

But whilst high quality deepfakes have the ability to fool humans into believing they are genuine, that is not the case with advanced physiological biometric engines. Whilst synthetically generated deepfake audio of a particular person may sound perfect to the human ear, an advanced voice biometric engine can discriminate between audio produced by a machine and that produced by a human vocal tract.

With the proliferation of malware infecting all devices today, it won't just be the banks or other legitimate organisations that are collecting behavioural metadata from keyboards and mice. If malware can collect this data, along with device and browser metadata, commonly used to passively authenticate a user, it is entirely logical to predict that GANs and other ML tools could also generate behavioural patterns of keyboard and mouse usage. Combined with some "noise" to compensate for being too accurate, behavioural biometric solutions don't have the same ability to discriminate between synthetic and genuine, given the lack of physiological component.

**"AI will advance both human interaction with machines and advanced fraud"**

AI, depending on how it's used and who's using it, will be both a force for advancement in how we interact with computers and therefore organisations in the future and, conversely, a force for more advanced fraud vectors based on machine learning technology. Neither scenario would appear to promote the idea that behavioural biometrics will be the future of user authentication, in fact, quite the opposite. The real question is, is this the beginning of the end for behavioural biometrics!