# A QUESTION OF TRUST

**Salvatore Sinno** *examines the changing face of biometrics in the light of the upcoming GDPR*

**For yet another year, 2017 saw "123456" and "password" being among the most popular passwords adopted by users. While some of this can be attributed to end-user security reticence and general lack of awareness, a lot of this is down to password overload and fatigue.**

Given the number of high-profile hacking and ransomware cases that occurred over the last year, this apparent apathy to password management is alarming. But it's easy to empathise when the average user, who more than likely has numerous online accounts, chooses to adopt a simple and hackable password for the sake of ease and speed of access.


**Fingerprint scanning is becoming increasingly common on phones**

At its core, biometric authentication was designed with this specific challenge in mind. It allows users and service providers to harness the ultimate in exclusive secure access – individual biological identifiers. However, as the technology becomes more accessible the final piece of the puzzle is reassuring the public so as to build trust between them and service providers.

In a recent survey looking at public perceptions of biometrics commissioned by Unisys, I welcomed the resounding indication that the public was ready to adopt biometric authentication.

The survey, which examined the attitudes of 3,500 people across seven European countries, revealed that just under seven out of 10 people (68 percent) said that they would trust organisations more if they used biometric authentication. Of those in favour of biometrics, fingerprint signatures were found to be the authentication method citizens would be most comfortable adopting (61 percent), indicating a willingness to ditch the password altogether.

## FINGERPRINT IDENTIFICATION

As fans of the Bourne trilogy will testify, fingerprint identification played a key role in getting Jason Bourne both in and out of trouble. It's such a simple concept to grasp and visualise on the big screen; having had his memory erased, the last thing Bourne was capable of doing was remembering a bunch of passwords. Full hand imprint scanning technology meant a world of assets and car chases awaited him.

> **BIOMETRICS WILL RAPIDLY BECOME PART OF MODERN SOCIETY'S SECURITY VERNACULAR**

Whether Hollywood inspired or not, the ease of user experience and security that fingerprint signatures offer is obvious. All the major smart device manufacturers have caught on to this having already introduced fingerprint scanning or Touch ID as access options for users, with over 90 percent of fingerprint reading activity taking place on these devices, according to Deloitte. Meanwhile, both retina scanning and facial recognition are also being integrated into recent versions of popular smart devices. This will further normalise a wider range of biometric authentication in everyday use. In fact, retina scanning was already acceptable to 41 percent of the sample surveyed by Unisys.

That users feel a greater sense of confidence in, and are perhaps a little enamoured by biometric technology is one thing. But the research from Unisys also exposed a lingering, lower level of trust in organisations to actually manage and store this data.

Drawing on the results, 47 percent of consumers are comfortable with fingerprint details being kept 'on file', but on average, 53 percent express some level of concern for precisely how the data is stored, and where it is used.

So, while the research proves that biometrics is seen as an enabler of organisational trust if it gives users a more seamless, secure and frictionless experience, there is also a basic discrepancy between the willingness to exchange biometric data and a lack of trust in organisations to keep it safe and use it wisely.

According to the survey, banks garnered the most trust (51 percent) followed by government institutions (45 percent), with over 27 percent of those surveyed having no confidence that any organisation can be trusted with managing and storing their biometric data.

But why is the level of distrust quite so high? Let's face it, biometric data is deeply personal. If people share unique physiological identifiers like facial features, iris scans and fingerprints, users will need to possess a high amount of trust in those organisations that are responsible for managing it.

This isn't painting a gloomy picture of the future of biometrics. On the contrary, as the physical and cyber worlds converge, the enhanced customer experience and the ability to offer robust and controlled security access means that biometrics will rapidly become part of modern society's security vernacular. However, what this also means is that policy makers will need to create standardised frameworks that address any public perception and distrust with clearly written and communicated policy. At its heart, any policy will inevitably need to enable implicit end user consent and awareness.

The upcoming GDPR (General Data Protection Regulation) is a positive step towards defining the future of regulating biometrics in a way that its predecessor – the Data Protection Act of 1989 – didn't. The GDPR now clearly identifies biometric data as a specific category of personal data, grouped under sensitive data. While there hasn't been a monumental shift to the position of how organisations handle biometrics per se, by highlighting it as sensitive data, companies will now be required to tread with utmost care when processing and managing this data.

Policy makers also need to keep up with the fact that the technology is additionally rapidly evolving. For example, a number of high-security workplaces have introduced 'behaviourmetric' authentication. Behaviourmetrics looks beyond physical identifiers and analyses the highly unique intricacies of personal behaviour, for example typing patterns, gait and voice. Behaviour-based biometrics are proving invaluable for enabling water-tight, multifactor security access.

## LEAP OF FAITH

It's easy to see how this might be useful outside the work place – for high-level security access to personal bank accounts or at passport controls in airports, for instance. Behaviourmetrics is a great example of how biometric systems are getting more nuanced, sophisticated and integral to secure access systems. However, it also requires the leap of faith for users to trust organisations with data will become greater. The onus is on policy makers at both a government regulatory and organisational level to provide the necessary checks and reassurances required to build this trust.

It's likely that in the future policy makers will also need to be more prescriptive and precise when

creating policy around the management of biometric data, but this is no simple task.

Today, multiple biometric solutions are available, each with their own standards, frameworks, and security objectives. This poses something of a challenge when considering regulation of data and policies to support this. Increasingly, organisations are looking to implement Federated Identity

## 47% OF CONSUMERS ARE COMFORTABLE WITH FINGERPRINT DETAILS BEING KEPT 'ON FILE'

Management systems, which is an arrangement that allows multiple enterprises to let people use a single electronic identification to access a number of different services.

Aside from the obvious benefits of Federated Identity to the customer experience, it also gives policy makers an opportunity to focus their regulations on existing biometric frameworks. Rather than simply creating standards from scratch, by actually utilising the biometric frameworks that have been created, they can evolve these dependent on the use case.

This would, in turn, allow a small number of profoundly successful and secure biometric authentication infrastructures, to be utilised by whole markets, with a regulated and tested security and operational underpinning it all.

### CONTINUED GROWTH

Biometrics is no longer simply a "cool" piece of technology innovation for our entertainment. As the use cases for safe, secure biometric authentication continue to grow in scope and reach, we can imagine a society where secure authentication becomes a seamless part of our daily lives.

While the primary driver is to enhance the user experience, and this is clearly welcomed by the public, organisations will need to continue to work on building trust between all stakeholders for the long term. Public awareness and consent, underpinned by unambiguous policy will no doubt be key to a more secure digital future for all

**Salvatore Sinno** is the Global Chief Security Architect at Unisys. Salvatore leverages advanced products, efficient managed services and vertical expertise to develop customised security architectures for his clients.

**Users have a low level of trust in organisations to manage and store their data effectively**