BIOMETRIC AUTHENTICATION IS THE FUTURE OF SECURITY — AND IT'S HERE NOW

By Andrew Tait

BIOMETRIC AUTHENTICATION — what was once sci-fi fantasy is now reality, and it's quickly gaining steam on a global scale. For example:

Apple introduced biometric authentication into their line of iPhones in 2013 with Touch ID[1], a fingerprint recognition system use to unlock the phone. They recently went a step further, introducing Face ID[2] with the iPhone X, a facial recognition feature meant to replace Touch ID.

Iris scanning technology is being introduced to India's national biometric ID system.[3] It's the largest such system in the world—with over a billion users—and is used to access services like banking and healthcare.

South Korea is trialing a facial recognition system[4] in an attempt to improve security at government buildings. Apple has apparently purchased a facial recognition startup, leading to speculation that they may use the technology for authentication in the future.

As biometric authentication becomes more prevalent in everyday life, it begs the question — is it really making us more secure?

THE PROBLEM WITH PASSWORDS

People hate passwords and are notoriously lax with password-based security. Many users see passwords as a barrier to the information they need to get things done, not a failsafe security measure. **Biometrics address many of the weaknesses of passwords:**

- **Does Not Need To Be Generated**
- **Does Not Have To Be Remembered**
- **Cannot Be Lost (Like Security Devices)**
- **Cannot Be "Dumbed Down"— I.e. There's No Biometric Equivalent Of "Password123"**

So, biometric technology addresses the aspects of human behavior that tends to undermine security. Given this, why is the Electronic Freedom Foundation (EFF) so keen on legislation that limits the use of biometric data?[5]

See next page to continue.

[1] *https://techcrunch.com/2013/09/10/apples-touch-id-a-500ppi-fingerprint-sensor-built-into-iphone-5s-home-button/*
[2] *https://www.cnet.com/news/apple-face-id-truedepth-how-it-works/*
[3] *https://oneworldidentity.com/2017/02/02/indias-aadhaar-id-program-improve-biometric-security-new-bionetra-iris-partnership/*
[4] *http://www.biometricupdate.com/201702/facial-recognition-trial-completed-at-south-korea-government-complex*
[5] *https://www.eff.org/deeplinks/2017/02/protect-biometric-privacy-montana*

BIOMETRIC AUTHENTICATION
IS THE FUTURE OF SECURITY — AND IT'S HERE NOW

THE POTENTIAL HARM IN BIOMETRIC SECURITY

One fundamental problem with biometric security is that once compromised, it's incredibility difficult (or impossible) to revoke it. Imagine you had a password — possibly a very strong one — assigned at birth and you had to use it until you died. You could never change it. That's essentially how biometric security works.

In fact, it may be worse than that as it's difficult to protect your biometric data. **You leak it constantly—every time your fingerprint-smeared glasses are cleared up at the bar, for example. Additionally:**

A hacker was able to recreate the fingerprints of Germany's defense minister from high-resolution photographs![6]	**The same hacker had previously demonstrated how to fool Apple's iPhone Touch ID using cheap, readily-available materials.**	**Face recognition technology has been fooled using photos from Facebook.[7]**

These examples just represent physical hacks. As this information is being used in a computer, at some point it will need to be digitalized. If captured in this form, it could be injected back into a system at the appropriate point bypassing the need to fool scanners.

We've seen how people's lives can be turned upside down by mistaken identity — such as those who are erroneously flagged as being on no-fly lists.[8] As biometric information starts being used more and more to control access to things like government services, financial services, and travel, **the consequences of having your biometric information compromised can become extremely dire.**

THE CONSEQUENCES OF A BIOMETRIC DATA BREACH

Think about what happens if your biometric data is compromised. Even if you could convince those in charge of the system that a mistake had been made, how would it be rectified? Swap out your old irises for a new pair? Choose another set of fingerprints? A new face? Unlike a password, biometric information isn't easily changed.

Maybe the interest in biometric security will die down once we have chips implanted[9] — like pets do. At least we could replace those. Ouch! — but at least it'll get you your life back.

Biometric technology is a quick fix, but, unless we are incredibly careful about how we use it, we are potentially baking in serious problems downstream.

LEARN MORE AT: LEARNINGTREE.COM/CYBER

[6] *https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands*
[7] *https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/*
[8] *http://edition.cnn.com/2015/12/07/politics/no-fly-mistakes-cat-stevens-ted-kennedy-john-lewis/*
[9] *http://www.news.com.au/technology/gadgets/wearables/australians-embracing-superhuman-microchip-technology/news-story/536a08003cb07cba23336f83278a5003*