Understanding the user experience of Biometrics

Simon Rubens, *new experience*, August 2017

Face the future

Biometrics are very much in the news at the moment. British banks like HSBC make use of voice recognition for phone banking. Touch ID has already become standard on many phones, and Apple is expected to replace it with facial recognition in the near future.

In theory biometrics offer the holy grail of 'frictionless' transaction *with* enhanced security. It is well known that the 'friction' around password recall and entry lowers security as a result of people creating easy-to-guess passwords or writing them down on paper. On the other hand biometrics require no memorising or recall, and are unique to an individual.

In China some banks allow customers to withdraw cash from ATMs by scanning their faces, but the technology is also being adapted for more Orwellian uses such as the country's 'social credit' rating system that is designed to enforce good behaviour through monitoring of citizens.

While the future is clearly biometric our research highlights some consumer concerns that companies would be wise to consider as they bring in new means of authentication. People's experience of biometrics is often very positive once they've tried it but to smooth adoption the following fears will need to be addressed by education and reassurance:

Reliability

Participants in our study had experience of biometric failure such as Touch ID when their finger was sweaty, or facial recognition when coming through the e-passport channel. They worried that facial recognition might be affected by sunlight, ageing or facial hair, and voice recognition by background noise. Furthermore with voice recognition there was a tendency to conflate it with voice activation technologies such as Amazon Echo where the user experience is not always perfect. While these fears may be unfounded they can lead to a deep-seated concern about being locked out of a service with nowhere to turn. While you may be able to change a password, if biometrics fail you can feel like there is nothing you can do to regain access to a service.

Risk of compromise

Several of our study participants worried that the security of biometrics could be compromised. Participants were concerned that a photo of them could be used to fool facial recognition and that their fingerprint could be lifted from a glass. Some had read about the recent BBC Click success in fooling HSBC's voice recognition system. Such fears are quite understandable when you think that once compromised, a biometric identity cannot be reclaimed, unlike a password that can always be changed.

Privacy

Many of our participants were concerned about what would happen to their biometric data; where it would be stored, who it might be shared with and whether it would be retained after they stopped using a service. It feels like Big Brother surveillance and a small number indicated they would reject biometrics outright on the basis of privacy.

Discrimination

One participant – who was from an ethnic background – had particular concerns around the potential of facial recognition for discrimination based on skin colour. Their concern stemmed from difficulties they had had using facial recognition at the airport which they had heard was designed to work primarily with white skin. Their fear was mainly about feeling 'less than'.

Companies who take these concerns into account will be well placed to help their customers gain from a frictionless future.

About *new experience*

new experience is a London-based user experience research consultancy specialising in ethnographic research, participatory design, service trials, ergonomic evaluation and usability testing.

To find out more:

visit www.new-experience.com or email
simon.rubens@new-experience.com