HEATHER SHAW, CHARLOTTE SIBBONS, STACEY CONCHIE & PAUL TAYLOR

ARE EMERGING DIGITAL BEHAVIOURAL BIOMETRICS ABLE TO IDENTIFY US?

This article considers the current state of play in emerging behavioural biometrics to see how far we have come, and what challenges lie ahead.

The proliferation of digital traces offers new ways to identify people from their actions and interactions with the world. Our pattern of website access can betray our political leaning; keystroke behaviour may reveal our identity; our smartphone use is unique and consistent enough to act as a discriminating fingerprint. These 'digital biometrics' are increasingly used across different settings from authentication of a person in the finance sector through to enhanced security in IoT devices, healthcare and defence.

The relative ease by which behavioural biometrics can be collected from the user as they interact with technology, the assurance they afford against human failure (such as forgotten passwords), their relative robustness to imitation by an imposter, and the fact that they don't require specialised hardware for data processing have increased their appeal over traditional biometrics. According to some researchers, behavioural biometrics are likely to become the dominant means by which a person's identity can be determined and authenticated.

Although digital behavioural biometrics hold great promise, they are far from ready to be deployed at scale. They carry ethical risk, are subject to bias, and have yet to address the challenge that human behaviour is not consistent across all contexts. We set out to understand the current state of play in emerging behavioural biometrics to see how far we have come, and what challenges lie ahead.

AN UMBRELLA REVIEW

We carried out a systematic analysis of review papers on emerging behavioural biometrics following PRISMA guidelines. To be included in our analysis, a review paper needed to focus on emerging digital behavioural biometrics, make inference about personal identity, review empirical work, and be written in English. We excluded reviews that focused exclusively on physiological markers, that were not peer-reviewed, and which focused on biometrics in non-human animals. Applying these criteria, we identified 41 review papers to include in our analysis.

For a digital footprint to act as a digital behavioural biometric it must be distinct (i.e., allow for unique expression), have *permanence* (i.e., behavioural consistency), be easily *collectable*, and be *prominent* across a population of interest. Our analysis showed that digital behaviours can manifest physically (e.g., mouse movement, typing pressure), but also socially (e.g., social media networking, patterns of game play). Emerging behavioural biometrics that have received the most attention are keystroke dynamics, handwriting, speech, walking gait, and touch gestures. Based on the reviews we analysed, these biometrics can achieve up to 90% accuracy when verifying a user, though their accuracy is weaker when they are used to identify a person in a crowd. The lack of standardisation across biometric systems makes it impossible to compare different systems.

A number of factors contribute to the error rate of biometrics; the prime among these is the fact that human behaviour is situation-dependent. As such, a person may act consistently when observed over time in Situation A, but this may bear little relation to how they act in Situation B. Defined broadly, 'situation' may cover changes in environment (e.g., a controlled lab vs. a natural environment), changes in state (e.g., mood, fatigue, intoxication, mental health, injury) and changes in task novelty (e.g., a well-practiced vs. novel task). There are several examples of how behaviours such as keystroke dynamics and gait are respectively altered by a person's mood or something as simple as the terrain on which a person walks. There was little evidence in our review that biometric systems are currently able to accommodate these situational-shifts in behaviour.

Digital behavioural biometric systems raise questions around ethics. Ethics comes to the fore when we consider a person's privacy. Hardware exists that allows a person's behaviour (e.g., keystroke dynamics) to be measured without their awareness. While the covert collecting of information may be defendable in some contexts, for example, surveillance of somebody under a warrant suspected to be in the process of carrying out a criminal act, it is harder to justify when applied to the general public, especially when such behavioural data may be used for discrimination, advertising, or unauthorised surveillance purposes. There are also unanswered questions around GDPR compliance and what behavioural data relate to sensitive categories and what may potentially lead to sensitive information disclosure when combined with other data.

Our umbrella review offered many areas for future work, alongside a checklist of how to standardise research to increase the efficacy and potential of digital behavioural biometrics. Multimodal systems that combine different types of digital footprint data can increase the accuracy of digital behavioural biometrics. This needs to be explored on large samples, in out-of-the-lab contexts, and across different hardware (e.g., different phone brands). Behavioural systems are continuous and temporal by nature and need updating over time to control for this behavioural drift. They need to adapt to the deviations in behaviour which can occur because of situation when authenticating (e.g., someone's mood or level of intoxication).

It is worth the time and effort exploring the nuances of human behaviour and the user acceptance, trust, and privacy perceptions of digital behavioural biometrics, as they hold much promise. If solutions are found to these challenges, then identity can be inferred continuously with little user effort, heightening the security of many personal and organisational systems.

Heather Shaw is a lecturer in psychology at Lancaster University. Charlotte Sibbons is a Behavioural Scientist at FCDO. Stacey Conchie is a professor of psychology at Lancaster University and Director of CREST. Paul Taylor is a professor of psychology at Lancaster University and the University of Twente.

© DedMityay | stock.adobe.com