



Aug 12, 2021 15:28 BST

EXPERT COMMENT: Paying with a palm print? We're victims of our own psychology in making privacy decisions

With reports that Amazon is offering customers credit in exchange for using their handprints to pay at Amazon's stores, what are the impacts of using our biometric data for everyday purchases? [Professor Pam Briggs](#), Research Chair in Applied Psychology at Northumbria University, writes for [The Conversation](#), outlining the complex issues involved in giving up your biometric data to another party and suggests we should be wary of being offered incentives to do so.

The online retail giant Amazon has moved from our screens to our streets, with the introduction of Amazon grocery and book stores. With this expansion came the introduction of Amazon One – a service that lets customers use their handprint to pay, rather than tapping or swiping a card. According to recent reports, Amazon is now [offering promotional credit](#) to users who enroll.

In the UK we're quickly becoming used to biometric-based identification. Many of us use a thumbprint or facial recognition to access our smartphones, authorise payments or cross international borders.

Using a biometric (part of your body) rather than a credit card (something you own) to make a purchase might offer a lot more convenience for what feels like very little cost. But there are several complex issues involved in giving up your biometric data to another party, which is why we should be wary of companies such as Amazon incentivising us to use biometrics for everyday transactions.

An Amazon store in Seattle, USA

Amazon's handprint incentive adds to an ongoing academic and policy debate about when and where to use biometrics to "authenticate" yourself to a system (to prove that you are who you say you are).

On the benefits side, you're never without your biometric identifier -- your face, hand or finger travel with you. Biometrics are pretty hard to steal (modern fingerprint systems typically include a ["liveness" test](#) so that no attacker would be tempted to chop a finger off or make latex copies). They're also easy to use -- gone are the problems of remembering multiple passwords to access different systems and services.

What about the costs? You don't have many hands -- and you can't get a new one -- so one biometric will have to serve as an entry point to multiple systems. That becomes a real problem if a biometric is hacked.

Biometrics can also be discriminatory. Many facial recognition systems fail ethnic minorities (because the systems have been trained with [predominantly](#)

[white faces](#). Fingerprint systems may [fail older adults](#), who have thinner skin and less marked whorls, and all systems would fail those with certain disabilities – arthritis, for example, could make it difficult to [yield a palm print](#).

Who should we trust?

A key issue for biometrics “identity providers” is that they can be trusted. This means that they will keep the data secure and will be “proportional” in their use of biometrics as a means of identification. In other words, they will use biometrics when it is necessary – say, for security purposes – but not simply because it seems convenient.

The UK government is currently [consulting on a new](#) digital identity and attributes trust framework where firms can be certified to offer biometric and other forms of identity management services.

As the number of daily digital transactions we make grows, so does the need for simple, seamless authentication, so it is not surprising that Amazon might want to become a major player in this space. Offering to pay for you to use a biometric sign-in is a quick means of getting you to choose Amazon as your trusted identity provider ... but are you sure you want to do that?

Privacy paradox

Unfortunately we’re victims of our own psychology in this process. We will often say we value our privacy and want to protect our data, but then, with the promise of a quick reward, we will simply click on that link, accept those cookies, login via Facebook, offer up that fingerprint and buy into that shiny new thing.

Researchers have a name for this: the [privacy paradox](#). In survey after survey, people will argue that they care deeply about privacy, data protection and digital security, but these attitudes are not supported in their behaviour. Several explanations exist for this, with some researchers arguing that people employ a privacy calculus to assess the costs and benefits of disclosing particular information.

The problem, as always, is that certain types of cognitive or social bias begin

to creep into this calculus. We know, for example, that people will underestimate the risks associated with things they like and overestimate the risks associated with things they dislike (something known as the [“affect heuristic”](#)).

As a consequence, people tend to share more personal data than they should, and the amount of such data in circulation grows exponentially. The same is true for biometrics. People will say that only trusted organisations should hold biometric data, but then go on to give their biometrics up with a small incentive. In [my own research](#), I’ve linked this behavioural paradox to the fact that security and privacy are things we need to do, but they don’t give us any joy, so our motivation to act is low.

Any warnings about the longer-term risks of taking the Amazon shilling might be futile, but I leave you with this: your biometrics don’t just confirm your identity, they are more revealing than that. They say something very clearly about ethnicity and age, but may also unknowingly reveal information about disability or even mood (in the example of, say, a voice biometric).

Biometric analysis can be done without permission (state regulations permitting) and, in some cases, [at scale](#). China leads the way in the use of face recognition to identify individuals in a crowd, [even when wearing masks](#). Exchanging a palm print for the equivalent of a free book may seem like a vastly different thing, but it is the thin end of the biometric wedge.

Northumbria is a research-rich, business-focused, professional university with a global reputation for academic excellence. Find out more about us at www.northumbria.ac.uk --- Please contact our Media and Communications team at media.communications@northumbria.ac.uk with any media enquiries or interview requests ---

Contacts



Rik Kendall

Press Contact

PR and Media Manager

Business and Law / Arts, Design & Social Sciences

rik.kendall@northumbria.ac.uk

07923 382339



Andrea Slowey

Press Contact

PR and Media Manager

Engineering and Environment / Health and Life Sciences

andrea.slowey@northumbria.ac.uk

07708 509436



Rachael Barwick

Press Contact

PR and Media Manager

rachael.barwick@northumbria.ac.uk

07377422415



James Fox

Press Contact

Student Communications Manager

james2.fox@northumbria.ac.uk



Kelly Elliott

Press Contact

PR and Media Officer

kelly2.elliott@northumbria.ac.uk



Gemma Brown

Press Contact

PR and Media Officer

gemma6.brown@northumbria.ac.uk