Investigating What You Share: Privacy Perceptions of Behavioural Biometrics

Sally Earl[0000−0002−3283−0274], James Campbell[0000−0003−0898−1280], and Oliver Buckley[0000−0003−1502−5721]

School of Computing Science, University of East Anglia, Norwich, NR4 7TJ, UK
{s.earl, j.campbell1, o.buckley}@uea.ac.uk
http://www.uea.ac.uk

Abstract. This study examines people's perceptions of biometrics, in the context of the inherent privacy concerns surrounding behavioural biometrics as an alternative to conventional password systems. We present the knowledge and opinions of behavioural biometrics collected in this study. The main theme which is present throughout the research is that users have privacy concerns around behavioural biometrics, but that these concerns do not necessarily translate into privacy-conscious actions.

Keywords: Behavioural Biometrics · Privacy · Perceptions

1 Introduction

Biometrics are becoming increasingly common as an alternative to conventional password and passcode systems, whether this be the use of a fingerprint to unlock a laptop or their face to open a mobile phone.

One of the reasons for the shift towards biometrics is the underlying issues associated with creating good passwords. It has long been stated that it is difficult for users to create passwords which are both memorable and secure [8], and many of the measures which websites and companies use to try to increase security can make things worse, for example [1], [12]. Additionally, users tend to be reluctant to use security measures which are an inconvenience [6]. Biometrics have the advantage of removing any cognitive load from the user - as they do not need to remember any information or have a specific item on their person.

Behavioural biometrics create a unique profile of a person through looking at how they act [17]. The key difference between physical and behavioural biometrics is that physical biometrics have a static measurement, whereas behavioural biometrics are dynamic.

While the public are likely to be familiar with physical biometrics due to their ubiquity in day-to-day life, behavioural biometrics are less likely to be at the forefront of their consciousness. Previous studies (such as in Furnell and Evangelatos [7] and Buckley and Nurse [4]) have looked at perceptions of biometrics both physical and behavioural, but none have focused on exclusively behavioural biometrics.

One large difference between physical and behavioural biometrics is that behavioural biometrics can frequently be gathered without the user's knowledge, unlike physical biometrics which usually require an action of the user. As a result of this, behavioural biometrics have the potential to be more privacy-infringing than physical biometrics.

In recent years, online privacy has become at the forefront of public consciousness, with the UK ICO [10] noting an increase of 70% of contacts from the general public surrounding issues of data privacy since the implementation of the Data Protection Act 2018. As a result, any technological development which has the potential to interfere with privacy may cause a lack of trust from users.

In this study we aimed to not only gather more information about people's knowledge and trust of behavioural biometrics, but also how this might link to their perceptions of privacy.

2 Literature Review

Many different behavioural biometrics have been studied, with 28 having been identified by Yampolskiy and Govindaraju [17]. Of these biometrics, the most commonly studied are Gait (the way a person walks), Keystroke Dynamics (the way a person types), Mouse Dynamics (the way a person uses their mouse), Signature (the dynamic movement when a person signs their name), and Voice (the way a person speaks).

Several studies have been completed regarding perceptions of biometrics. In 2007 Furnell and Evangelatos [7] found 45% of participants felt passwords were inadequate for large-scale systems, and most had positive opinions towards biometrics. The study found that the behavioural biometrics studied were ranked as being less reliable than the physical biometrics, with keystroke dynamics in particular being ranked as not at all reliable. Keystroke dynamics were also the biometric the participants were least aware of. This trend can also be seen in a study by Krupp et al. [13], which looked at attitudes to biometrics within Germany, and found that whilst voice biometrics and facial recognition were known, they were not well-accepted. This trend is again seen in a study by Buckley and Nurse [4], with the behavioural biometrics being ranked as least secure (again, with the caveat that these biometrics were also those which were less familiar to the participants).

Studies throughout the last decade have found that people have seen biometrics as a secure authentication method [2], [5], and [13]. Despite these positive opinions of biometrics; however, studies still show people prefer using passwords to other methods including biometrics and other password alternatives (such as graphical passwords) [19].

Some previous studies have discussed the potential privacy issues and other ethical concerns of biometrics. Norval and Prasopoulou [15] found that there was a wide variety of attitudes towards biometrics, with some seeing biometrics as intrusive, whilst others saw them as more neutral. A similar dichotomy has been found in other studies, with some users preferring passwords due to their

lack of privacy concerns, despite security issues, and others preferring biometrics due to their heightened security, regardless of risk [18]. Zimmerman and Gerber [19] found that signature elicited the most privacy concerns of the authentication methods used. The authors also found that privacy concerns and preferred authentication method did not directly relate to one another, with fingerprint being the second most-liked authentication method, but also having high security concerns. None of these studies considered how a participant's existing opinions on privacy might factor into their feelings on biometrics generally.

When discussing biometrics, it is also important to note that the knowledge (or lack thereof) that a participant has may effect their understanding of the potential benefits and issues. Mwapasa et al. [14] highlights the knowledge-gap between potential users of biometric systems and those who implement and write policies concerning them, particularly in countries with high illiteracy levels. As a result of this, it is important to note that users do not necessarily have all the information available to make informed choices.

Based on the literature above, this research looks to understand user's perceptions of biometrics and contrast this with their knowledge on the subject. Furthermore, we look to incorporate online social media presence data to understand if the perceptions of biometrics, match their own online privacy settings.

3 Method

In order to facilitate data collection, we designed a survey for this study, comprised of a mixture of closed and open-ended questions. Prior to study launch, we obtained ethical approval from our University.

Participant recruitment took place primarily through the Prolific platform, which allowed us to obtain a diverse pool of respondents. This recruitment was supplemented with more ad-hoc recruitment from the general public, primarily through social media, and snowball sampling [9].

Our survey began with collecting a range of demographic data from participants including gender, age, and highest level of education. Additionally, we collected data on what social networks participants used, and whether their accounts were public or private.

We then asked a number of questions which focused on participant's opinions on privacy; to allow us to use this as a baseline for their opinions on behavioural biometrics.

The study then followed closely that of Buckley and Nurse [4], asking participants to define what they felt was meant by the term 'behavioural biometrics'. We then presented them with a list of behavioural biometrics (Gait, Keystroke Dynamics, Mouse Dynamics, Voice, and Signature/Handwriting) to see which they had previously heard of. We chose these specific behavioural biometrics as they were the biometrics identified in [17] which were most likely to be usable in a variety of situations. Similarly to the previous study, we then asked participants to rank the domains of Airport, Banking, Home, Mobile Devices, and

Online Shopping in terms of need for security, then rank which behavioural biometrics (if any) they would trust to secure each domain. This was to ascertain how secure they felt each biometric was (as if they trusted a biometric in the domain they felt was the most needing security, they likely trusted the biometric). Our study concluded with asking participants whether they felt behavioural biometrics infringed on their privacy, and asking them to recall how many days we planned to retain their data.

The data analysis consisted of a variety of quantitative and qualitative techniques. For the closed questions we used statistical methods for analysis, including looking for correlation using the Pearson Chi-Squared test. For the open-ended questions, we first used Thematic Analysis [3], which allowed us to manually explore all the data to find patterns and themes.

4 Results

Our survey received a total of 238 responses. Of these, 104 were female and 134 were male. A significant minority of our participants (40%) were aged 19-25, with 72% of our participants being aged 30 or below. As a result of this, it is important to note there is a bias towards younger people within our data, all of whom will have grown up with access to the internet and technology.

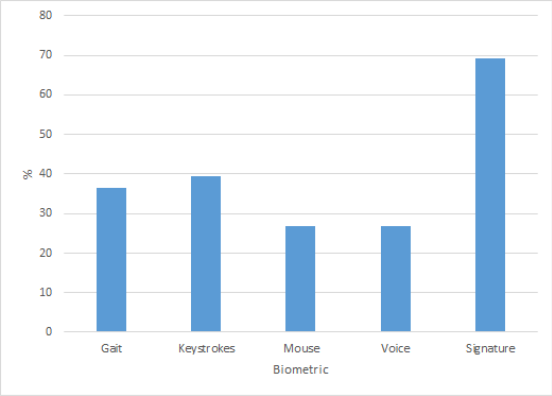

Fig. 1. Percentage of participants who had heard of each biometric

Before participants were asked their opinions on behavioural biometrics, we first asked them what they thought was meant by the term, and conducted thematic analysis on the responses. The most commonly occurring theme was that the participants did not know, with 20% responding such. Other common themes included the idea of monitoring a user's actions on a computer or online, with many participants explicitly mentioning monitoring social media behaviour. Other themes in the data included monitoring of a person's actions or patterns,

and the use of identification or determination of personal features and characteristics. A not insubstantial number of participants guessed or knew behavioural biometrics had something to do with monitoring an action or behaviour of some sort.

After participants had given their definition, they were then given an accurate definition of behavioural biometrics. When asked if they had ever heard of any of the behavioural biometrics considered in our study, only signature had been heard of by a majority of our participants (69%) (Figure 1). This is likely to be in part due to a misunderstanding conflating signing for something and the biometric, as considered in [4].

Our results are similar to those found in [4], with the exception of voice, which only 26% of our participants had heard of. This seems unlikely, as voice recognition has been used by banks for several years, including all of the UK's Big 4 banks (Barclays, HSBC, Lloyds Group, and NatWest Group). Additionally this result is significantly below that of Buckley and Nurse [4], who found over 60% of their participants had heard of voice biometrics. It is unclear what factor has caused this discrepancy.

	Airport	Banking	Home	Mobile Devices	Online Shopping
1	80	104	40	12	2
2	52	103	39	18	26
3	36	27	64	61	50
4	33	4	34	95	72
5	37	0	61	52	88
Average	2.5588	1.7101	3.1555	3.6597	3.9160

Table 1. Breakdown of rankings of security in each domain, with the lower the value indicating the higher need for security.

We also asked participants to rank specific situations in terms of their need for security (results shown in Table 1). As expected, the areas ranked as most needing security were banking and the airport. After this, we asked our participants which biometrics they would trust in each domain, to give us an idea of which biometrics they trust the most. Voice biometrics was most consistently ranked the most trusted biometric.

The feasibility of each individual biometric to provide security in each situation seems to have been taken into account somewhat. This can be seen when looking at the ranking for gait analysis, which despite coming last in 3 of the domains, it came second in the other two (home and the airport). This makes sense that for online shopping and mobile devices, gait would be unlikely to be a feasible authentication method.

When asked about whether behavioural biometrics infringed on their privacy, just over 50% of our participants reported being unsure (Figure 2). Of the remainder, more felt behavioural biometrics were privacy infringing than felt they

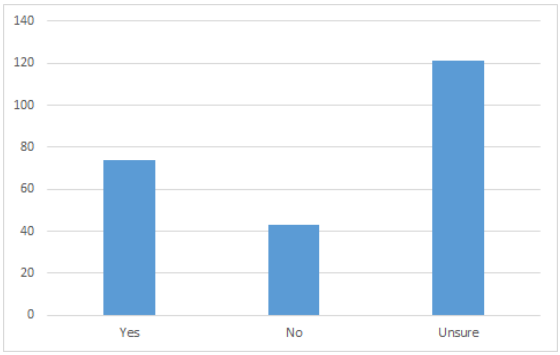

Fig. 2. Participants' response to the question "Do you think behavioural biometrics infringe on your privacy"

were not. This is unsurprising, given the majority of the participants reported being concerned or very concerned about their privacy online.

Our participants' lack of certainty in the potential implications of behavioural biometrics is highlighted by 25 of our participants responding they felt behavioural biometrics gathered lots of personal data, whilst 25 other participants responded that they did not. These are in direct opposition to each other, showing either a lack of understanding by our participants, or alternatively a real disagreement about whether behavioural biometric data actually constitutes further personal data.

It is important to note here that the EU agrees with the latter of these 2 positions, with GDPR counting behavioural biometrics as 'special category data,' meaning it must be processed within specific settings. One of these is 'explicit consent'. The guidance from the ICO states that explicit consent in terms of biometric authentication must include the ability to opt-out [11]. This shows that the EU's opinions on the privacy and consent concerns surrounding behavioural biometrics are similar to many members of the public.

When asked if they thought behavioural biometrics infringed on privacy, our participants highlighted their desire to have knowledge of the information being gathered, and the ability to consent to it (with this idea being present 28 times). This again helps indicate that the GDPR requirements for explicit consent reflect the opinions of the public. Whilst this view has been explicitly expressed by our participants, their actions did not necessarily reflect it. 72.27% of the participants incorrectly selected a specific number of days which were specified in the Terms and Conditions at the beginning of the survey. This is not an uncommon finding, with previous studies showing that 79.7% of their participants agreed to the terms and conditions without reading them [16]. This highlights an ethical dilemma, that whilst users wish to be notified of behavioural biometric collection, ensuring they receive this information is difficult. This means that users may lose trust in sites they use if they later discover behavioural biometric collection.

5 Conclusion

The main theme which is present throughout the research is that users have concerns around behavioural biometrics regarding privacy. Specifically, these concerns included issues surrounding the intrusion into personal data, and the knowledge that this data is being collected. The actions of our users; however, contradicted their opinions, as can be seen from the number of users that responded incorrectly when asked how long their data would be held for, despite this having been displayed to them at the beginning of the study.

We can therefore surmise that whilst privacy is important to users, their actions do not always line-up with their beliefs, particularly when convenience is involved.

Future work should focus on improving the privacy implications of collecting behavioural biometric data, without compromising on the usability of a system. Further discussion is needed to understand perceptions of biometrics, and how their reputation and use as a form of security can be improved.

References

1. Adams, A., Sasse, M.A.: Users are not the enemy. Communications of the ACM **42**(12), 40–46 (1999)
2. Bhagavatula, R., Ur, B., Iacovino, K., Kywe, S.M., Cranor, L.F., Savvides, M.: Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption (2015)
3. Braun, V., Clarke, V.: Thematic analysis. (2012)
4. Buckley, O., Nurse, J.R.: The language of biometrics: Analysing public perceptions. Journal of Information Security and Applications **47**, 112–119 (2019)
5. Cornacchia, M., Papa, F., Sapio, B.: User acceptance of voice biometrics in managing the physical access to a secure area of an international airport. Technology Analysis & Strategic Management pp. 1–15 (2020)
6. Fagan, M., Khan, M.M.H.: Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In: Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016). pp. 59–75 (2016)
7. Furnell, S., Evangelatos, K.: Public awareness and perceptions of biometrics. Computer Fraud & Security **2007**(1), 8–13 (2007)
8. Gehringer, E.F.: Choosing passwords: security and human factors. In: IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No. 02CH37293). pp. 369–373. IEEE (2002)
9. Goodman, L.A.: Snowball sampling. Ann. Math. Statist. **32**(1), 148–170 (03 1961). https://doi.org/10.1214/aoms/1177705148, https://doi.org/10.1214/aoms/1177705148
10. Information Commissioner's Office: Information commissioner's annual report and financial statements 2019-20. Tech. rep., Information Commissioner's Office (2020)
11. Information Commissioner's Office: Information commissioner's office. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/conditions1 (2020)

12. Inglesant, P.G., Sasse, M.A.: The true cost of unusable password policies: password use in the wild. In: Proceedings of the sigchi conference on human factors in computing systems. pp. 383–392 (2010)
13. Krupp, A., Rathgeb, C., Busch, C.: Social acceptance of biometric technologies in germany: A survey. In: 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG). pp. 1–5. IEEE (2013)
14. Mwapasa, M., Gooding, K., Kumwenda, M., Nliwasa, M., Kaswaswa, K., Sambakunsi, R., Parker, M., Bull, S., Desmond, N.: "are we getting the biometric bioethics right?"–the use of biometrics within the healthcare system in malawi. Global Bioethics **31**(1), 67–80 (2020)
15. Norval, A., Prasopoulou, E.: Seeing like a citizen: Exploring public views of biometrics. Political Studies **67**(2), 367–387 (2019)
16. Steinfeld, N.: "i agree to the terms and conditions":(how) do users read privacy policies online? an eye-tracking experiment. Computers in human behavior **55**, 992–1000 (2016)
17. Yampolskiy, R.V., Govindaraju, V.: Taxonomy of behavioural biometrics. In: Behavioral Biometrics for Human Identification: Intelligent Applications, pp. 1–43. IGI Global (2010)
18. Zimmermann, V., Gerber, N.: "if it wasn't secure, they would not use it in the movies"–security perceptions and user acceptance of authentication technologies. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. pp. 265–283. Springer (2017)
19. Zimmermann, V., Gerber, N.: The password is dead, long live the password–a laboratory study on user perceptions of authentication schemes. International Journal of Human-Computer Studies **133**, 26–44 (2020)