"I don't like putting my face on the Internet!": An acceptance study of face biometrics as a CAPTCHA replacement

Kat Krol, Simon Parkin, and M. Angela Sasse
University College London
Department of Computer Science
{kat.krol.10, s.parkin, a.sasse}@ucl.ac.uk

Abstract

Biometric technologies have the potential to reduce the effort involved in securing personal activities online, such as purchasing goods and services. Verifying that a user session on a website is attributable to a real human is one candidate application, especially as the existing CAPTCHA technology is burdensome and can frustrate users. Here we examine the viability of biometrics as part of the consumer experience in this space. We invited 87 participants to take part in a lab study, using a realistic ticket-buying website with a range of human verification mechanisms including a face biometric technology. User perceptions and acceptance of the various security technologies were explored through interviews and a range of questionnaires within the study. The results show that some users wanted reassurance that their personal image will be protected or discarded after verifying, whereas others felt that if they saw enough people using face biometrics they would feel assured that it was trustworthy. Face biometrics were seen by some participants to be more suitable for high-security contexts, and by others as providing extra personal data that had unacceptable privacy implications.

1. Introduction

A CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart") is a challenge-response test where the user is asked to enter a sequence of characters identified from a distorted image. CAPTCHAs are intended to restrict use of online services to humans, preventing automated programs (robots) from accessing – and exploiting – those services. CAPTCHAs however demand a high amount of effort to complete and Pogue [12] calls for alternatives to be found.

We conducted a study that looked at the user perception and acceptance of three mechanisms: (i) traditional text-based CAPTCHAs, specifically Google's reCAPTCHA[1], (ii) an alternative called Play Thru[2] which requires the user to drag and drop elements on the screen and (iii) NoBot[3] which is a face biometric technology. While another publication [11] discusses all three mechanisms tested in the study; in this paper, we focus on just the biometric one, exploring in depth user perceptions and challenges it might face to gain user acceptance. NoBot is a face-recognition technology that uses capabilities of the host computer device (*i.e.*, a camera) to collect a sample sequence of face images which are then processed centrally by the technology provider. This processing determines if a live human is using the device, as opposed to a – potentially automated – replay of images that are not current (and as such not "live").

A realistic ticket-buying website was created for the purposes of the study, where participants engaged with the human verification process as part of their purchasing activity. For NoBot in particular, we assessed the user experience of repeated use across either laptop or tablet. Examining use on a tablet is important as interactions and purchases become increasingly mobile, posing significant usability challenges such as entry of characters on a virtual keyboard [13, 7].

We conducted a between-subjects study with 87 participants across three conditions: 29 participants used reCAPTCHA, PlayThru and NoBot once, 27 used NoBot three times on a laptop, and 31 used NoBot three times on a tablet. Our study informs the understanding of deploying biometrics as part of consumer services, and how prepared people are to use biometrics in place of more familiar technologies. The NoBot face biometric is studied across different devices, but also compared to existing and competing verification technologies. A realistic ticket-buying scenario promotes discussion of the technologies as part of typical

[1] https://developers.google.com/recaptcha/old/intro

[2] http://areyouahuman.com/demo-playthru

[3] The developer did not commercialise this product and wishes not to be named.

online activities, as opposed to being assessed in isolation.

Face biometrics, as a replacement technology, are assessed for a variety of verification and authentication situations: participants not only used the technologies as part of a ticket-buying website, but were also encouraged to discuss their impressions of each technology (where comments were analysed), in addition to completing specialised questionnaires: this included an instantiated Technology Acceptance Model (TAM) survey, and a questionnaire identifying different service contexts that the participant perceived were appropriate applications for the verification solution(s) they had used (including NoBot).

The remainder of the paper is organised as follows. The next section summarises the findings of related studies of face biometrics, taking a critical look at the methodologies used. The Methodology of the present study is then described in Section 3, followed by a presentation of results in Section 4 (including analysis of dialogue, and the TAM and context questionnaires). Findings are then discussed in Section 5 before concluding remarks and suggestions for future work in the area in Section 6.

2. Related work

In this section, we describe related work evaluating the user experience of biometric solutions.

Bhagavatula *et al.* [1] explored usability and participant experience of both face- and fingerprint-based verification for mobile devices, through a lab study and structured survey. Both mechanisms were compared side-by-side with more traditional PINs within subjects. The study scenarios were designed with physical settings in mind, such as using the mechanisms while in motion or in a dark room, aiming to assess user and technology performance. The results show that participants preferred unlocking devices with a fingerprint more than a PIN. Participants had more problems with face unlock and many abandoned using it.

Heckle *et al.* [9] asked participants to role-play purchases on an online bookstore with role-played use of fingerprint technologies. From the results the authors suggested that application contexts with more apparent user benefits were seen as more usable and acceptable

Trewin *et al.* [17] explore user demands – in terms of time, effort, error and task disruption – of voice, face and gesture, in a within-subjects study. Biometrics were recorded as being faster than using passwords, although none of the mechanisms were considered usable – this is important, as although a mechanism can be regarded as better than others, its "absolute" measure of usability may be poor. The authors include a primary task which is a memory exercise.

Khan *et al.* [10] explore the usability of implicit authentication compared to explicit authentication solutions, through a study in the lab and in the field. Participants completed simulated tasks, where a field study engaged real tasks and implications (such as annoyance). Implicit authentication was simulated on participants' own devices (although they were unaware that the authentication application was not operational), including simulated false rejects. The authors collected both quantitative and qualitative data, through task timing data and coded semi-structured interviews respectively. Security perceptions were captured (including responses to fabricated "interruptions" produced by the authentication technology), including implicit authentication as a replacement of existing approaches and willingness to adopt the technology.

In the research so far, primary tasks have been limited to assess user performance and did not entirely put participants into realistic every-day scenario that would make them behave naturally. In the study presented here, we aim to make the experience more realistic to ensure our findings are generalisable to the real world.

Where Heckle *et al.* [9] role-played the occurrence of errors, we assess a real (face) verification technology, including the complications of preparing for verification and responses to any problems such as false negatives, which contribute to the perceived usability of the mechanism. Here we have participants use a genuine third-party face biometric solution in a lab-based setting. Participants completed tasks typical of a mobile device, such as reading information from a website, which were interrupted by the mechanism – here an online ticket purchase site was used which weaves the biometric directly into the task itself, interrupting the primary task. While Heckle *et al.* [9] used structured interview questions prompting participants to consider their current and potential online habits, here an online ticket purchasing website and follow-up questions serve a similar purpose.

3. Methodology

The study was advertised as looking at the usability of online shopping check-outs. To limit introduction of biases, CAPTCHAs, biometrics or security were not referred to specifically at any time in the recruitment process or the information sheet. The study sessions were conducted in a usability laboratory with one participant at a time. In the study, participants were tasked with purchasing three tickets on a mock-up website and verification using a CAPTCHA was part of the check-out. Figure 1 shows the verification page of the website, here with PlayThru. There were 87 participants in a between-subjects study with three conditions: 29 participants used reCAPTCHA, PlayThru and NoBot once (condition abbreviated as $\mathrm{M3}_{all}$), 27 used NoBot three times on a laptop (NB_{Lap}), and 31 used NoBot three times on a tablet (NB_{Tab}). After the study, participants were asked about their experience and filled in a series of questionnaires assessing their perceptions of and experiences with the mechanisms.

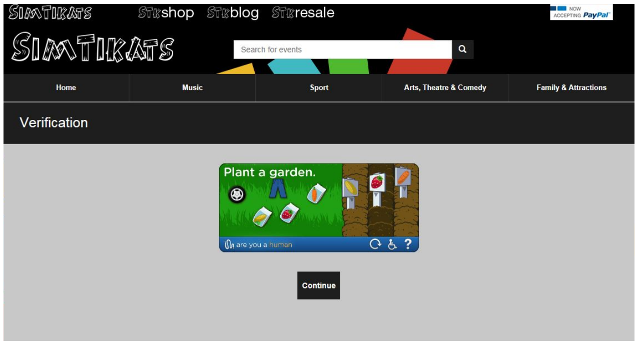

Figure 1. A screenshot of the verification page from the study showing PlayThru.

Any comments participants made and answers they gave to interview questions were recorded and transcribed. Transcriptions were assigned participant codes to protect the identities of individuals in line with the research ethics approval process at our university.

3.1. NoBot's verification stages

The NoBot verification mechanism differs from reCAPTCHA and PlayThru in that it has multiple stages. When activated, the application uses the entire screen of the device (as opposed to functioning only in the box seen in Figure 1). NoBot then provides brief instructions for positioning one's face for image capture. After instructions have been acknowledged, the user positions their face according to visual guides on the screen. The application then uses the device camera to capture a series of images. There is an interim stage where the application contacts the central service to have the images processed, after which the user is informed of the outcome and permitted to continue the primary task or retry (should verification fail).

4. Results

The study transcripts were analysed using thematic analysis [2]. The interviews were conducted so as not to prime and bias participants, who were free to make any comments and share their spontaneous reactions with the experimenter. This is a reason why some of the issues mentioned below have low counts, and may potentially be under-representative – here we capture user perceptions which have implications for the deployment of biometrics, but may also influence the uptake of those solutions.

4.1. Perception of face credentials

4.1.1 Use of personal images for human verification

Out of 87 participants, 24 expressed concern that someone may see their picture once it is captured, or that someone may be able to identify them based on that picture. PT29[4] explained:

> "[NoBot] *may be very dangerous in a way, it makes me wary if all the data will be saved, what sort of pictures have they actually taken, and will they be able to figure out who I am."*

Eight participants believed any gain in security was not worth the loss in privacy. 14 participants believed that other people may be concerned about their personal biometric data being used. 18 participants thought that taking their picture was intrusive, PT15 questioned the need for images:

> *"Why did they want my photo? I feel a bit like spied, why do they need my photo if I'm just buying tickets?"*

Overall, 12 participants were concerned that how their image is used would be dictated by NoBot and not them, or that the background scene around them could not be controlled by them (such as what else in the room is captured and analysed). Participants also worried about when in the process their picture can be taken and not just when they are explicitly told that images are being captured (this might have been influenced by the researchers setting camera permissions on the study machine ahead of the study). PM07 emphasised that they would be concerned about the security of their home:

> *"if you have a very nice house, for example. Then they know your address and where you live, then they know what the inside of your house looks like, through the windows. If you really think about this, it's a bit not dangerous but risky."*

4.1.2 Use of personal image as service credential data

Seven participants believed that their own face (or a person's face generally) was very personal, PT02 told us:

> *"at the same time it feels like something quite intimate as well, it is your face, it feels quite different to say Google scans your emails for keywords where that's just text, whereas* [your face] *is you."*

However, five participants appeared neutral about a process that uses face images to verify a person. For a smaller number of participants, the personal nature of a person's face was seen as making it more secure. For six participants, the uniqueness of a face as an identifier was a hindrance, preventing them from delegating use of an online service to someone else, PL27 explained:

> *"if it's for me only, it's fine. If I was sharing my computer with other people, it's not such a great thing, it stops them from doing stuff for me."*

[4] The first letter of the participant number indicates which condition they were in: "M"–M3$_{all}$ "L"–NB$_{Lap}$ and "T"–NB$_{Tab}$.

Three participants wondered if their camera images would be analysed by the service provider or verification technology to create targeted advertising, PL13 expressed their concern:

> *"they're storing the details to the face that you put in and you start getting spam, like things that are relevant to you because of your skin colour, make-up relevant to that."*

4.2. Expectations for use of personal image data

Of 87 participants, 68 (78%) requested that their images be deleted after the study. The highest number of deletion requests was in the mixed condition when participants tried all three mechanisms (90%) and the lowest in NB$_{Tab}$ when NoBot was used on the tablet (71%).

Ten participants believed that use of their image should be short-lived and dictated by the need of the service provider to use their image to provide them the service, PT09 explained:

> *"I just don't like my pictures being stored on the computer, and how long do they have that information for? When will it be discarded... when I've finished purchasing the ticket?"*

Similarly, ten participants wanted there to be an explicit assurance that images would be deleted after they have been used to provide the service. Nine participants asserted that persistent storage of their personal images would not be appropriate. For seven participants, seeing other people using the technology would be assurance for them that they can also use the technology. Eight participants wanted an explicit assurance of what it was that NoBot was able to do with their image or what they intended to do with it, and two participants wanted NoBot to demonstrate legitimacy using certificates. PT12 stated:

> *"it's implied that what I see is what they see, but it's not quite transparent."*

4.3. Perception of the NoBot implementation

A total of 20 participants believed that the purpose of NoBot was to verify that they were a human and not a robot. Five participants assumed that NoBot verified a person's identity or that the person was the legitimate account holder for ticket payment – one participant assumed that facial images could be used in cases of fraud after the fact. Two participants misunderstood what aspect of their face the technology was capturing, where one believed NoBot captured only eye movement. 18 participants thought NoBot was intended to identify an individual, and 18 thought it was specifically used to support the identification process related to live entertainment events. PT18 explained:

> *"I think it might be on my ticket, that would make sense, there'd be a picture on my ticket, it's me, it'll probably waste less time."*

Seven participants wanted an explanation of the whole process before it started (in some cases to help them understand why verification had failed, should the process go wrong), PT10 stated:

> *"I guess it's a bit odd if you don't know why they're doing it... 'Why do they need a picture of me?' "*

Three participants thought it was important for there to be an explanation of the motivation behind the product and why it was doing what it was doing. Three participants wanted instructions more specific to the context of use. Three participants thought the existing instructions should be clearer, whereas one person felt that having seen the instructions once they did not need to see them again during subsequent use of the product. PT12 suggested:

> *"what would be helpful would be if they said: 'Hold the tablet closer to your face.' "*

Nine participants preferred not see their face during image capture, and be guided by the application to the appropriate position in front of the device's camera, as this sidestepped any sense of self-consciousness. However, seven participants assumed that what was being captured by the application was the same as what they saw on the device screen (which was a simplified representation of their outline and not the full-colour photo image).

4.4. Technology Acceptance Model

To gauge participants' acceptance of the three mechanisms, they were asked to complete an instantiated Technology Acceptance Model (TAM) questionnaire [4]. The instantiation took several rounds of iteration between the members of our research team. To illustrate an example of a change that was made: "productivity" was replaced with "security".

Table 1 presents the statements used and average scores of in how far participants agreed with them on a 1-7 Likert scale (1 – strongly disagree, 7 – strongly agree). An ANOVA and then post-hoc tests were conducted on the mean scores for each mechanism and any significant differences are highlighted. Where table cells are shaded there was a statistically significant difference between mechanisms, with the darker cell being the lower value in each pair. For conditions NB$_{Lap}$ and NB$_{Tab}$, there were no statistically significant differences between the scores that participants gave. In the comparison M3$_{all}$, the differences in average scores between reCAPTCHA and PlayThru were small and not statistically significant. NoBot received the

Statement	reCAP	PlayThru	NoBot
1. Using this product increases the security of my online activities.	5.3	5	4.48
2. Using this product gives my greater protection of my online activities.	5	5	4
3. This product enables me to accomplish tasks more quickly.	3	3.6	3.3
4. This product supports critical aspects.	4.2	4.2	3.6
5. This product increases my productivity.	3.2	3.4	2.8
6. This product encourages me to conduct more activities online.	3.4	3.6	2.5
7. This product allows me to finish tasks quicker and more securely.	3.7	4.4	3.2
8. This product enhances my effectiveness in protecting my online activities.	4.8	4.3	3.8
9. This product makes it more secure to do my activities online.	5.1	4.8	3.8
10. Overall, I find this product useful for my online activities.	4.9	4.5	3.3

Table 1. Statements for an instantiated Technology Acceptance Model and an average score of in how far participants agreed with them on a 1-7 Likert scale.

lowest ratings of all mechanisms for all statements that were statistically significant. Participants rated NoBot as offering them not as great protection of their online activities, less encouraging them to conduct more activities online and overall, being less useful for their online activities.

The lower scores for protection and security are interesting here since in the interviews ten participants considered NoBot to be more secure than other mechanisms. An explanation for this apparent discrepancy could be that our participants perceived security more broadly, considering not just the protection of the website from bots but also the security of their own user account and associated data. 17 participants in the study imagined myriad attacks that could be performed on NoBot and 32 worried about the implications of a compromise of the NoBot image database.

4.5. Different service contexts

After the ticket purchases, participants were asked to indicate in what contexts they would be willing to use the mechanism(s) they tried. The contexts such as contributing to an online forum or buying a ticket were taken from real-life deployments of CAPTCHAs.

Table 2 shows the different contexts and the percentages of participants willing to use the three mechanisms to verify to complete these activities. There was no statistically significant difference between the NB$_{Lap}$ and NB$_{Tab}$ conditions, so they are combined in the first column. Overall, participants indicated greatest willingness to use the mechanisms for ticket purchasing which is not surprising given this was the scenario used in our study.

Participants were least willing to verify when contributing to a forum using PlayThru and NoBot. For NoBot, six participants stressed that the nature of forums is that the contributors want to be anonymous. This reveals a common perception that the service provider or other users would see the pictures taken by NoBot which was, to our knowledge, not the intention or expectation of its developers.

We saw that frequency of use mattered to participants as PM03 stated:

> *"Topping up my Oyster[5] is a small task so why do you have to get my picture? Because I top up like every month or every week so I don't want to do it, it gets in the way."*

Similarly PM05 stated frequency of use and value of the transaction mattered in other contexts,

> *"For Oyster, I felt it's such a basic thing where you're not going to be spending that much money, it doesn't make that much sense. For bidding on eBay, it would slow everything down, it wouldn't work. I spend a lot of time on eBay so that just wouldn't be a thing."*

Outside of the structured preference elicitation exercise around service contexts, throughout the study sessions participants shared thoughts about suitable or unsuitable situations for using NoBot. 21 participants stressed that they would use NoBot in situations where they would need to prove their identity, with eight mentioning travel-related transactions such as purchasing plane tickets. Nine participants also thought NoBot would be good to prove their identity for money-related activities with two participants suggesting it for banking and four for high-value transactions. In line with this, some participants also considered NoBot to be too heavy-handed for trivial ticket-buying (6) and low-value transactions (1). However, some participants expressed contrasting views due to their lack of trust towards NoBot, with one participant stressing they would not use it for anything involving money and another wanting to use it only for low-value transactions.

Within the suggested service contexts participants stated they would not use NoBot for time-critical purchases where they had to buy the tickets or goods fast (4 mentions) or if they needed to delegate a purchase (2), since they believed the item or ticket was then tied to their identity. Additionally, three participants emphasised they would not wish to be photographed to verify if they were in a private setting (*e.g.*, in their bedroom) or if they were buying sensitive items (2).

[5] An Oyster card is a payment card for London's public transport.

Context	**NB**$_{L+T}$	**reC**$_{mix}$	**PT**$_{mix}$	**NB**$_{mix}$
Contributing to an online forum	16	59	15	24
Buying tickets online	76	93	79	55
Browsing for plane tickets	50	76	55	45
Checking in for flights online	62	86	54	52
Topping up your Oyster online	52	66	69	31
Bidding on items on eBay	38	66	69	31
Logging in to Facebook from a different computer	47	66	66	34

Table 2. Percentages of participants willing to use reCAPTCHA, PlayThru and NoBot in different contexts.

5. Discussion

5.1. Biometrics – usable by default?

Researchers assumed that biometric solutions would be usable by default [6] as users do not need to memorise a password or remember to carry a token. However, a study by Sasse *et al.* [15] showed that usability is still a problem if a biometric solution is not integrated well, meaning if it is just added on and the underlying structure is not changed. In the organisation they studied, some participants used a biometric fingerprint reader to log in to their computer. Regular passwords changes were mandated by policy, and the participants who used a biometric fingerprint for logging in remained subject to these password changes. When asked to change their password, they had to find where they had written their previous password (usually on a post-it kept in a drawer), enter it, come up with a new password that would comply with the policy, enter it, note it down and re-enrol their fingerprint against that new password.

The study on NoBot presented here showed that the user interface confused participants, and that the technology did not explain itself, its purpose, or its process enough to avoid creating – rather than minimising – confusion. Participants became more accepting of the technology once provided with an explanation of what the technology was doing and why. Providing an explanation is important as demonstrated by Egelman *et al.* [5], who showed that users are more accepting of security-related delays if they are provided with a reason for why it is happening. Similarly, if face biometrics have a dedicated sampling stage, this in turn requires user effort and involvement in the capture process, and so guidance is needed to support the user. Different physical conditions may influence the reliability of the technology (as seen elsewhere [1]), and so users may need guidance to limit capture of poor-quality images.

5.2. Adoption by others as determinant of acceptability

A proportion of participants spoke about what "others" would think, or otherwise determined that they would use face biometrics (with the associated data retention and protection requirements) once a critical mass of users was reached. Heckle *et al.* [9] found participants were fatalistic about fingerprints, and keen to follow what others do. Sharing of biometric data with commercial entities has been noted as a concern for users elsewhere [8], although in this study there was a perception amongst some participants that if a company became successful, this very same success would compel them to treat personal image data appropriately with respect to customer privacy.

Biometrics would not necessarily be deployed in a "greenfield" environment where no verification or authentication technology already exists, and so they may compete not just with established technologies but also with the pervading perceptions of those technologies. Wash [18] for instance showed that home computer users can develop their own rationalisations for how technologies and related security threats affect them. Several participants in our study emphasised that it was hard to compare NoBot and PlayThru to reCAPTCHAs since they were so familiar with text-based CAPTCHAs.

Participant perceptions of security were another interesting finding. On the one hand, some participants thought NoBot was more secure than reCAPTCHA and PlayThru; while on the other hand, they rated it as giving them less security and protection. One explanation for it could be that participants distinguished between the security for the service provider as opposed to the security of their data. Another explanation might be that different participants had different contexts of application in mind where they might have thought for example that different situations required different levels of security.

It is important to note that NoBot is an unusual application of biometric capabilities since the user does not have to enrol to use it. This is an advantage in one way because it requires less effort; however, the enrolment can normally be used to explain the technology to the user [14], tell them how to present their biometric feature [16] and overcome a first hurdle which can increase user acceptance [3] and facilitate future interactions with the technology.

6. Conclusions

In this paper, we presented the results of a viability study of NoBot, a biometric solution using face recognition, as a CAPTCHA replacement, compared with the established reCAPTCHA and a game alternative – PlayThru. We found that participants perceived NoBot to be more suitable to use in some service contexts more than others, and that their sense of trust towards the company mattered. Our study stresses the importance of user testing of proposed technologies, looking at both their perceived usability and user acceptance, exploring what sense users make of the mechanisms for themselves and what explanations might be needed.

For future work, we will assess the face biometric technology across a wider range of services, beyond the ticket-buying context. We will also study use of the technology in the wild, not just outside the lab environment but also on participants' personal computers and mobile devices. These observations will be instrumented to capture expected use, but also user reactions when encountering difficulties.

6.1. Recommendations

In our study, we assessed a range of existing and prototype commercial products. Not every product was perceived as appropriate or a natural fit in every context. When biometric technologies are being developed or assessed for viability, it is important to examine user understanding of these technologies and how they interact with them, as specialised instructions may be necessary. Any instructions should be crafted so as not to overload the user, but nonetheless in the absence of supporting information individuals may formulate their own rationalisations as to how the technology works (for instance remaining still only at the start of image capture or turning their head during capture).

Further, it is crucial to assess a technology within the context of the task(s) that they would support (here ticket buying). On needs to determine where users perceive the technology as being most appropriate to use – this can not only identify where a biometric technology is seen as a natural fit for a task, but also expose any misconceptions about what the technology would do in that given context.

It is important to examine user perceptions not just of the technology being assessed, but also relative to the technology it may supplant – biometric solutions can potentially replace "what you have" and "what you know" authentication technologies that are already in use, and existing user understanding of those technologies may be applied to a new technology or related to it in some way.

References

[1] C. Bhagavatula, K. Iacovino, S. M. Kywe, M. Savvides, B. Ur, J. Jung, S. Schechter, L. F. Cranor, A. L. Durity, A. Marsh, et al. Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. In *USEC 2015*, 2015.

[2] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[3] L. Coventry, A. De Angeli, and G. Johnson. Usability and biometric verification at the atm interface. In *Conference on Human Factors in Computing Systems (CHI'03)*, pages 153–160. ACM, 2003.

[4] F. D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340, 1989.

[5] S. Egelman, A. Acquisti, D. Molnar, C. Herley, N. Christin, and S. Krishnamurthi. Please Continue to Hold: An empirical study on user tolerance of security delays. In *Workshop on the Economics of Information Security (WEIS'10)*, 2010.

[6] M. C. Fairhurst, R. M. Guest, F. Deravi, and J. George. Using biometrics as an enabling technology in balancing universality and selectivity for management of information access. In *Universal Access Theoretical Perspectives, Practice, and Experience*, pages 249–259. Springer, 2003.

[7] K. K. Greene, M. A. Gallagher, B. C. Stanton, and P. Y. Lee. I Can't Type That! P@$$w0rd Entry on Mobile Devices. In *Human Aspects of Information Security, Privacy, and Trust (HAS 2015), HCI International 2014*, pages 160–171. Springer, 2014.

[8] T. Halevi, T. K. Kuppusamy, M. Caiazzo, and N. Memon. Investigating users' readiness to trade-off biometric fingerprint data. In *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, pages 1–8. IEEE, 2015.

[9] R. R. Heckle, A. S. Patrick, and A. Ozok. Perception and acceptance of fingerprint biometric technology. In *Symposium on Usable Privacy and Security (SOUPS'07)*, pages 153–154. ACM, 2007.

[10] H. Khan, U. Hengartner, and D. Vogel. Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In *Symposium on Usable Privacy and Security (SOUPS'15)*, 2015.

[11] K. Krol, S. Parkin, and M. A. Sasse. Better the devil you know: A user study of two CAPTCHAs and a possible replacement technology. In *Under Review*.

[12] D. Pogue. Time to Kill Off Captchas. *Scientific American*, 306(3):23–23, 2012.

[13] G. Reynaga, S. Chiasson, and P. C. van Oorschot. Exploring the Usability of CAPTCHAS on Smartphones: Comparisons and Recommendations. In *USEC 2015*, 2015.

[14] M. A. Sasse. Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems. *Security & Privacy, IEEE*, 5(3):78–81, 2007.

[15] M. A. Sasse, M. Steves, K. Krol, and D. Chisnell. The great authentication fatigue–and how to overcome it. In *International Conference on Cross-Cultural Design, HCI International 2014, Heraklion, Crete, Greece*, pages 228–239, 2014.

[16] M. Theofanos, R. Micheals, J. Scholtz, E. Morse, and P. May. Does habituation affect fingerprint quality? In *CHI'06 Extended Abstracts on Human Factors in Computing Systems*, pages 1427–1432. ACM, 2006.

[17] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David. Biometric authentication on a mobile device: A study of user effort, error and task disruption. In *Annual Computer Security Applications Conference*, pages 159–168. ACM, 2012.

[18] R. Wash. Folk models of home computer security. In *Symposium on Usable Privacy and Security (SOUPS'10)*. ACM, 2010.