The New Domain of Automotive Biometric Privacy: The Link Between Privacy Concerns and Privacy Behaviours

Liam Ashby: 12240087

Masters of Behavioural Data Science

Supervised by Abdallah El Ali (Centrum Wiskunde Informatica) and Robert Zwister (UvA)

Submitted 20th November 2019

Word count: 8228

Abstract

Biometric technologies are predicted to be included in one third of all new cars by 2025 (Allianz, 2016). However, no research has investigated the relative value of biometric data in an automotive context, or the mechanisms that may drive users' to share personal biometric data. In this early work two separate card sorting studies were conducted to investigate users privacy concerns surrounding forty different types of biometric data. From these two card sorting studies, four *low* concern, and four *high* concern types of biometric data were selected to be used in an online forced-choice decision task. In the forced-choice task, participants were asked whether or not they would share the four *low* concern, and four *high* concern types of biometric data, in exchange for two different benefits - authentication, and alertness monitoring. Participants were found to share *low* concern biometric data more frequently than *high* concern biometric data in exchange for the benefit of *alertness monitoring*, but not for the benefit of *authentication.* Future work should look to explore how users share other types of biometric data in an automotive context, and in exchange for benefits other than *authentication* and *alertness monitoring*

Automobiles are no longer just a means of transportation. Now equipped with a wide variety of different sensors, automobiles are capable of collecting large volumes of high fidelity data about drivers in real time. With more data about drivers car manufactures are now looking to provide more personalised features that benefit driver experiences. Examples of personalised experiences include personalised authentication, map routes, alertness monitoring, and detecting medical emergencies (Villa, Gofman, & Mitra, 2018). Therefore, designing a vehicle that can transport a person from one location to another is no longer enough, car manufacturers are also looking to optimise the personalised experiences of drivers'.

In order to facilitate more advanced automotive user experiences, naturally more sensitive data needs to be collected from drivers. Such sensitive data is often biometric in nature. The word biometric comes from the combination of the two Greek words *bio* and *metric*, essentially translating to life measurement (Alsaadi, 2015). Strictly speaking, for data to be biometric, it must be *universal* (every person has the characteristic), *distinctive* (any two people should be different in terms of the characteristic), *permanent* (characteristic should not vary over time), and *collectable* (characteristic should be measurable) (Obaidat, Traore, & Woungang, 2018).

Many different types of biometrics exist. Examples of common physiological biometrics include fingerprints, facial features, and hand geometry (Alsaadi, 2015). Examples of common behavioural biometrics include keystroke dynamics, mouse dynamics, gesture dynamics, signature dynamics, voice, and gait features (Obaidat et al., 2018). Biometrics can be used in automotive context in a wide variety of ways, including but not limited to; fingerprint authentication, facial authentication, and heart rate monitoring (Rathore & Gau, 2014; Villa et al., 2018).

Although collecting biometric data can improve driver experiences, the sensitive nature of biometric data has the capacity to lead to privacy concerns amongst drivers (Nawrath, Fischer, & Markscheffel, 2017). If drivers are concerned about how their biometric data is being collected, and used by car manufacturers, it follows that they will be less likely to want to share their data. Therefore some drivers may be willing to forgo more personalised experiences, in exchange for not sharing personal biometric data. In other words, drivers who choose not to share their biometric data can be seen as placing a higher *value* on their data and privacy.

Personalised automotive experiences are becoming more and more ubiquitous (Lozoya-Santos, Sepúlveda-Arróniz, Tudon-Martinez, & Ramirez-Mendoza, 2019), yet no work has specifically attempted to measure the *value* of automotive biometric data. Understanding the relative *value* of different types of personal automotive biometric data is important, because it in turn sheds further light on the nature of the cost-benefit analyses drivers undergo when deciding to share their data. Thus, without an understanding of the *value* of automotive biometric data, it is difficult to design biometric technologies and policy that maximise driver experiences whilst also maintaining driver privacy. Therefore, it follows that more research is needed to investigate the *value* users' assign to their personal biometric data in an automotive context.

In what follows of the research of the introduction, provide an account of theoretical and methodological approaches often used to quantify the *value* users' assign to their personal data. First, the privacy calculus model, which outlines how personal data *value* is conceptualised within the context of data sharing. Second, monetary and behavioural approaches to measuring the *value* of personal data. Lastly, the link between personal data *value* and general privacy concerns. Ultimately, concluding that a behavioural approach that takes into account privacy concerns, is the most suitable approach to measuring the *value* of automotive biometric data.

Privacy Calculus Theory: A Brief Review

The privacy calculus model is a popular framework for investigating how users make cost-benefit trade offs (Dinev & Hart, 2006). The theory outlines that when making a decision to share their data, users' consciously weigh up the costs (e.g. loss of privacy), with the benefits of sharing their data (e.g. personalised services). If the benefits are found to outweigh the costs, users' are more likely to share their data. For example, a social media user may choose to share their data to connect with other social media users, or they may chose to abstain from social media due to privacy concerns. A user who does not share their personal data, can be thought of putting a relatively higher *value* on their data (Krasnova, 2009). Furthermore, other work has provided empirical support that users are more likely to share their data, if they believe the costs outweigh the benefits (Dinev & Hart, 2006)

Privacy calculus theory is helpful in the context of measuring the *value* of personal data, because it explicitly defines the costs and benefits of sharing personal data. In the case of sharing data, the "cost" of sharing for each user is their respective loss of personal privacy. Therefore the *value* of personal data can be thought of as the personal cost of sharing data in exchange for personal benefits. Two main approaches have been explored within the literature to estimate the *value* of personal data - monetary and behavioural. I will review literature relating to each approach, with the ultimate aim of detailing that a behavioural approach is a preferable method for estimating the *value* of personal data.

The Value of Data: A monetary approach

Various studies have adopted a literal approach to measuring the *value* of personal data, in which participants are instructed to place a monetary value on different types of personal data (Staiano et al., 2014; Hirschprung, Toch, Bolton, & Maimon, 2016). Typically, these studies utilise either a *willingness to pay* (WTP) or *willingness to accept* (WTA) framework. The former, relates to the amount of money users' are willing to pay to keep their data private, and the latter, the amount of money users' are willing to accept in the case of a loss of data privacy. For example, if a participant is willing to pay a larger amount of money to keep their location data private, compared to their social media data, conceptually they can be seen to place a higher *value* on their location data.

Survey approaches have been often been utilised to evaluate the *value* of personal data in monetary terms (i.e. WTP or WTA). In a study conducted by Bauer, Korunovska, and Spiekermann (2012), Facebook users' were asked to estimate the amount of money they would be willing to pay to keep their personal information private. Interesting, approximately half of participants were found to not be willing to pay at all. Suggesting that participants in general placed a very low *value* on their personal social media data. In another study by Personal Information Protection Commission (2013) participants were presented with hypothetical situations in which they had to decide the amount of money they would pay to keep their data private. Amongst different types of data (e.g. basic, healthcare), identification information was found to be most highly valued. Surveys which adopt a monetary approach therefore present a seemingly practical and valid means of measuring the relative *value* of different types of data, and in different contexts.

However studies which utilise surveys as means of pricing personal data have drawn considerable criticism, in that they often ask participants to imagine hypothetical situations. In response to these criticisms, other work has looked to estimate personal data *value* using more real world approaches (Staiano et al., 2014; Hosio et al., 2016). Rather than asking participants to respond to hypothetical situations in which they imagine they are selling their data, participants are tasked with selling their actual data in exchange for benefits. Often, data is collected with an experience sampling methodology, in which participant data is collected over time on a regular basis.

For example, Staiano et al. (2014) conducted a six week long user study with sixty participants, and collected the daily valuations of four different types of personal information (i.e. location, communications, media, apps). Reverse-price auctions were used, where users had to bid to sell their personal information. Amongst these different data types, it was found that location data was sold at the highest average price. Thus on average users requested the largest compensation for their loss in location data privacy (i.e. largest WTA). In another similar field study conducted by Hosio et al. (2016), it was found that users' value the first and last ten percent of the smartphone value differently in terms of monetary value. Therefore *data amount*, as well as *data type* is important in determining the *value* of personal data. Real world studies like surveys, therefore present a means of estimating data *value* but in a more ecologically valid manner.

Yet monetary approaches to placing a *value* on data in general have also drawn some criticism. As argued by Buck, Stadler, Suckau, and Eymann (2017), privacy should not be valued in terms of monetary terms for the reason that users are not able to evaluate the monetary value of their data. In a survey conducted by Nget, Cao, and Yoshikawa (2017), it was found that nearly half of the participants stated they had no idea for how much they would sell their personal data. Most users' are far more familiar with the concept of using services and implicitly 'paying' by sharing their data, than they are with the concept of selling their data for money. Therefore asking participants to sell their data can feel contrived, and not very realistic. In the next section I will present an alternative approach to investigating the *value* of data, by investigating the sharing behaviours of users.

The Value of Data: A behavioural approach

Another body of work has looked to investigate the value of data, but not in monetary terms. Rather, by conceptualising *value* as the willingness (or unwillingness) to share personal data. Often, this achieved by presenting participants with different scenarios in a survey form, and asking participants to rate each scenario or select their preferred option. For example, a participant could be presented with a situation in which they can choose to share *data X* with *company Z*, or *data Y*. If they choose to share *data X*, but not *data Y*, then it is inferred that the user places a higher *value* on *data X*. Thus, unlike methods which measure monetary value, behavioural approaches do not force users' to artificially place a monetary value on their data. Rather, the relative *value* of data is inferred by comparing the sharing behaviours of users' across different types of data.

Various studies have adopted this approach in a wide range of different contexts, and with different types of data. Martin (2013) conducted a context-based survey with 979 participants to rate over 39,000 hypothetical vignettes to investigate people's privacy expectations about using mobile apps. By manipulating different contextual factors including *who* (the data collector), *what* (type of disclosed information), *why* (application purpose), and *how* (use of data by data collector), it was found that certain types of data to be particularily sensitive (image and contact), but not others (i.e. demographic and friend information).

Grande et al. (2015) assigned nationally representative participants (N = 3,336) with and without prior cancer to six of 18 scenarios describing different uses of electronic health information. Participants rated each scenario on a scale of 1 to 10 assessing their willingness to share their electronic health information. It was found participants with cancer were more willing to share genetic information that participants without cancer. Thus in this case, because cancer patients were more willing to share sensitive genetic information, they can be conceptualised as placing a lower *value* on sensitive information compared to non-cancer patients.

Similar to monetary survey approaches, behavioural survey approaches have however drawn criticism for using survey based approaches to investigating sharing behaviours. As such, some research has begun to investigate the privacy behaviours using mobile phone applications to record data sharing (Shih, Liccardi, & J.weitzner, 2015; Perentis et al., 2017). Similar to studies which utilise experience sampling methodologies to value data in monetary terms, these studies have arguably a higher ecological validity than survey based approaches. However, practically they are far more challenging to deploy, as applications have to built to collect data, and participants are required to participate for extended periods of time (e.g. up to three months) (Shih et al., 2015).

Behavioural survey approaches, although arguably not as ecologically valid as other behavioural real world approaches, are still preferable to monetary approaches in general, in that data *value* can be derived but without asking participants to artificially value their data in monetary terms for reasons described earlier. Furthermore, other research has actually shown that behavioural survey approaches approximate real-world decision making and results can be generalised to real-world data sharing behaviours (Hainmueller, Hangartner, & Yamamoto, 2015). Thus, survey based behavioural approaches are arguably the most ecologically valid and low cost means to measuring the relative *value* of data in an applied context.

A new domain: Value of Automotive Biometric Data

The previous two sections have highlighted two different approaches to estimating the *value* of data in wide variety of different contexts. From my analysis, I concluded that survey based behavioural approaches are a more powerful, practical, and ecologically valid means to estimating *value*. I will now provide an overview of how a survey based behavioural approach can be applied to the domain of automotive biometric data. First I will provide a overview of biometric technology, and how it can be applied to an automotive domain. Then, I will justify why a behavioural approach is a justified and powerful methodology to estimating the *value* users' assign to their automotive biometric data.

Two notable benefits of using biometrics in cars include (1) *authentication*, and (2) *driver alertness monitoring*. *Authentication* as the name suggests, involves using biometric technologies to verify the drivers identity. *Authentication* can be achieved with many different biometrics in cars, including but not limited to using fingerprints, facial recognition, and speech. For example, a driver may authenticate themselves using their fingerprint or voice, to unlock the car, or gain access to personalised features (e.g. maps, media/entertainment) (Villa et al., 2018). Driver *alertness monitoring* on the other hand involves monitoring the psychological state (e.g. fatigue) of the driver, with the aim of reducing potential accidents. An example of *alertness monitoring* is yawn detection (Akrout & Mahdi, 2017), which can detect if a driver is yawning frequently, and should potentially take a break before resuming driving (Villa et al., 2018).

In order to benefit from biometrics in automobiles, users' are required to share their data often with car manufacturers. In sharing their data users' can potentially become subject to a wide variety of privacy related attacks. For example, it has been found that with the use of fifteen different automobile sensors it is possible to identify fifteen different drivers with 100 percent accuracy (Enev, Takakuwa, Koscher, & Kohno, 2015). If insurance companies have access to information which can so easily identify drivers, they may want to change the premiums of drivers who specifically violate their terms of agreement. Therefore, there is cause for privacy concerns amongst drivers when sharing their personal biometric data.

Given there is cause for privacy concerns amongst drivers who share their biometric data, it important to investigate how drivers perceive the relative *value* different types of automotive biometric data. Understanding the *value* drivers' assign to their data, can shed on the cost-benefit decisions drivers make when sharing personal data. Understanding how drivers make decisions to share personal data can then in turn help develop policies, and personalised privacy preferences that optimise driver privacy, whilst still allowing drivers to enjoy the benefits provided by sharing their data.

Work by Soley, Siegel, Suo, and Sarma (2018) represents the first attempt to place a *value* on automotive data. In developing and testing a linear model with data type, quantity and value as inputs, it was estimated that collectively automotive data is worth between 11.6bn and 92.6bn US dollars. Importantly, the *value* of automotive data was found to vary depending on the type of data. Although an important first step, more work is needed, as Soley et al. (2018) adopted a monetary approach, and made a wide array of assumptions regarding the supply, demand and elasticity of automotive data. Furthermore, as illustrated in a previous section, behavioural approaches to measuring the *value* of data more readily approximate real-world decision making. Thus more work is required to investigate the relative *value* of different types of automotive biometric data, but with a behavioural approach that is not constrained by the limitations of monetary approaches.

Linking attitudes to behaviours

In the previous section I illustrated that more work is needed to evaluate the relative *value* users' place on their automotive biometric data. Although a behavioural approach is a sufficient means of investigation, behavioural approaches in the past have been found to commonly suffer from one unifying flaw. They often compare the sharing behaviours of users' across different data types without trying to link attitudes to behaviours. For example, using a behavioural approach, Martin (2013) found certain types of data (e.g. image, location) to be share less frequently. Martin (2013) did not investigate why image and location data may have been shared less frequently. Merely finding that certain types of data to be shared more or less frequently does not help explain the mechanisms that underlie users' decisions to share data.

Some research has looked into investigate the mechanisms behind *privacy behaviours*, albeit, without using the specific *behavioural approach* outlined in previous sections. These studies often look to link *privacy concerns* to *privacy behaviours* (i.e. sharing behaviours). Privacy concerns as defined by Kolakis (2017) as quite generic attitudes towards privacy that do relate to a specific context, and can be generalised. For example, a user may have a high degree of concern for their privacy in general, reflected by behaviours that maintain their privacy in a wide range of domains (e.g. healthcare, social media).

Moreover, recent surveys support the direct link between *privacy concerns* and *privacy behaviours.* In a survey conducted by Boyes et al. (2012) it was found that 54 percent of mobile application users' chose to uninstall applications after learning how much personal information was being collected. In a telephone survey conducted by Lutz and Strathoff (2014), participants completed several questionnaires relating to privacy concerns and privacy behaviours. Furthermore, a weak but significant relationship was found between the two.

Other work has however found no relationship between privacy concerns and privacy behaviours. For example, Lee, Park, and Kim (2013) conducted a series of different semi-structured interviews and found users to report they share personal information despite privacy concerns, because of the benefits they receive from sharing. As outlined by Kokalakis (2017), one reason as to why past research has found inconclusive evidence linking *privacy concerns* to *privacy behaviours*, is studies in these area often use a wide variety of different methodologies. Furthermore, *privacy behaviours* are often measured via self-report surveys, which do not provide reliable and valid predictions of actual user *privacy behaviours.* A survey based behavioural approach as outlined in previous sections, would arguably measure actual user *privacy behaviours* in a valid manner.

Although no work has looked to see if there is a link between *privacy concerns* and *privacy behaviours* in the automotive biometric domain, some research has begun to investigate *privacy concerns* relating to biometrics. In work conducted by Merrill, Chuang, Cheshire, and Holgate (2019), participants were asked to rank a list of different biosensors by how by likely they are to reveal what participants are thinking and feeling. They found that participants to rank certain biosensors (e.g. facial expressions, brainwaves) as more revealing than others (e.g. step count, accelerometers). In other words, participants were found to have different *privacy concerns* relating to each biometric.

Although important preliminary work, Merrill et al. (2019) did not look to link general *privacy concerns* to *privacy behaviours* (e.g. in an automotive domain). Furthermore, other issues with Merrill et al. (2019) are also worth noting. First, only a very limited number of biometrics were selected for ranking. Second, Merrill et al. (2019) chose to use ranking as oppose to clustering, despite other work demonstrating that it is possible to segment users based upon *privacy concerns* (Lim, Woo, Lee, & Huh, 2018). Although ranking tasks are better than self-report surveys, they do not produce distinct groupings that one gets from using clustering. Grouping biometrics into *high concern* and *low concern* segments creates a taxonomy which can be easily applied to try explain differences sharing behaviours. Ranking does not produce a taxonomy, simply an ordering of features.

Current Study

Throughout the introduction I have illustrated several points. First, behavioural approaches are preferable to monetary approaches when comparing the relative *value* of personal data. Second, studies which utilise behavioural approaches often do not look to account for mechanisms explain why certain types of data are shared more often, such as *privacy concerns.* Thus, the aims of the current study were two-fold. First, to investigate biometric privacy concerns, addressing the limitations of Merrill et al. (2019). This resulted in the first research question being formed as such.

Research Question 1: How do users' cluster biometric features based upon privacy concerns?

The second aim of the current study was to build upon previous behavioural approaches to estimating personal data. Although previous work has investigated *privacy behaviours* in other domains (e.g. healthcare, insurance), no work has looked into automotive biometric data. Furthermore, no work has looked to see if differences in automotive biometric data sharing can be explained by privacy concerns. The second research question was therefore formulated as such:

Research Question 2: Do users' privacy concerns explain differences in automotive data sharing behaviour?

Design. In order to answer both of these research questions, the study was split into three sub-studies. First, an open card sorting study was conducted to investigate how users group biometric features based upon their *privacy concerns.* Participants were asked to cluster biometrics by how well they could be identified by each biometric features. Second, a closed card sorting study was conducted to confirm the results of the open card sorting study, and select features which were deemed to be *low concern* and *high concern.*

These features were then used in an online decision task to in which participants chose to either share or not share these *low concern* and *high concern* concern biometric features with a hypothetical car manufacturer. The benefit for sharing data was also manipulated to see if differences between *low concern* and *high concern* concern existed irrespective of benefit type. The two benefits that were chosen were *authentication* (e.g. unlocking car with fingerprint), and *alertness monitoring* (e.g. detecting driver who is yawning).

Hypotheses. As studies one and two were exploratory in nature, no specific hypotheses were formed. However, hypotheses were formed for decision task in study three. Although past research has provided conflicting evidence that privacy concerns lead to congruent privacy behaviours, these studies often did not utilise behavioural measures which approximate real-world sharing. Thus, it was predicted that participants would still be more likely to share the *low concern* features than *high concern* features. Given there is no evidence to suggest otherwise, it was also predicted than this would be the case for both benefit types of *authentication* and *alertness monitoring.*

Hypothesis 1 *Participants will be more likely to share low concern data than high concern data irrespective of benefit type.*

Method

An ethics application was submitted and approved by the ethics board for the department of Psychology for all three studies. The application id was *2019-PML-10145.*

Study One: Measures

Open Card Sorting. The primary purpose of study one was to create a list of biometric features (e.g. face, eyes), and investigate how participants cluster the features into distinct groupings. Thus, open card sorting was deemed an appropriate method to investigate such a question. Open card sorting is a popular method, shown to have high cross-study reliability (Katsanos et al., 2019), which asks participants to sort features (i.e. cards) into groups based upon a question. For the purposes of study one, this involved participants sorting different biometric features based upon how well they could be identified by each biometric feature. Although the task instructed participants to think about *accuracy*, features deemed to be *high accuracy* and *low accuracy* can also be thought of as being *high concern* and *low concern* features respectively. Materials for open card sorting task can be found in Appendix A.

Card selection process. An extensive literature search was conducted to create a list of biometric features to be grouped using open card sorting. The ACM and Google Scholar digital libraries were queried for biometric technologies used in various contexts (e.g. mobile, health). Biometric technologies that could be theoretically applied to an automotive context were then selected to be used in the open card sorting study. In total, thirty-three cards were selected. It is worth noting that instead of labelling cards with the biometric technology (e.g. EEG), cards were labelled with the feature the technology measures (e.g. my brain wave patterns). This was to help participants with little technical background understand the card, and focus on what the technology measures, not the technology itself. The cards used in the open card sorting task can be seen in Table 1, along with their associated biometric technologuy.

Table 1

Cards used in the open card sorting task, their associated technology, and references.

Card	*Technology*	*References*
My face	Face recognition (2D,3D)	(Obaidat et al., 2018)
My facial expressions	Facial emotion expression recognition	(Obaidat et al., 2018)
My ears	Ear identification	(Ragan, Johnson, Milton, & Gill, 2016))
My eyes	Eye tracking; iris and retina	(Obaidat et al., 2018)
My physical activity	Physical activity recognition	(Lu et al., 2017)
My fingerprints	Fingerprint recognition	(Obaidat et al., 2018)
My walking style	Gait recognition	(Obaidat et al., 2018)
My hands	Hand geometry recognition (2D,3D)	(Obaidat et al., 2018)
My sleeping patterns	Sleep classification	(Längkvist, Karlsson, & Loutfi, 2012)
My smell	Odor recognition	(Inbavalli & Nandhini, 2014)
My handwriting	Optical Character Recognition (OCR)	(Hartanto, Sugiharto, & Nur Endah, 1999)
My touches on a smartphone	Touchscreen dynamics	(Obaidat et al., 2018)
My mouse movements	Mouse movement dynamics	(Obaidat et al., 2018)
My typing on a keyboard	Keystroke recognition	(Obaidat et al., 2018)
My voice	Speaker identification, verification	(Zhang, Tan, & Yang, 2017)
My teeth	Teeth recognition	(Kumar, 2016)
My footprints	Footprint (size and shape) recognition	(Nazmi et al., 2016)
My heartbeat	Electrocardiogram	(Obaidat et al., 2018)
My writing style	Stylometry	(Obaidat et al., 2018)
My smartphone app usage	App usage fingerprints	(Tu et al., 2018)
My posture	Posture recognition	(Patel, Bhatt, & Patel, 2017)
My media listening history	Music emotion recognition	(Yang, Lin, & Chen, 2009)
My media watching history	Profiling TV viewers using data mining	(Spangler, Gal-Or, & May, 2003)
My driving style	Driver and driving style recognition	(Van Ly, Martin, & Trivedi, 2013)
My SMS messages	User classification	(Hu, Sun, Tu, & Huang, 2013)
My locations on a given day	Location tracking	(De Montjoye, Hidalgo, Verleysen, & Blondel, 2013)
My hand sweat	Galvanic Skin Response	(Liu, Fan, Zhang, & Gong, 2017)
My hand gestures	Hand gesture recognition	(Panwar & Singh Mehra, 2011)
My electrical brain activity	Electroencephalography	(Tan & Nijholt, 2010)
My breathing	Breathing monitoring	(Niu et al., 2019)
My genetic makeup	DNA matching	(Obaidat et al., 2018)
My interaction patterns with an in-car information system	Modelling driver interactions	(Harvey, 2011)

Study One: Procedure

Participants were tested in a laboratory environment. First participants completed a signed information and consent form, and were presented with a demonstration of an open card sorting study. Before starting, participants were instructed that if they wished to they could talk through their decision making aloud. Participants then completed the open card sorting task on a table, during which time instructions remained at the top of the table to remind participants. The instructions stated *"Please group the cards into distinct sets by how accurately someone can identify you using only the feature stated on the card".* After sorting all the cards, participants were provided with pen and paper to provide a label for each group. For those participants which did not talk aloud during the task, their decision making was then discussed with the instructor. All sessions were audio recorded, and lasted approximately ten to thirty minutes.

Study One: Participants

Eleven participants (6 female, 5 male) were recruited, aged between 21-38 (M = 25.6, SD = 5.4). Eight were students, and the remainder graduate-level or higher. Seven stated they had a technical background. Three participants had driving experience, two were learning how to drive, and the rest no experience. Participants did not receive monetary compensation.

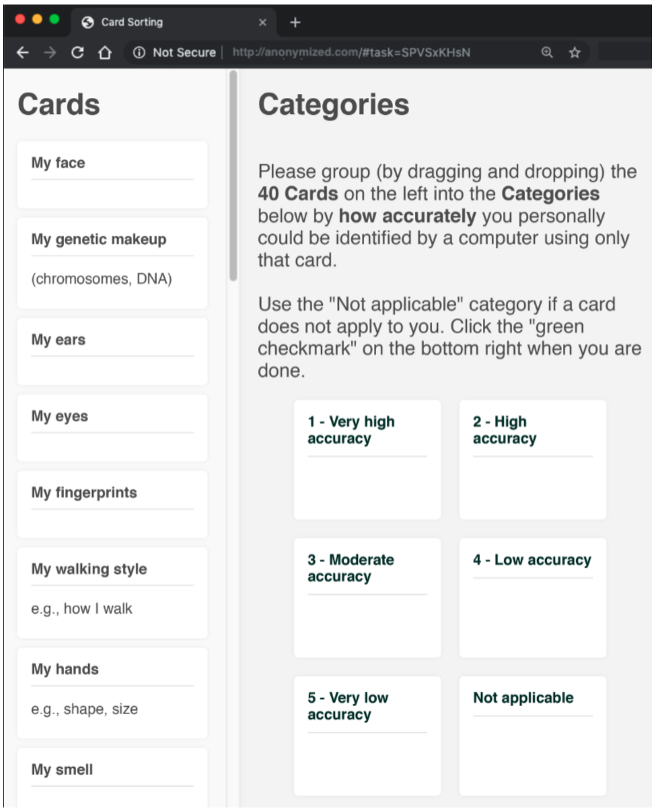
Study Two: Measures

Online Closed Card Sorting. Like open card sorting, closed card sorting is a widely used method (in web design) to create taxonomies based on users' groupings of the content. Unlike open card sorting however, closed card sorting aims to group content into a predefined set of groups (i.e. number of groups). It is therefore common to first use open card sorting to explore how participants group content, devise a appropriate labels for each group, and then using closed card sorting to confirm content groupings. An online website was built to host the closed card sorting task. Research has found twenty to thirty participants to be sufficient to investigate content groupings (Tullis, Wood). As such, upon launching the aim was to collect over twenty participants.

Card Selection Process. Cards that were used in the open card sorting study were again used in this study. Unlike in the closed card sorting study, examples were subtitled underneath certain cards that were found to be somewhat ambiguous. For example, for the card 'my genetic makeup', in parentheses "DNA" and "Chromosomes" were added. Participants were also instructed to focus on how accurately they could be identified by a computer, and not a human. These alterations were made, given feedback from the open card sorting study. A few cards were also added that were missed in the initial literature search for the open card sorting study (i.e. muscle movements, eye gaze patterns). In total, forty cards were used.

Study Two: Procedure

Participants were tested in an online environment. As shown in Figure 1, participants were presented with cards on the left-hand side of the screen, with descriptions underneath. Seven boxes served as categories for participants to drag cards into. Each box was labelled from Very High Accuracy to Very Low Accuracy. Instructions were also provided above the boxes. Instructions stated, *“Please group (by dragging and dropping) the 40 cards on the left into the Categories below by how accurately you personally could be identified by a computer using only that card”.* Once participants had completed the task, they clicked ’next’ and were presented with a new page. On the new page, participants were able to enter their email address for the chance to enter a gift voucher lottery.



Cards

My face

My genetic makeup

(chromosomes, DNA)

My ears

My eyes

My fingerprints

My walking style

e.g., how I walk

My hands

e.g., shape, size

My smell

Categories

Please group (by dragging and dropping) the **40 Cards** on the left into the **Categories** below by **how accurately** you personally could be identified by a computer using only that card.

Use the "Not applicable" category if a card does not apply to you. Click the "green checkmark" on the bottom right when you are done.

1 - Very high accuracy

2 - High accuracy

3 - Moderate accuracy

4 - Low accuracy

5 - Very low accuracy

Not applicable

Figure 1. A screenshot of the closed card sorting study. Forty cards were placed on the left hand side, some with extra descriptions. On the right hand side six categories existed for respondents to click and drag cards into

Study Two: Participants

Thirty nine respondents completed the closed card sorting task. No further demographic information was collected.

Study Three: Measures

Decision Task. No pre-existing measure was available to investigate the sharing behaviours of users in an automotive biometric context. Therefore, a new measure had to be designed and developed. The new measure needed to be able to both explore how willing participants are to share their biometric data in regard to (1) data type and (2) the benefit they would receive by sharing their data.

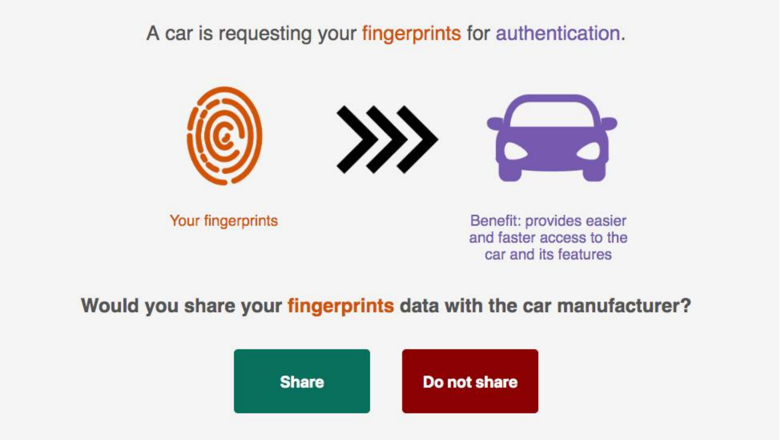
Taking inspiration from other similar tasks (Grande et al., 2015; Martin, 2013) the new measure included a series of hypothetical scenarios, in which participants could choose to share or not share their data. For example, as can be seen in Figure 2, participants were presented with situations in which they could share their data (e.g. fingerprint), and in turn receive a benefit (e.g.authentication). The task was colour coded, such that objects and text relating to benefits were coloured purple, and objects and text relating to feature type were coloured red. This was to aid in separating the different elements on the screen for ease of reading.

Study Three: Procedure

The decision task was distributed online on various forums, and social media. In total, respondents were required to make the decision to share or not to share eight different features (i.e. types of data) in exchange for two different benefits (i.e. authentication and alertness monitoring). Thus participants completed sixteen trials in total. All authentication and alertness trials were separated into two groups of eight. Whether participants received the alertness or authentication trials first was alternated. The order different features within each of the two blocks were presented was randomised.

Study Three: Participants

One hundred participants were recruited (34 female, 52 male, 5 non-binary, 9 non-disclosed), aged between 18 and 57 (mean = 28.56, SD = 8.44). Fifty three percent of participants had over five years of experience driving, with 19 percent of participants having no driving experience.



A car is requesting your fingerprints for authentication.

Your fingerprints

Benefit: provides easier and faster access to the car and its features

Would you share your fingerprints data with the car manufacturer?

Figure 2. Example trial used in the decision task. Images and words relating to data were coloured in orange, and data relating to benefit and car manufacturer were coloured in purple

Results

Study One: Open Card Sorting

Descriptive. Most participants were found to create a ranked list of groups ranging from low to high accuracy. Example labels that participants wrote down from the high accuracy (*high concern*) groups included "That's me!", and "Bio features". Examples from the low accuracy (*low concern* group included "No one can identify me" and "Things I do almost the same as other people". Although the labelling was fairly consistent across participants, group size did vary, with the mean group size being 5.8 (SD = 1.1).

Group clustering. To further investigate the nature of participant groupings, Ward's hierarchical clustering method was applied to the clustering card sorting data with Jaccard similarity used as a distance measure (Kruskal & Black, 2012). There was no reason to presume the optimal number of clusters, hence, hierarchical clustering was chosen over K-means clustering. Ward's linkage method was selected for several reasons. First, Ward's linkage has been shown to produce even sized clusters (Strauss, Trudie and von Maltitz, 2017). Second, Ward's linkage has shown to be robust when there is noise between clusters when compared to other linkage methods, such as *single linkage* (Balcan & Gupta, 2010).

Visual inspection of the dendrogram seen below in figure 3, shows evidence for seven distinct groups. Whilst some groups were found to contain mostly physical, or physiological features (e.g. face, genetic makeup), others groups were found to contain technologies (e.g. mouse movements, sms messages). Some contained a range of different features, with no clear grouping apparent (e.g. facial expressions, driving style). Given some groupings didn't seem to be clear, a non-applicable group was included in the closed card sorting study so that participants were not forced to sort dissimilar or non-applicable cards together. Instead they could be placed miscellaneous cards in the non-applicable group. Although observing the contents of the groupings was in itself interesting, the main take way from the dendrogram was that seven groups were required for the follow up closed card sorting study.

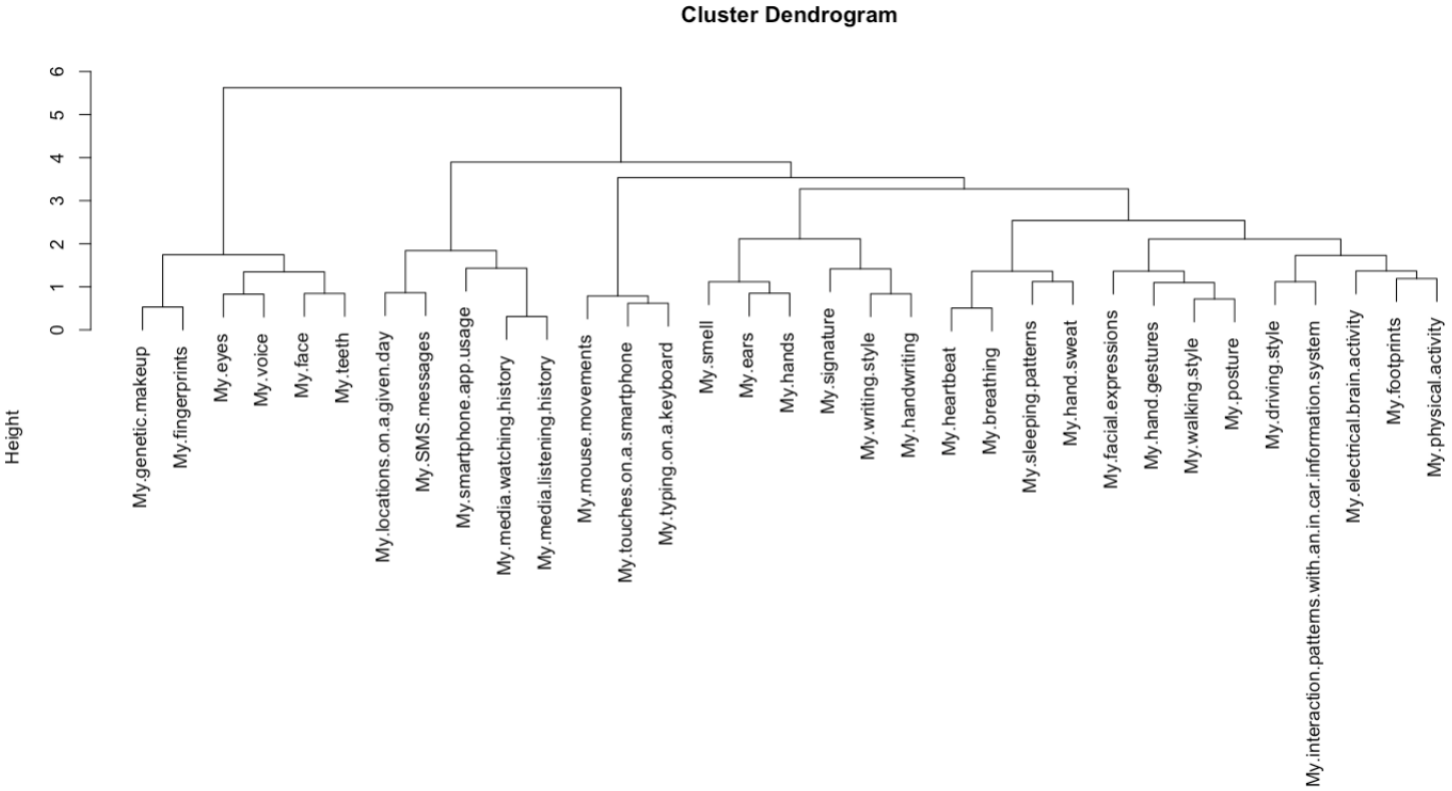


Figure 3. Dendrogram showing the output of wards hierarchical clustering method (Kruskal & Black, 2012)

Study Two: Closed Card Sorting

Descriptive. The frequencies of each card being placed in each category can be seen below in figure four. Several cards referring to the driving were found to be commonly placed in the not applicable category. These included 'my interactions with an in-car information system" and "my company in a vehicle". The cards that were placed most frequently in the "Very High Accuracy" category included 'my genetic makeup', "my fingerprints", and "my face". The cards that were placed most frequently in the "Low Accuracy" category included "my body temperature", "my interactions with an in-car navigation style", and "my driving style". Cards that were placed frequently in the "Moderate Accuracy" to "Low Accuracy" range included "my breathing", "my eye gaze pattern" and "my personality", and "my physical activity".

There seemed to be very little agreement regarding the accuracy of cards relating to digital media and technology (e.g my touches on a smartphone, my media watching history, my smartphone app usage'). These cards can be seen to have more uniform distributions, in that participants placed them in each of the seven categories with fairly equal frequency. Conversely, there was more agreement for cards relating to physiological features (e.g. my genetic makeup, my fingerprints). These cards have more skewed distributions, with participants more frequently placing them in the high accuracy or low accuracy categories. All code for the open and closed card sorting studies can be found in Appendix B.

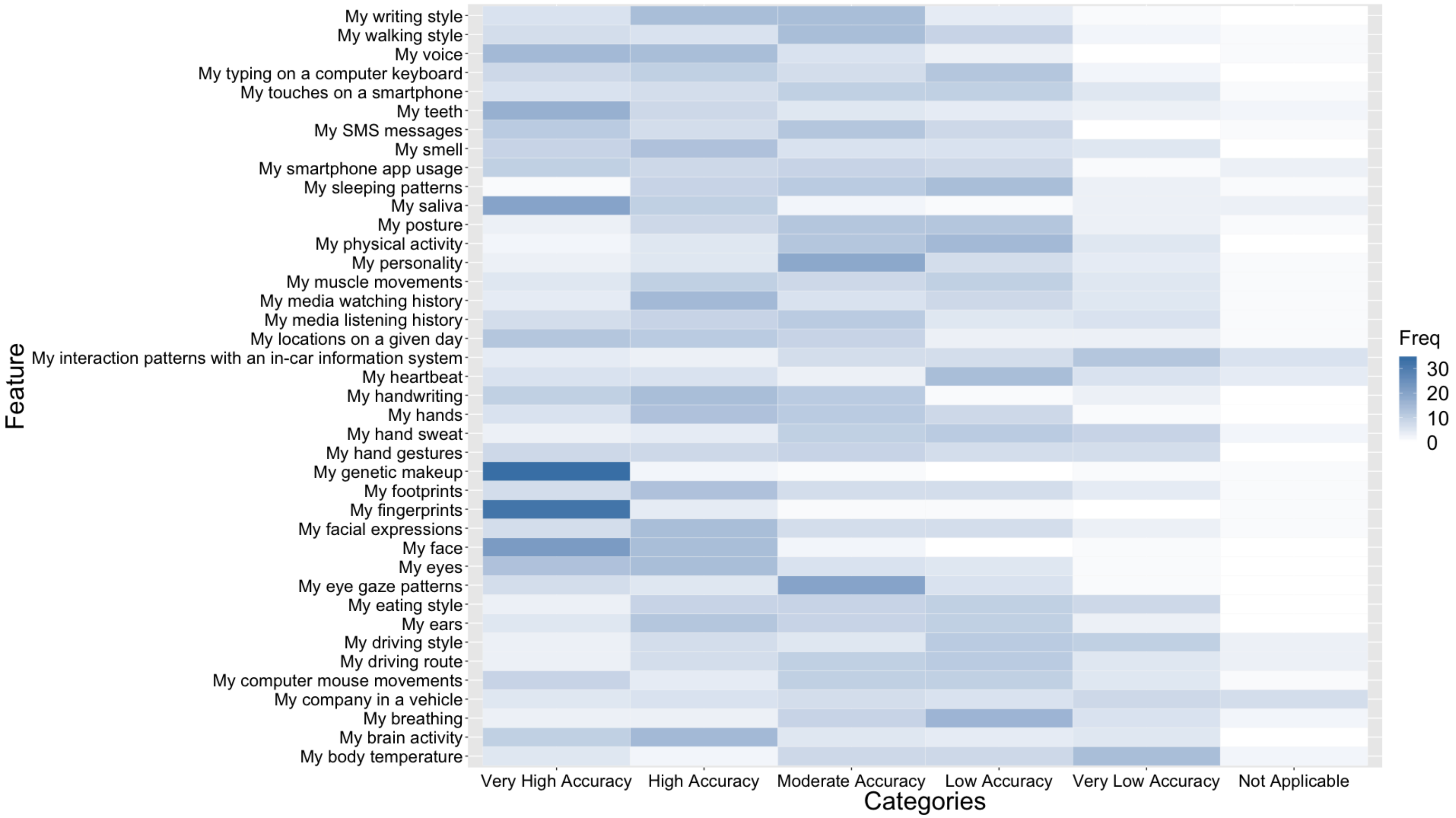


Figure 4. Heat map showing the frequency of each card being placed in each category. White represents low sharing frequency, light blue represents moderate sharing frequency, and dark blue represents high sharing frequency

Biometric Feature Selection. For study three (online decision task) eight features needed to be selected based of the results of study two. In order to maximise the chances of finding a meaningful difference in sharing behaviour across low and high accuracy groups, it was decided the best course of action was to select the extremes of each respective group. In other words, four cards were selected from the high accuracy (*high concern*) group, and four from the low accuracy (*low concern*) group. Cards were selected on the basis of having a relatively high frequency count (i.e. a large number of participants placed the card in that category), and how appropriate they are to the automotive domain.

Cards that had more uniform distributions (i.e. less agreement on accuracy amongst participants), and related to automobiles were excluded. It was decided that including automobile related features may have excluded some participants who don't drive, and thus can't relate to the idea of sharing personal automotive data. Taking the above qualifications into consideration resulted in body temperature, hand sweat, full muscle movements, and heart rate being selected as low accuracy (*low concern*) features for the decision task in study three. Furthermore, fingerprints, facial features, eye features, and brain wave patterns were selected as high accuracy (*high concern*) features. Henceforth, low and high accuracy features will be exclusively referred to as *low* and *high* concern features.

Study Three: Online Decision Task

Descriptive. Frequency of sharing across different biometric features, and benefits can be seen below in figure five. The most shared feature for the benefit of authentication was fingerprints, and for alertness monitoring it was heart rate. The least shared feature for authentication was brain wave patterns, and for alertness monitoring, it was fingerprints. For the benefit of authentication, all four *low concern* features were shared more often than all four *high concern* features. This was not the case for authentication, with no clear distinction in sharing frequency observable between *low* and *high* concern features. With the exception of fingerprints, every feature was shared more frequently for the benefit of alertness monitoring than authentication.

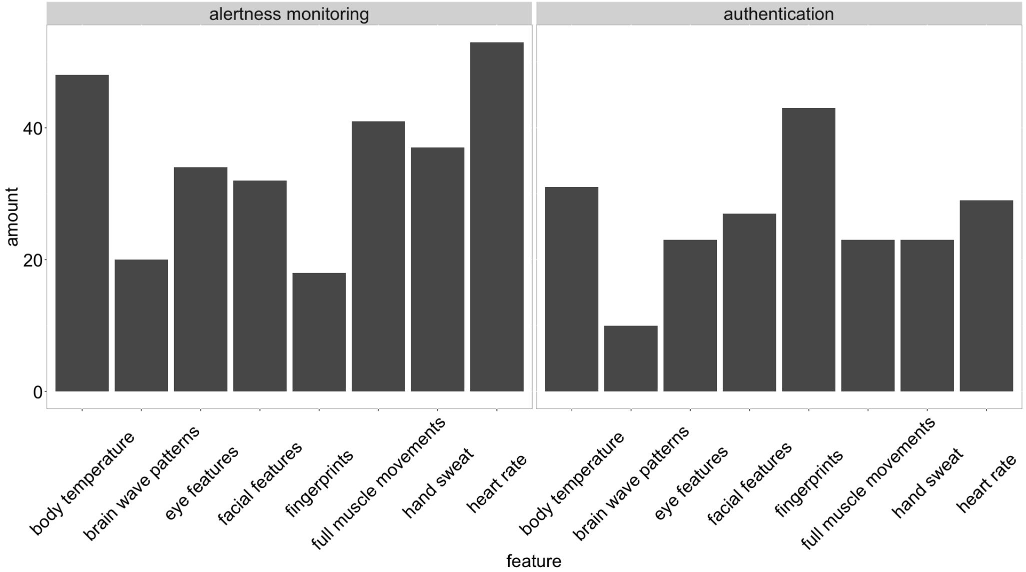


Figure 5. Sharing frequency of biometric feature type across benefit type

A similar figure to figure five can be seen below in figure six, except with sharing frequency aggregated across all low and high concern features. A clear distinction in sharing behaviour can be observed across low and high accuracy features for the benefit of alertness monitoring, with low concern features been shared more frequently. Sharing frequency for low and high concern features was found to be approximately equal for the benefit of authentication.

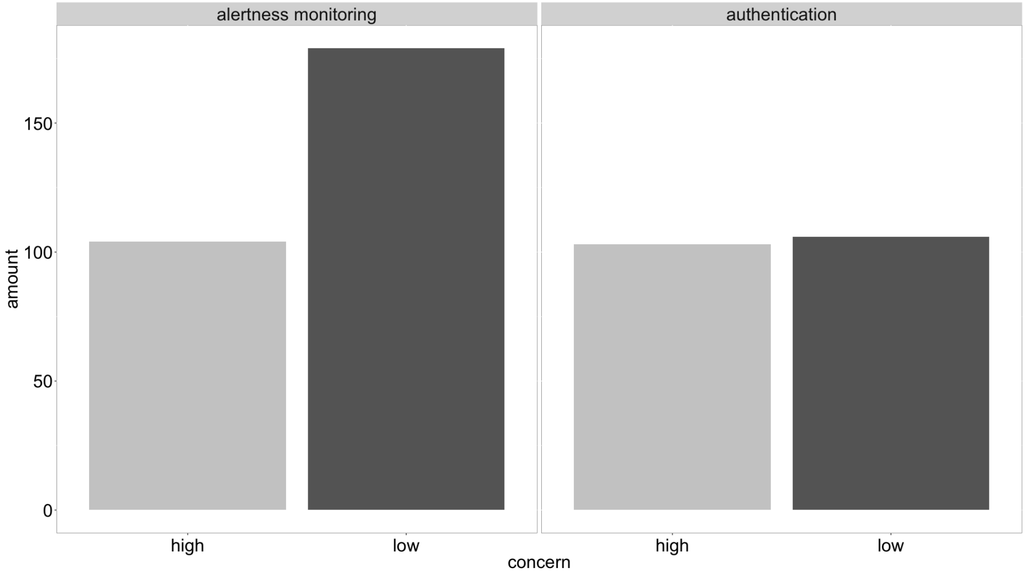


Figure 6. Sharing frequency of low and high concern features across benefit type. Sharing behavioural across low concern and high concern features were aggregated together

Inferential. To restate, the current study had one hypothesis, that *low concern* biometric features would be shared more often than *high concern* features irrespective of benefit type. A generalised mixed effect model was used to test this hypothesis. This model was selected for two reasons. First, every participant completed all sixteen trials, thus, a random effect was required in the model to account for the effect of participant. Second, sharing behaviour was a binary outcome (i.e share or not share), therefore a generalised model was also required. The final model therefore included two fixed parameters to represent the fixed effects of concern (i.e. high and low) and benefit type (i.e. authentication and alertness monitoring), as well as random effect to account for the effect of participant.

Results from the generalised mixed effect model can be seen below in Table 2. The first row in the table represents the reference variable for the model, the final row represents the interaction effect, and the remaining two represent the simple main effects. A significant interaction effect was found, whereby the effect of concern on sharing frequency depended on whether or not the benefit was *authentication* or *alertness monitoring.* Simple main effects revealed significant differences in sharing frequency between *low concern* and *high concern alertness monitoring*, but no significant difference in sharing frequency between *high concern alertness monitoring* and *high concern authentication.*

Table 2
Analysis of effect of concern and benefit type on sharing behaviour. With high concern sharing for alertness set as reference

Comparison	Est	SE	$ZValue$	$Pr(>\|z\|)$
HCAL (*intercept*)	-1.60	0.23	-7.06	1.62e-12
HCAL - LCAL (*comparison*)	1.21	0.18	6.65	2.90e-11
HCAU - HCAL (*comparison*)	-0.02	0.19	-0.12	0.91
LCAU (*interaction*)	-1.15	0.26	-4.41	1.02e-05

Note. HCAL = high concern alertness, LCAU = low concern authentication,
HCAU = high concern authentication, HCAL = high concern alertness

In order to obtain the two remaining simple main effects, the model was re-run with *low concern authentication* set as the reference point. The model output as can be seen below in Table 3, revealed no significant difference between *low* and *high* concern sharing for the benefit of *authentication*, but a significant difference in sharing frequency between *low concern authentication* and *low concern alertness monitoring.*

Table 3

Analysis of effect of concern and benefit type on sharing behaviour. With low concern sharing for authentication set as reference.

Trial type	Est	SE	$ZValue$	$Pr(>\|z\|)$
LCAU (*intercept*)	-1.60	0.23	-6.90	5.36e-12
HCAU - LCAU (*comparison*)	-0.06	0.18	-0.34	0.74
LCAL - LCAU (*comparison*)	1.17	0.18	6.44	1.17e-10
HCAL (*interaction*)	-1.15	0.26	-4.41	1.02e-05

Note. HCAL = high concern alertness, LCAU = low concern authentication, HCAU = high concern authentication, HCAL = high concern alertness

Several log-likelihood tests were conducted to access model-fit. A Log-likehood test revealed a model containing both parameters (i.e. benefit and concern) to have better model fit than a one-parameter model only including benefit; $\chi^2(1) = 22.9$, $p < 0.01$. A second log-likelihood ratio test further revealed that model fit was significantly better for the model including the interaction, compared to the model with only the fixed effects; $\chi^2(1) = 19.11$, $p < 0.01$. The R-code for all analyses from study three can be found in Appendices C and D.

Discussion

The aim of this study was two-fold. First, to investigate users' privacy concerns surrounding biometrics, and second, investigate if users' privacy concerns translate into congruent privacy behaviours in an automotive context. Two studies were conducted to investigate users' groupings of biometric features, and select four *low concern*, and four *high concern* biometric features. These features were then used to build a online forced choice task, in which respondents chose to either share or not share their biometric data in exchange for two different benefits, authentication, and alertness monitoring.

How does users' group biometrics based upon privacy concerns?

Given the exploratory nature of research question, no specific hypotheses were formed prior to the open and closed card sorting studies. Their collective primary aims was to select biometric features that participants perceived to either be of low or high accuracy. In other words, *low* and *high* concern biometric features. Several results from the open card sorting task are noteworthy. First, although the groupings were not extremely well defined, in the open card sorting study participants were found to group often by pre-existing biometric types (e.g. physiological, behavioural). This is interesting, because it potentially reveals that participants are already referring to pre-existing categories when evaluating each features' potential accuracy and their personal privacy concerns. In other words, it provides some insight into the thought processes of participants when evaluating how concerned they are about a biometric feature.

Second, it is also interesting that there seemed to be some overlap with the results from (Merrill et al., 2019). Similar to Merrill et al. (2019), brain wave patterns, facial expressions, and eye movements were found to relatively *high concern*, whilst other features such as 'skin conductance' were also found to be relatively *high concern.* Unlike Merrill et al. (2019) heart rate was found to be assigned a relatively higher level of concern. This difference could be potentially explained by the differences in the instructions used. Asking participants to rank by "how well the feature can identify their thoughts and emotion"' as oppose to by "how well you can be identified". Perhaps heart rate has a more emotional connotation, so priming participants to think about emotions may have elicited a relatively higher level of privacy concern. Although Merrill et al. (2019) is the closest comparison to the current study, one should however be weary however of directly comparing the results of this study with Merrill et al. (2019), given the difference in instructions, list of biometric features and nature of the respective tasks.

There are also some additional methodological considerations which need to be taken into account for both studies one and two. During the open card sorting study some participants reported that they had forgotten the instructions when sorting the cards by level of accuracy, and instead, they had begun to sort by type. Furthermore, for some cards there was some confusion as to what the biometric feature entailed. For example, some participants were unsure what cards like "sms messages" were referring to. For example, when participants were asked during the task, some reported they were thinking about the actual text messages, and others reported they were thinking about just their contacts. Some participants also mentioned they were thinking about computer identification (e.g. machine learning algorithm), whilst others were thinking about human identification (e.g. friends).

Steps were taken for the closed card sorting study to address each of these concerns. However, unlike the open card sorting study, there was no way of interviewing participants to see how well they followed, or were conscious of, the instructions during the task. This is worth keeping in mind, given the features for the decision task were selected based upon the results of the open card sorting study. Perhaps the features selected for the decision task were not really valid representations of *low* and *high* concern biometric data. Future work should look to include an explicit measure in open card sorting context which validates that participants were indeed following instructions. For example, by asking participants after completing the task questions like *"how were you grouping the cards by accuracy, or type?"*.

Do users' share low concern data more often?

Unlike the open and closed cards sorting studies, a specific hypothesis was formed the decision task. It was predicted that participants would share all *low concern* data more often than *high concern* data irrespective of benefit type. With every *low concern* and *high concern*feature aggregated into their respective groups, a significant concern by benefit type interaction was found, where by the effect of concern on sharing behaviour was found to depend on the benefit type. Thus, the sole hypothesis for the decision task study was not supported.

It is difficult to directly compare this finding to past research for several reasons. First, no other work has specifically looked to investigate if *privacy concerns* translate into congruent *privacy behaviours* in the automotive domain. Given privacy is highly contextual phenomena, comparing this studies findings to other results found in other domains is somewhat futile. Second, research which has often looked to link privacy concerns to privacy behaviours have often utilised very different methodologies. Often, either questionnaires and self report measures for privacy concerns and privacy behaviours, or contrived experiments which do not emulate real world sharing decision making (Kokolakis, 2017).

Taking these considerations into mind, it is worth noting that past research has found benefit type to influence the relationship between *privacy concerns* and *privacy behaviours.* In a study conducted by Lee et al. (2013), participants reported during semi-structured interviews that despite having privacy concerns users' may actually share their *high concern* data if the benefit is substantial enough. In the case of the current study, perhaps for *authentication* trials the benefit was substantial enough for participants to equally share their *low concern* and *high concern* data. In other words, the benefit of sharing always outweighed the cost, even if participants had more privacy concerns about certain biometrics.

Why is it then that differences were found between *low* and *high* concern biometrics for alertness monitoring trials? Lee et al. (2013) offers an potential explanation, by stating that users' adapt their own sharing strategies in such a way that maximises expect benefit. Participants may not have seen the benefit of sharing certain *high concern* biometric features (e.g. fingerprints, eye features) for alertness monitoring purposes, because intuitively they are not really the sort of features one would expect to need to track a drivers alertness. However, some of *low concern* features (e.g. body temperature, heart rate) may have seemed far more appropriate for the purposes of alertness monitoring. In other words, the benefit of sharing the *low* and *high* concern biometrics for *alertness monitoring* may have differed. By comparison, the benefit of sharing *low* and *high* concern biometrics for *authentication* may have not differed, as research validates each biometric being used for *authentication* purposes (Villa et al., 2018).

It is also worth noting again that comparing sharing behaviour across *low* and *high* concern biometrics assumes that the labels derived from the closed and open card sorting studies are valid. Given the aforementioned considerations mentioned in the previous sections, it is difficult to evaluates the degree to which the selected features are truly representative of *low* and *high* privacy concern features. Perhaps if 'valid' *low* and *high* privacy concern were selected, significant differences between the two would have been found across both authentication and alertness monitoring. However, this purely speculative, no research has investigated privacy concerns and privacy behaviours in a automotive context.

Implications

The findings from this study have several practical implications. First, the current study's findings emphasise the need and rationale for users to be put in control of their automotive data. This study has shown that participants decision to share their data depends on the benefit type, and the type of biometric. Furthermore, sometimes there is a paradox, where by even if participants state their are concerned about a piece of data, their sharing behaviour might actually be different. Therefore it is not enough for car manufactures to set blanket privacy policies for all data sharing that rely on simple surveys of driver attitudes. If the right to privacy is to be maintained, there is clearly a need for drivers to be able to specifically choose the types of data they want to share, and the types they do not.

Second, this studies findings can aid in educating the general public about the preferences of other people when it comes to privacy. Research has shown that if people are informed of the preferences of users', they are more likely to read privacy policies(Malgieri & Custers, 2018). For example, car manufacturers could start presenting drivers with information about other drivers preferences. Furthermore, educating drivers that sometimes their *privacy behaviours* do not match their *privacy concerns*, may in turn enable them to make decisions that better reflect their *privacy concerns.* Finally, the study presents findings which are an important first step to placing a literal monetary value on privacy. As outlined by Malgieri and Custers (2018), individuals do not seem to be fully aware of the monetary value of their personal data. Somewhat ironically, by looking to avoid measuring value in monetary terms, this study's results can aid in developing pricing mechanisms which reflect actual user preferences.

Limitations

This study had several general limitations that are worth noting. First, actual user data was not collected. Rather, participants were tasked with imagining hypothetical situations in which they would be sharing their own data with a car manufacturer. Although work has validated the use of survey based behavioural approaches in approximating real world decision making (Hainmueller et al., 2015) it is possible that participants may have acted differently if they had their own biometric data collected and asked whether or not they would share it. Furthermore, it is possible most participants have little to no experience with biometric technology in cars, let alone biometrics in general. Therefore the experiment may have come across as somewhat contrived, something which again could have been solved if actual biometric participant data was collected.

Second, the sample that was used to select *low* and *high* concern biometric features in the card sorting task was a different sample to the one that completed the decision task. Although data from both studies was collected via similar means (i.e. crowd sourcing online), privacy concerns have been found to vary amongst different individuals (Kokolakis, 2017). Perhaps the sample for the card sorting task had different privacy concerns than the decision task sample. Ideally, the same participants would have participated in all three studies to control for individual differences in privacy concerns.

Future work

Future work should look to build upon this study in several ways. First, by collecting actual user data, rather than asking participants to respond to hypothetical situations. This could be achieved by using collecting actual user biometric data, and then asking participants if they would be willing to sell their data. For example fingerprint data could be collected on a daily basis, and then participants could be prompted via a mobile phone application to sell their data. Second, different benefit types should be explored to see their effect on sharing. This study only included authentication and alertness monitoring, where in fact their are many other potential benefits of biometrics in automobiles, such as detecting medical emergencies, personalised features (e.g. automatic seat and mirror adjustments), and using gestures to control vehicle functions (e.g. turning up stereo using hand gesture) (Villa et al., 2018)). Lastly, future work should look to investigate the relationship between *privacy concerns* and *privacy behaviours* in an automotive context, using a wider range of biometric features. For example, only *low* and *high concern* biometric features were selected for the decision task. Although one would expect a linear relationship where by sharing frequency decreases as concerns increase, it would be interesting to explore how users share neutral or "medium concern" features.

Conclusion

In adopting an survey based behavioural design, this study is the first to explore the relationship between biometric privacy concerns and sharing behaviours of biometrics in an automotive context. Given biometrics are predicted to become increasingly popular in an automotive context, understanding how users' share automotive biometric data, and their reasons for sharing or not sharing, is an necessary and important first step to ensuring that user' privacy is maintained. Without such, it is difficult to shape policy that maintains privacy, whilst optimising user experiences. Importantly, the results from this paper reveal the complexity and context dependent nature of sharing behaviours in an automotive context, and the need for future work to explore new benefit types, and biometric data sharing in a real world context.

References

Akrout, B., & Mahdi, W. (2017). Yawning detection by the analysis of variational descriptor for monitoring driver drowsiness. *IPAS 2016 - 2nd International Image Processing, Applications and Systems Conference*, 1–5. doi: 10.1109/IPAS.2016.7880127

Alsaadi, I. (2015). Physiological Biometric Authentication Systems Advantages Disadvantages And Future Development A Review. *International Journal of Scientific & Technology Research*, *4*(8), 285–289.

Balcan, M. F., & Gupta, P. (2010). Robust hierarchical clustering. *COLT 2010 - The 23rd Conference on Learning Theory*, *15*, 282–294.

Bauer, C., Korunovska, J., & Spiekermann, S. (2012). On the value of information-what Facebook users are willing to pay. *ECIS 2012 - Proceedings of the 20th European Conference on Information Systems.*

Buck, C., Stadler, F., Suckau, K., & Eymann, T. (2017). Privacy as a Part of the Preference Structure of Users App Buying Decision. *Proceedings der 13. Internationale Tagung Wirtschaftsinformatik (WI)*, *13*(Feburary), 792–806. Retrieved from `http://www.wi2017.ch/de/proceedings`

De Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, *3*. doi: 10.1038/srep01376

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. doi: 10.1287/isre.1060.0080

Enev, M., Takakuwa, A., Koscher, K., & Kohno, T. (2015). Automobile Driver Fingerprinting. *Proceedings on Privacy Enhancing Technologies*, *2016*(1), 34–50. doi: 10.1515/popets-2015-0029

Grande, D., Asch, D. A., Wan, F., Bradbury, A. R., Jagsi, R., & Mitra, N. (2015). Are Patients With Cancer Less Willing to Share Their Health Information? Privacy, Sensitivity, and Social Purpose. *Journal of Oncology Practice*, *11*(5), 378–383. doi: 10.1200/jop.2015.004820

Hainmueller, J., Hangartner, D., & Yamamoto, T. (2015). Validating vignette and conjoint survey experiments against real-world behavior. *Proceedings of the National Academy of Sciences of the United States of America*, *112*(8), 2395–2400. doi: 10.1073/pnas.1416587112

Hartanto, S., Sugiharto, A., & Nur Endah, S. (1999). Optical character recognition Algoritma Template Matching Correlation. , *5*, 1–12.

Harvey, C. (2011). Modelling and evaluating drivers' interactions with in-vehicle information systems (IVIS).

Hirschprung, R., Toch, E., Bolton, F., & Maimon, O. (2016). A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior*, *61*, 443–453. Retrieved from `http://dx.doi.org/10.1016/j.chb.2016.03.033` doi: 10.1016/j.chb.2016.03.033

Hosio, S., Ferreira, D., Goncalves, J., Van Berkel, N., Luo, C., Ahmed, M., ... Kostakos, V. (2016). Monetary assessment of battery life on smartphones. *Conference on Human Factors in Computing Systems - Proceedings*, 1869–1880. doi: 10.1145/2858036.2858285

Hu, D., Sun, F., Tu, L., & Huang, B. (2013). We know what you are - A user classification based on mobile data. In *Proceedings - 2013 ieee international conference on green computing and communications and ieee internet of things and ieee cyber, physical and social computing, greencom-ithings-cpscom 2013* (pp. 1282–1289). doi: 10.1109/GreenCom-iThings-CPSCom.2013.223

Inbavalli, P., & Nandhini, G. (2014). Body Odor as a Biometric Authentication. , *5*(5), 6270–6274.

Katsanos, C., Avouris, N., Stamelos, I., Tselios, N., Demetriadis, S., & Angelis, L. (2019). Cross-study Reliability of the Open Card Sorting Method. *Conference on Human Factors in Computing Systems - Proceedings*, 1–6. doi: 10.1145/3290607.3312999

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, *64*, 122–134. doi: 10.1016/j.cose.2015.07.002

Kruskal, J. B., & Black, P. (2012). A Run Length Transformation for Discriminating Between Auto Regressive Time Series. *Journal of Classification*, *6*(June 2011), 4–6. doi: 10.1007/s00357

Kumar, R. (2016, dec). Teeth recognition for person identification. In *2016 international conference on computation system and information technology for sustainable solutions, csitss 2016* (pp. 13–16). Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/CSITSS.2016.7779432

Längkvist, M., Karlsson, L., & Loutfi, A. (2012). Sleep Stage Classification Using Unsupervised Feature Learning. *Advances in Artificial Neural Systems*, *2012*, 1–9. doi: 10.1155/2012/107046

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on social network services? a qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human Computer Studies*, *71*(9), 862–877. Retrieved from `http://dx.doi.org/10.1016/j.ijhcs.2013.01.005` doi: 10.1016/j.ijhcs.2013.01.005

Lim, S., Woo, J. R., Lee, J., & Huh, S. Y. (2018). Consumer valuation of personal information in the age of big data. *Journal of the Association for Information Science and Technology*, *69*(1), 60–71. doi: 10.1002/asi.23915

Liu, M., Fan, D., Zhang, X., & Gong, X. (2017, jan). Human Emotion Recognition Based on Galvanic Skin Response Signal Feature Selection and SVM. In *Proceedings - 2016 international conference on smart city and systems engineering, icscse 2016* (pp. 157–160). Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/ICSCSE.2016.0051

Lozoya-Santos, J. d. J., Sepúlveda-Arróniz, V., Tudon-Martinez, J. C., & Ramirez-Mendoza, R. A. (2019). Survey on biometry for cognitive automotive systems. *Cognitive Systems Research*, *55*, 175–191. doi: 10.1016/j.cogsys.2019.01.007

Lu, Y., Wei, Y., Liu, L., Zhong, J., Sun, L., & Liu, Y. (2017, apr). Towards unsupervised physical activity recognition using smartphone accelerometers. *Multimedia Tools and Applications*, *76*(8), 10701–10719. doi: 10.1007/s11042-015-3188-y

Malgieri, G., & Custers, B. (2018). Pricing privacy – the right to know the value of your personal data. *Computer Law and Security Review*, *34*(2), 289–303. Retrieved from `https://doi.org/10.1016/j.clsr.2017.08.006` doi: 10.1016/j.clsr.2017.08.006

Martin, K. (2013). (the Data Collection Actor, E.G. the Application Developer or Mobile Phone Provider),. *TPRC41 Research Conference on Communication, Information and Internet Se-*

curity September 27-29, 1–27.

Merrill, N., Chuang, J., Cheshire, C., & Holgate, S. A. (2019). Sensing is Believing: What People Think Biosensors Can Reveal About Thoughts and Feelings. *Proceedings of the 2019 on Designing Interactive Systems Conference*, *159*(2147), 413–420. Retrieved from `http://doi.acm.org/10.1145/3322276.3322286%0Ahttp://dx.doi.org/10.475/123_4` doi: 10.1145/3322276.3322286

Nawrath, T., Fischer, D., & Markscheffel, B. (2017). Privacy-sensitive data in connected cars. *2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016*, 392–393. doi: 10.1109/ICITST.2016.7856736

Nazmi, N., Abdul Rahman, M., Yamamoto, S.-I., Ahmad, S., Zamzuri, H., & Mazlan, S. (2016, aug). A Review of Classification Techniques of EMG Signals during Isotonic and Isometric Contractions. *Sensors*, *16*(8), 1304. Retrieved from `http://www.mdpi.com/1424-8220/16/8/1304` doi: 10.3390/s16081304

Nget, R., Cao, Y., & Yoshikawa, M. (2017). How to balance privacy and money through pricing mechanism in personal data market. *CEUR Workshop Proceedings*, *2311*.

Niu, J., Cai, M., Shi, Y., Ren, S., Xu, W., Gao, W., . . . Reinhardt, J. M. (2019, dec). A Novel Method for Automatic Identification of Breathing State. *Scientific Reports*, *9*(1). doi: 10.1038/s41598-018-36454-5

Obaidat, M. S., Traore, I., & Woungang, I. (2018). *Biometric- Based Physical and Cybersecurity Systems.*

Panwar, M., & Singh Mehra, P. (2011). Hand gesture recognition for human computer interaction. In *Iciip 2011 - proceedings: 2011 international conference on image information processing.* doi: 10.1109/ICIIP.2011.6108940

Patel, P., Bhatt, B., & Patel, B. (2017, jul). Human body posture recognition - A survey. In *Ieee international conference on innovative mechanisms for industry applications, icimia 2017 - proceedings* (pp. 473–477). Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/ICIMIA.2017.7975660

Perentis, C., Vescovi, M., Leonardi, C., Moiso, C., Musolesi, M., Pianesi, F., & Lepri, B. (2017). Anonymous or not? Understanding the factors affecting personal mobile data disclosure. *ACM Transactions on Internet Technology*, *17*(2). doi: 10.1145/3017431

Ragan, E. J., Johnson, C., Milton, J. N., & Gill, C. J. (2016). Ear biometrics for patient identification in global health: a cross-sectional study to test the feasibility of a simplified algorithm. *BMC Research Notes*, *9*(1), 1–12. doi: 10.1186/s13104-016-2287-9

Rathore, R., & Gau, C. (2014). Integrating biometric sensors into automotive Internet of Things. *Proceedings of 2014 International Conference on Cloud Computing and Internet of Things, CCIOT 2014*(Cctot), 178–181. doi: 10.1109/CCIOT.2014.7062532

Shih, F., Liccardi, I., & J.weitzner, D. (2015). Privacy tipping points in smartphones privacy preferences. *Conference on Human Factors in Computing Systems - Proceedings*, *2015-April*, 807–816. doi: 10.1145/2702123.2702404

Soley, A. M., Siegel, J. E., Suo, D., & Sarma, S. E. (2018). Value in vehicles: economic assessment of automotive data. *Digital Policy, Regulation and Governance*, *20*(6), 513–527. doi: 10.1108/DPRG-05-2018-0025

Spangler, W. E., Gal-Or, M., & May, J. H. (2003, dec). *Using data mining to profile TV viewers* (Vol. 46) (No. 12). doi: 10.1145/953460.953461

Staiano, J., Oliver, N., Lepri, B., De Oliveira, R., Caraviello, M., & Sebe, N. (2014). Money walks: A human-centric study on the economics of personal mobile data. *UbiComp 2014 - Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 583–594. doi: 10.1145/2632048.2632074

Strauss, Trudie and von Maltitz, M. J. (2017). Generalising Ward's method for use with Manhattan distances. *PloS one*, *12*.

Tan, D., & Nijholt, A. (2010). Brain-Computer Interfaces and Human-Computer Interaction. In (pp. 3–19). doi: 10.1007/978-1-84996-272-8$_1$

Tu, Z., Li, R., Li, Y., Wang, G., Wu, D., Hui, P., ... Jin, D. (2018, sep). Your Apps Give You Away. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(3), 1–23. doi: 10.1145/3264948

Van Ly, M., Martin, S., & Trivedi, M. M. (2013). Driver classification and driving style recognition using inertial sensors. In *Ieee intelligent vehicles symposium, proceedings* (pp. 1040–1045). doi: 10.1109/IVS.2013.6629603

Villa, M., Gofman, M., & Mitra, S. (2018). Survey of Biometric Techniques for Automotive Applications. *Advances in Intelligent Systems and Computing*, *738*, 475–481. doi: 10.1007/978-3-319-77028-4$_6$2

Yang, Y. H., Lin, Y. C., & Chen, H. (2009). Personalized music emotion recognition. In *Proceedings - 32nd annual international acm sigir conference on research and development in information retrieval, sigir 2009* (pp. 748–749). doi: 10.1145/1571941.1572109

Zhang, L., Tan, S., & Yang, J. (2017). Hearing Your Voice is Not Enough: An Articulatory gesture based liveness detection for voice authentication. *Proceedings of the ACM Conference on Computer and Communications Security*, 57–71. doi: 10.1145/3133956.3133962

Appendix A
Open card Sorting Materials

Participant information form

Dear Participant,

Before the research begins, it is important that you are aware of the procedure that is followed in this study. Please read the text below carefully and do not hesitate to ask for clarification on this text, if it is not clear please ask the researcher before beginning.

Purpose of the study

Biometric technologies generally refer to the use of technology to identify a person based on some aspect of their physiology (e.g. DNA) or behaviour (e.g. writing style). During this experiment we are interested in getting an understanding of how people sort different biometric technologies into groups. An understanding of how people sort biometric technologies is an important first step into understanding peoples attitudes towards sharing their own biometric data.

Explanation of task

Each card has different feature (i.e. type of biometric) written on it. Please **group** the cards into distinct sets by **how accurately** someone can identify you using only these feature stated on a card. You can have as many groups as you like. We also ask you to **label each group** that you have created. The experiment is expected to take around **30 minutes in total**.

Experimental Procedure

1. Read information form (this sheet), and fill in the consent form
2. Fill in the subject information sheet (e.g. age, gender)
3. Watch a demonstration of the card sorting task
4. Complete the card sorting task

Freedom to withdraw

If you decide not to participate in this study, this will in no way affect you. If you gradually decide to stop the research, you can do so at any time without giving reasons and without any consequences for you in any way.

Your privacy is guaranteed

Your personal information (who you are) remains confidential and will not be shared without your explicit consent. Your research data are further analyzed by the researchers who collected the data. Research data published in scientific journals are anonymous and cannot be traced back to you. Fully anonymized research data may also be shared with other researchers.

Further information

If you have questions about this research, in advance or afterwards, you can contact the responsible researcher; Liam Ashby (Liam.Ashby@cwi.nl).

Sincerely,
Liam Ashby

Informed Consent Form

I hereby declare that I volunteer to participate in the biometric open card sorting collection experiment conducted by Distributed and Interactive (DIS) group, *Centrum Wiskunde & Informatica (CWI)*.

1. I understand that this experiment is held to collect data on how people group different biometric technologies.
2. I understand that my participation is completely voluntary, and I may discontinue my participation at any time without negative consequences.
3. I understand that the researchers have to ask questions. However, if I feel uncomfortable answering the questions, I have the right to decline or pass the question.
4. I understand that the data breaches and security incidents are minimized in the infrastructure via one or more of the following technical measures: a) specific OS users, b) protected databases, c) secured VPN if access is required outside CWI, d) no transmission and sharing of data.

The following table summarizes the basic information on personal data protection:

Controller	**Name**: Liam Ashby, Distributed and Interactive (DIS) group, Centrum Wiskunde & Informatica (CWI) **Address:** Science Park 123, 1098 XG Amsterdam, the NETHERLANDS **Telephone:** 068 548 1773. **Data Protection Office email:** Liam.Ashby@cwi.nl
Purpose	Your personal data will only be used for the purposes specified on the forms, which you have provided your personal data.
Legitimation	The legal basis for the processing of personal data is your voluntarily consent.
Storage period	Your data will be stored during the life of project (until July 01st, 2022) + 5 years for auditing purposes. When it will be no longer necessary to keep your data, they will be removed with adequate security measures. Your personal data will not be shared with any third parties, except for legal obligations.
Rights	You have the rights of transparency, information, access, rectification, deletion, portability, limitation and opposition to the treatment of your personal data. To exercise any of these rights, data subjects shall send us an email to Liam.Ashby@cwi.nl, including a copy of a valid proof of identity.

"I have both read and understood the information written on this form and hereby give permission to participate in the research and allow the use of the resulting data. I reserve the right to withdraw this permission without giving any reason. I also preserve the right to stop the experiment at any time."

Thus, signed in duplicate:
Date:

....

Participant Name **Signature**

My face	My hands
My genetic makeup	My smell
My ears	My signature
My eyes	My touches on a smartphone (e.g., movement, pressure, etc.)
My fingerprints	My mouse movements
My walking style	My typing on a keyboard
My voice	My locations on a given day
My teeth	My smartphone app usage
My footprints	My sleeping patterns
My heartbeat	My physical activity
My writing style	My hand sweat
My posture	My media watching history (e.g. channels, movies, etc.)

My handwriting	My SMS messages
My driving style	My media listening history (e.g. songs, podcasts)
My hand gestures	My interaction patterns with an in-car information system (e.g. GPS, volume control, media player)
My electrical brain activity	My facial expressions
My breathing	My eye gaze patterns
My handwriting	My SMS messages

Appendix B

Study one and two: card sorting analyses

```
#################### Open Card Sorting ##################

#Loading in libraries
library(tidyverse)

#Defining functions
compare <- function(x1, x2) {
  x3 <- x1 + x2
  ints <- sum(x3 > 1)
  uno <- sum(x3 > 0)
  return (ints / uno)
}

getJaccard <- function(data) {
  l = length(data[1,])
  jmatrix <- matrix(nrow=l,ncol=l)
  for (i in 1:l) {
    for (j in i:l) {
      s <- compare(data[i], data[,j])
      jmatrix[i,j] <- s
      jmatrix[j,i] <- s
    }
  }
  return (jmatrix)
}

cardsort <- function(filename, blocks) {
  filedata <- read.table(filename, header = T, sep=",")
  data <- getJaccard(filedata)
  colnames(data) <- colnames(filedata)
  hc <- hclust(dist(t(data)), method="ward.D")
  hc$labels <- colnames(data)
  plot(hc)
  rect.hclust(hc, k=blocks, border="black")
}

#Figure 3 (Dendrogram)
cardsort("/Users/liamashby/Dropbox/Masters/Thesis/Card sorting/Open/Data/data.csv")

#################### Closed Card Sorting ##################

#Loading in libraries
library("RColorBrewer")
library(tidyverse)

if (!require(reshape2) | !require(jsonlite)){
  install.packages('reshape2')
  install.packages('jsonlite')
  library(reshape2)
  library(jsonlite)
}


# Unpacking json data
j_obj_list = NULL
for (j in 1:NROW(df)) {

  if (df[j,2] == '') next
  j_obj_list = rbind(j_obj_list, jsonlite::fromJSON(as.character(df[j,2])))
}

j_lists = NULL
for (k in 1:NROW(j_obj_list)) {

  j_lists = rbind(j_lists, j_obj_list[k,]$categories$topics)
}


## Creating clean df
j_lists_sub = NULL
for (i in 1:NROW(j_lists)) {

  if (is.null(colnames(j_lists[[i,1]]))) next
  for (k in 1:NROW(j_lists[i,])) {

    if(is.data.frame(j_lists[[i,k]]) && nrow(j_lists[[i,k]])==0) next
    j_lists_sub = rbind(j_lists_sub, cbind(i, k, j_lists[[i,k]]))
  }
}


cl_card_df = NULL
for (i in 1:NROW(j_lists_sub)) {
  if (NROW(j_lists_sub[j_lists_sub$i == i,]) == 40) {
    cl_card_df = rbind(cl_card_df, j_lists_sub[j_lists_sub$i == i,])
  }
}
cl_card_df = as.data.frame(cl_card_df)


# Figure 4 (Heat Map)

## frequency by category (1-strong accuracy; 6-n/a)
table(cl_card_df$k,cl_card_df$title)

## transpose for easier view of distribution. TODO: create heatmap / bar plot of table
feat_dist = t(table(cl_card_df$k,
                    cl_card_df$title))

input <- as.data.frame(feat_dist) %>%
  rename('Feature'= 'Var1') %>%
  rename('Level' = 'Var2') %>%
  mutate('Categories' = ifelse(Level == 1, "Very High Accuracy",
                               ifelse(Level == 2, 'High Accuracy',
                                      ifelse(Level == 3,
                                             'Moderate Accuracy',
                                             ifelse(Level == 4, 'Low Accuracy',
                                                    ifelse(Level == 5,
                                                           'Very Low Accuracy',
                                                           'Not Applicable'))))))

ggplot(input, aes(Categories, Feature)) +
  geom_tile(aes(fill = Freq), colour = "white") +
  scale_fill_gradient(low = "white", high = "steelblue") +
  scale_x_discrete(limits=c('Very High Accuracy', 'High Accuracy', 'Moderate Accuracy',
                            'Low Accuracy', 'Very Low Accuracy', "Not Applicable")) +
  theme(axis.text.x  = element_text(angle = 0, vjust = 0.5, size = 17, colour = "black"),
        axis.text.y = element_text(vjust = 0.5, size = 17, colour = "black"),
        axis.title.x = element_text(color = "black", size = 25),
        axis.title.y = element_text(color = "black", size = 25),
        legend.title=element_text(size=20),
        legend.text=element_text(size=20))
```

Appendix C

Study three: exploratory analyses

```
#Loading libriaries
library(RSQLite)
library(tidyverse)
library(jtools)
```

```
#Loading in data
filename <- "biometric_database_191001.db"
sqlite.driver <- dbDriver("SQLite")
db <- dbConnect(sqlite.driver, dbname = filename)
dbListTables(db)

#Creating tables
responses <- dbGetQuery(db,"SELECT * FROM responses")
benefits <- dbGetQuery(db,"SELECT * FROM benefits")
features <- dbGetQuery(db,"SELECT * FROM features")
user_sessions <- dbGetQuery(db,"SELECT * FROM user_sessions")

#Joining tables
data <- responses %>%
  left_join(features, c('feature_id' = 'id')) %>%
  left_join(user_sessions, c('user_session_id' = 'id')) %>%
  left_join(benefits, c('benefit_id' = 'id')) %>%
  select(id, user_session_id, choice, name.x, complete,
         remote_address, name.y, first_benefit_id, demographics) %>%
  rename('feature' = name.x) %>%
  rename('benefit' = name.y) %>%
  mutate(accuracy = ifelse(feature == 'brain wave patterns', 'high',
                           ifelse(feature == "fingerprints", 'high',
                                  ifelse(feature == "eye features", "high",
                                         ifelse(feature == "facial features", "high", "low"
                                         )
                                  )
                           )
  )
  )



#Figure 5

frequency_choice_benefit <- data %>%
  filter(complete == 1) %>%
  select(choice, feature, benefit) %>%
  group_by(feature, choice, benefit) %>%
  tally() %>%
  rename('amount' = n) %>%
  filter(choice == 'share') %>%
  ungroup() %>%
  select(-choice)

ggplot(data = frequency_choice_benefit) +
  geom_col(aes(x = feature, y = amount)) +
  facet_wrap(~ benefit, nrow = 1,) +
  theme(axis.text.x  = element_text(angle = 45, vjust = 0.5, size = 25, colour = "black"),
        axis.title.x = element_text(color = "black", size = 25),
        axis.title.y = element_text(color = "black", size = 25),
        axis.text.y = element_text(vjust = 0.5, size = 25, colour = "black"),
        strip.text = element_text(size = 25),
        panel.background = element_rect(fill = "white", colour = "grey50"))

#Figure 6

frequency_accuracy <- data %>%
  filter(complete == 1) %>%
  mutate(concern = accuracy) %>%
  select(choice, benefit, concern) %>%
  group_by(choice, benefit, concern) %>%
  tally() %>%
  rename('amount' = n) %>%
  filter(choice == 'share') %>%
  ungroup() %>%
  select(-choice)


ggplot(data = frequency_accuracy) +
  geom_col(aes(x = concern, y = amount, fill = concern)) +
  facet_wrap(~ benefit, nrow = 1,) +
  theme(axis.text.x  = element_text(vjust = 0.5, size = 25, colour = "black"),
        axis.title.x = element_text(color = "black", size = 25),
        axis.title.y = element_text(color = "black", size = 25),
        axis.text.y = element_text(vjust = 0.5, size = 25, colour = "black"),
        panel.background = element_rect(fill = "white", colour = "grey50"),
        strip.text = element_text(size = 25),
        legend.position = "none") +
  scale_fill_grey(start = 0.8, end = 0.4)
```

Appendix D

Study three: generalised linear models

```
#Loading Libraries
library(RSQLite)
library(tidyverse)
library(lme4)
library(optimx)

#Loading in data
filename <- "biometric_database_191001.db"
sqlite.driver <- dbDriver("SQLite")
db <- dbConnect(sqlite.driver, dbname = filename)
dbListTables(db)

#Creating tables
responses <- dbGetQuery(db,"SELECT * FROM responses")
benefits <- dbGetQuery(db,"SELECT * FROM benefits")
features <- dbGetQuery(db,"SELECT * FROM features")
user_sessions <- dbGetQuery(db,"SELECT * FROM user_sessions")

#Joining tables
data <- responses %>%
  left_join(features, c('feature_id' = 'id')) %>%
  left_join(user_sessions, c('user_session_id' = 'id')) %>%
  left_join(benefits, c('benefit_id' = 'id')) %>%
  select(id, user_session_id, choice, name.x,
         complete, remote_address, name.y, first_benefit_id) %>%
  rename('feature' = name.x) %>%
  rename('benefit' = name.y) %>%
  mutate(accuracy = ifelse(feature == 'brain wave patterns', 'high',
                           ifelse(feature == "fingerprints", 'high',
                                  ifelse(feature == "eye features", "high",
                                         ifelse(feature == "facial features", "high", "low"
                                                )
                                         )
                                  )
                           )
         )

l

#Creating model data set

model_data <- data %>%
  filter(complete == 1) %>% #filtering for complete responses
  select(user_session_id, accuracy, feature, benefit, choice,) %>%
  mutate(benefit = as.factor(benefit)) %>%
  mutate(choice = as.factor(choice)) %>%
  mutate(feature = as.factor(feature)) %>%
  mutate(user_session_id = as.factor(user_session_id)) %>%
  mutate(accuracy = as.factor(accuracy))


#Table 1: Generalised linear model
```

```
glm_model <- glmer(choice ~ accuracy*benefit + (1|user_session_id),
                   family = binomial,
                   data = model_data,
                   control = lmerControl(optimizer ='optimx',
                                         optCtrl=list(method='L-BFGS-B')
                   )
)


#Table 2: Generalised linear model (with releveling)

model_data$accuracy <- relevel(model_data$accuracy, ref="low")
model_data$benefit <- relevel(model_data$benefit, ref="authentication")


glm_model <- glmer(choice ~ accuracy*benefit + (1|user_session_id),
                   family = binomial,
                   data = model_data,
                   control = lmerControl(optimizer ='optimx',
                                         optCtrl=list(method='L-BFGS-B')
                   )
)

summary(glm_model)


#Log likelihood ratio tests

# Model 1
glm_full<- glmer(choice ~ accuracy + benefit + (1|user_session_id),
                   family = binomial,
                   data = model_data,
                   control = lmerControl(optimizer ='optimx',
                                         optCtrl=list(method='L-BFGS-B')
                   )
)


# Model 2
glm_accuracy <- glmer(choice ~ accuracy + (1|user_session_id),
                   family = binomial,
                   data = model_data,
                   control = lmerControl(optimizer ='optimx',
                                         optCtrl=list(method='L-BFGS-B')
                   )
)


#Comparing model 1 with model 2
anova(glm_accuracy, glm_full)

#Comparing model with the the full model
anova(glm_full, glm_model)
```