# Demystifying Detection: The Effects of Experience, Culture, and Personality on System Acceptance of Facial Recognition Technology

**Shaleila Louis**
HCI-E MSc Final Project Report 2020
UCL Interaction Centre, University College London
Supervisor: Daniela Romano

## ABSTRACT

Facial Recognition technology as a subset of Artificial Intelligence-driven technology grows increasingly advanced, ubiquitous, and controversial. Numerous factors impact one's inclination to trust and accept such facial recognition technology. This study investigates three primary factors: one's level of experience with the technology, one's country of residence and its place on the cultural dimension scale of Individualism/Collectivism, and one's personality characteristics (as measured by the Big Five Inventory and Locus of Control). Two hundred and forty-six participants from ten countries (consisting of both Naive users unfamiliar with the technology, as well as Expert users of the technology) completed a digital questionnaire measuring personality and attitudes.

It was found that expert users of the technology are more accepting of facial recognition systems and less wary of risks, though they trust the system less than naive participants do. Participants from Collectivist countries (India, Russia, and Singapore) were found to be more accepting of, trustful of, and positive towards systems, and less concerned about risks than those from Individualistic countries (the USA, the UK, and Canada). Lastly, Locus of Control and three of five dimensions of the Big Five Inventory (Agreeableness, Neuroticism, and Openness) were found to be predictors of trust in systems, and closely correlated with each other.

The findings demonstrate that attitudes towards facial recognition technology are impacted by one's experience level, cultural background, and personality. Thus, implementation of new facial recognition systems should be informed by cultural norms and personality in order to better understand perceptions of the system and encourage acceptance.

**MSC HCI-E FINAL PROJECT REPORT**

*Project report submitted in part fulfilment of the requirements for the degree of Master of Science (Human-Computer Interaction with Ergonomics) in the Faculty of Brain Sciences, University College London, 2020.*

***NOTE BY THE UNIVERSITY***

*This project report is submitted as an examination paper. No responsibility can be held by London University for the accuracy or completeness of the material therein.*

**Author Keywords**
Facial Recognition; Artificial Intelligence; Trust; Cultural Dimensions; Big Five Personality Traits; Locus of Control.

**ACM Classification Keywords**
K.4.m: Computers and Society: Miscellaneous; I.2.1: Artificial Intelligence: Applications and Expert Systems; H.5.m: Information Interfaces and Presentation (e.g., HCI): Miscellaneous

**MSc Contribution Type**
Empirical.

## 1. INTRODUCTION

Following rapid advancements in its accuracy and ease of use, the prevalence of facial recognition technology has risen markedly in recent years. Facial recognition is quick, non-intrusive, easy to set up, and requires no action by the user to function. It has thus swiftly come to replace traditional biometric forms of identification, such as keycards, tokens, and passwords [49]. Facial recognition technologies encompass a variety of forms and functions, ranging from the readily available Apple Face ID locking mechanism to Automatic Face Recognition Technology (AFR), primarily used by police to scan faces in a crowd and automatically detect individuals on watchlists. Local governments have employed facial recognition for numerous functions, from security terminals at airports and train stations in London, to the automatic inclusion of identification card pictures in national databases in Australia [100].

With facial recognition technology being installed in public locations and being increasingly readily available for purchase and installation in one's home, a variety of attitudes towards the technology have arisen. Acceptance of traditional biometric identification technologies have been studied in contexts such as restaurants [72] and hotels [73, 36], though attitudes towards biometrics do not necessarily extend to facial recognition due the "black box" perception of obfuscation. It is not immediately apparent how and when they work, and where and when information is stored.

Facial recognition technology has received widespread coverage in the news and technosphere in 2020, due to mainstream acknowledgement of the numerous capacities in which it is available to and present in the lives of the public. Reporting has focused on issues of power and distribution [35], ethics and databases [41], proposals of regulatory legislation in the United States [29], and the involvement of tech giants in the ownership and distribution of facial recognition-based systems [41, 61, 88]. Much of this reporting has been driven by critiques of facial recognition technology in the wake of the Black Lives Matter movement worldwide that have catalyzed the reexamination of technologies, corporations, and policies vulnerable to racial discrimination [27]. Federal agencies in the United States have signed contracts with leading facial recognition companies such as Clearview AI for use by the Air Force and the department of Immigration and Customs Enforcement (ICE) [63]. The police department of the city of Miami recently used Clearview AI's facial recognition technology to identify and arrest a protestor [26]. The COVID-19 pandemic has sparked reflection on facial recognition as well, owing to discussions about mask wearing as a deterrent to systems that make use of the technology, and the advancements in technology required to address this [38, 98, 96]. Schools in the United States have instituted plans to install AI-driven facial recognition and temperature check systems that scan students for face coverings, symptoms of illness, and monitor social distancing [39].

These discussions have led to a rift in attitudes towards facial recognition technology. A recent survey of a representative sample of the UK population by the Ada Lovelace Institute [2] found that 67% of the population are uncomfortable with the use of facial recognition in schools, and 61% with its use on public transport. The Lovelace Institute's survey also found that only 15% of the UK's population are aware of the current use of facial recognition technology in workplaces, shops, and commercial areas. The present study was carried out in conjunction with o.vision, a Russian-based technology company that develops AI-driven technology that is in the process of being implemented in the UK in select commercial spaces. Their most visible and widely used product is the Face Gate, a facial recognition system that can digitally operate turnstiles and control entry to locations [75]. It is currently in use in Russia in student residences, a number of offices and commercial buildings, and is being pilot tested for use in the United Kingdom. Users of the technology in these existing locations served as the "Expert" participants for the study.

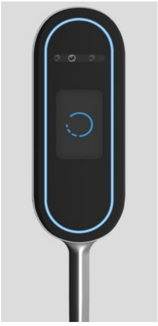

**Figure 1. The o.vision Face Gate**

The renewed cultural awareness of and interest in facial recognition technology begets an urgency to study the factors influencing the acceptance of such systems. The following study will attempt to study technology acceptance of facial recognition systems as influenced by three factors: experience, culture, and personality. Scales of measurement of technology acceptance, as well as these three factors are explored further in the Literature Review section.

## 2. LITERATURE REVIEW

### 2.1 Technology Acceptance and the TAM

The Technology Acceptance Model (TAM) proposed by Davis in 1986 as an adaptation of the Theory of Reasoned Action [3] is a powerful model for understanding and distilling system acceptance, and has been an influential and leading model in the field of Information Systems since its inception. It is commonly used to provide a framework to study the reasoning behind variation in the acceptance of novel technologies among various populations. The TAM can be used to measure the efficacy of a system in addition to its acceptance [76]. A meta-analysis of the TAM by King and He [56] evaluates the TAM and indicates strong reliability, and finds that "students may be used as surrogates for professional users" in research involving the TAM. The original model proposed two primary variables that affect the acceptance of a system: Perceived Usefulness and Perceived Ease of Use. Over time, the TAM has been adapted and extended to include additional variables, including Perceived Innovativeness, Attitude, and Intentions [60, 19]. These adaptations have allowed the seminal TAM to apply more closely to newer and more specific technologies, such as voice-assistant system adoption [74], new email systems [90], social media usage [81], online banking [77], and novel health technologies [46]. The present study will build on existing extensions of the TAM, constructing the core questionnaire around variables used in similar and linked research. These inclusions are detailed in the Methodology section.

### 2.2 Factor 1: System Acceptance and Experience

The speed at which facial recognition systems work, combined with their "watchful eye" appearance recalls the theory of the Uncanny Valley, first proposed by Masahiro Mori in 1970 [71]. He explained that the human reaction towards robots grows increasingly distasteful and full of wariness as it becomes apparent that it can carry out human-like tasks without a human-like appearance [71, 78]. According to the model, a device's manifestation of ability must be congruent with our mind models. In other words, if it behaves very much like a human, then it must look like a human [33]. Cameras used for facial recognition, particularly the o.vision Face Gate (Figure 1) have a distinctly robotic and futuristic appearance. The o.vision face gate carries out a task with a very high level of complexity – face recognition. This is a deeply human task at its core, and conflicts with the clinical outward appearance of the device. This could be seen dissonant with its level of automation at first, though it is possible to grow accustomed to the device and its task. It is thus interesting to explore whether experienced users who have had time to attain familiarity and comfort with the device are more accepting of the system than non-users, or if familiarity with the device is insufficient to build trust and positivity. Troshani et al [93] studied the impact of AI "humanness" on acceptance, finding the influence of anthropomorphism and emotion were strong, and that the uncanny valley-ness of an AI-technology affected its acceptance in specific contexts - for example, AI-based healthcare in a hospital was found to be less acceptable as it lacked a human touch required for care, while AI-based text message and autocomplete suggestions were deemed acceptable as they aided the user. Similarly, Gursoy et al [34] found that the acceptance of AI-based devices is guided by emotion and based on personal preferences regarding human contact and perceived performance. Thus, acceptance of AI is contextual and based on the specific expectations that users have of the system at hand.

The impact of experience and expertise specifically on acceptance of various technologies has been studied previously only in limited contexts. A 2007 study used an adaptation of the TAM tailored specifically towards websites - the Website Acceptance Model (WAM) - to study the impact of experience with a specific health and wellness website and with the Internet as a whole on the user's intent to revisit the website. Their results determined that experience level moderated how the users viewed the website: users with a lower experience level prioritized perceived ease of use of the website when deciding to visit, while more experienced users were impacted more by the perceived usefulness of the website [16]. Koch et al [57] studied the effect of novelty on user reactions to large display field prototypes, finding that excitement was increased only directly after the initial installation of prototypes, or after changes were made to an existing prototype. Tzeng [95] studied college students' reactions to an eportfolio system, comparing attitudes towards the system before and after use. It was found that perceived functional value mediated initial attitudes towards the system, while perceived contextual value later influenced attitudes further. Karahanna et al [55] acknowledge a gap in the traditional TAM models and adaptations in incorporating individual compatibility into the study of technology acceptance. In response to this research gap, they propose and test a measure of compatibility which includes "compatibility with prior experience" into their model. Their findings suggest strength in their compatibility model, lending validity to the inclusion of experiential-based attitudes in studying technology acceptance. Similar attitudes to novelty and experience such as technology readiness have been studied [62], though there is a dearth of research on novelty of technology as it applies to AI-driven technologies and biometrics. The present study addresses this gap in the literature.

Public perception of facial recognition technology is adversely affected by numerous perceived risks. Concerns regarding racial discrimination and data privacy have been resurfaced recently, but represent only a selection of the primary risks that shape perception of such technologies. Privacy is a concern for many users of facial recognition technology, due to the possibility of data leaks and breaches. Users have little control over the regulation and maintenance of databases holding biometric data, and a leak of such sensitive information is permanent [101]. In the United States, facial recognition technology has been banned in San Francisco, and a bill has been introduced to ban police use altogether [50]. In the EU, GDPR data protection regulations cover all biometric data, including personal likeness. A rising awareness of data rights and privacy has sparked worldwide debate on facial recognition and its potential infringement on personal privacy.

There are also issues of racial bias and misidentification at play: Krishnapriya et al [58] found that facial recognition is more likely to make a false match when presented with an African-American face than a Caucasian face. An evaluation of facial recognition systems by IBM, Megvii, and Microsoft found the systems 34.4% more likely to misidentify darker-skinned females than lighter-skinned males [15]. As stated by Andrejevic and Selwyn [6], "frequent concern has been raised over the disproportionate emphasis that facial recognition places on 'detecting' the gender and race of those individuals that it identifies". Furthermore, a test using facial recognition systems by Google, IBM, and Microsoft of participants wearing masks found that masks on women's faces were misidentified as duct tape 28% of the time by Google's Cloud Vision API, as compared to only 15% of the time on men's faces. On IBM's Watson Visual Recognition system, masks were misidentified as gags and restraint chains in 23% of cases on women versus only 10% of the time on men. Similarly, with Microsoft's Azure Cognitive Services Computer Vision system, the system showed low reliability across gender, but was much more likely to mistake a mask for a fashion accessory on women and a beard on men [9]. Facial recognition systems are not perfectly accurate, and their error rates vary drastically between different technologies and algorithms. They can be spoofed by Deepfake videos and "face swapping" technology, resulting in false positives. The South Wales Police reported an error rate of 91% when testing its facial recognition system's ability to detect target matches from among members of the public [79].

Public concerns about facial recognition stem, too, from a lack of knowledge about the process behind the camera, and the lack of the ability to "opt out" in most instances [2]. There is an unease that widespread facial recognition technology in public areas will "normalize surveillance" [2], and result in abuse of power. An Ipsos survey of adults across 26 countries found that 65% believe that facial recognition may be deployed by the government "to maintain order in the country, but only under certain circumstances and subject to strict regulations" [12]. There is concern around the pliable ethics of constant surveillance. As stated by Mann and Smith [67] in a legal examination of facial recognition, "one prominent concern about the inadequacy of privacy protections is the potential for 'function creep', where the use of information taken for a particular purpose is used for other purposes for which consent was not obtained."

These risks are likely to impact system acceptance, as the average person aware of facial recognition technology is likely to be concerned about or have been impacted by the public conversation around them. Experience using facial recognition technology for a period of time may not necessarily alleviate concerns over these risks, as many are concerned with the larger-scale operation of database maintenance and legislative governance that is distanced from the user's control. However, increased time spent with a system may dull these concerns, as comfort and familiarity with its functionality may eclipse worries regarding its operation.

### 2.3 Factor 2: Cultural Dimensions and System Acceptance

Satisfaction and urgency regarding legislation on facial recognition remains a regional debate, varying by country and state. Attitudes towards facial recognition may be culturally shaped; influenced by social norms and a collective openness to efficient yet opaque technology. A relevant cultural dimension that may help explain attitudinal differences between countries towards facial recognition technology is Individualism. Individualism is one of five cultural dimensions proposed and refined by Geert Hofstede through his research at IBM [43]. The spectrum of individualism vs. collectivism represents "the degree to which individuals are integrated into groups". Table 1 describes the two ends of the spectrum.

| | |
|---|---|
| Individualism | Societies in which the ties between individuals are loose: everyone is expected to look after him/herself and his/her immediate family. |
| Collectivism | On the collectivist side, we find societies in which people from birth onwards are integrated into strong, cohesive in-groups, often extended families (with uncles, aunts and grandparents) which continue protecting them in exchange for unquestioning loyalty. |

**Table 1. Individualism and Collectivism as described by Hofstede [44]**

Countries such as Russia [66], India [45], and Singapore [80] are considered collectivist, while countries such as the United States of America [45], the United Kingdom [92], and Canada [45] are considered individualistic.

These cultural leanings profoundly influence social norms of acceptance and openness. In a study of the effect of culture on technology mediated learning, Hornik and Tupchiy [47] found that collectivist tendencies towards benevolence and conformity, and individualistic tendencies towards power, achievement, and self-direction affected the sense of community during learning. Culture impacts openness and receptiveness, which in turn shapes technology acceptance. It appears that more individualistic cultures may exhibit limited openness to the risks and novelty of facial recognition technology, while more collectivist cultures may weigh the social utility of the technology higher than its hazards, and exhibit acceptance and openness. For example, a 2012 study [14] of the integration of biometric technology into healthcare solutions in China and the United States revealed different population needs and recommendations progress in distinct directions despite similar patient needs. China progresses towards greater digitization of patient data and demographics than the United States. Further, a 2009 study comparing biometric technology acceptance between India, South Africa, and the United Kingdom on culture found that Indian respondents displayed the greatest positivity towards biometric technology, citing its security and efficiency, while respondents from the United Kingdom were most wary, citing issues with reliability and privacy [82]. Widespread attitudes towards technology can be instrumental in determining the acceptance of facial recognition technology specifically, as was recently observed during uprisings against CCTV street cameras and sensors in Hong Kong during protests against extraditions to Mainland China [97]. Blas [11] describes the "emerging "global face culture," exemplified by biometrics and facial detection technologies, driven by ever obsessive and paranoid impulses to know, capture, calculate, categorize, and standardize human faces" that is "rooted in commercial, state, and military interests".

As Gates states on page 4 of her 2011 book [32], "Our biometric future: Facial recognition technology and the culture of surveillance", "U.S. border, airports, cities, suburbs, shopping malls, bars, casinos, banks, schools, workplaces homes—and the bodies and behaviors of the inhabitants of these spaces—are special areas of experimentation for new surveillance technologies, in no small part because contemporary U.S. culture exhibits an intense preoccupation with the combined priorities of security and technology." Gates speaks further about the American "idea that the events of 9/11 could have been prevented with the sophisticated technological products of modernity" in a 2004 paper [31]. Fujawa, in a 2005 report [28] on national security and individualism, poses a strongly worded follow-up, "If biometric national identity cards are put into effect, and do indeed destroy the liberties and freedoms that American citizens once enjoyed, then the terrorists will have won. They will have destroyed the United States of America, the land of the free." In the United Kingdom, a report by The University of Essex's Human Rights Centre on the Metropolitan Police's use of facial recognition technology unearthed sizable qualms over its lawfulness and whether it could be deemed "necessary in a democratic society" [30].

In contrast, Payal Arora speaks to two distinct but linked sets of governance models in India and in China: the "Aadhaar" biometric identity initiative, and the Social Credit System, respectively. She poses that both systems represent a heretofore unprecedented large scale digitization of sensitive citizen data. However, both serve the stated goal of improving the quality of life for citizens, and fostering enthusiasm around these systems that begets community trust. She stresses that by "focusing on the outcomes including citizen's perceptions, we may be able to move beyond the narrow democratic versus authoritarian construct that has dictated the analysis of governance systems", forming a "complex narrative that goes beyond the Western conceptualization of democracy" [7]. These pointed distinctions in response to large-scale surveillance as it serves the goal of national prosperity pinpoint a clear cultural rift in attitudes linked to individualism and collectivism.

### 2.4 Factor 3: Trust in Technology and Personality Characteristics

The present report builds substantially on recent work by Sharan and Romano [87], who recently studied the effect of personality traits and the locus of control on trust, specifically between trust in humans versus trust in artificial intelligence (AI). Trust has been shown to be instrumental in determining technology acceptance. Bradford et al [13] conducted a study of public attitudes towards the police use of Live Facial Recognition technology to conduct real-time identity checks in London, concluding that trust (alongside legitimacy) is the most critical factor in assuaging concerns and fostering acceptance of the technology, and "alleviates privacy concerns". As stated by Chien et al [18], trust is an "intervening variable between user intention and actions involving reliance on automation." The relationship between humans and AI is mediated by a number of factors influencing trust and distrust, and feelings range from "calmness and security" to "fear and worry" [63]. Trust is a complex social process, and is thus subject to numerous factors when applied to AI [42, 59]. Sethumadhavan [85] notes that the correct level of trust in AI needed can be achieved by considering dispositional, internal, environmental, and learned factors, thus designating trust a complex yet influential aspect of technology acceptance.

Transparency is also critical in breaking open the "black box" and helping create "accurate mental models" of the workings of AI-based systems [8]. Siau and Wang [86] analyze the building blocks of trust in AI, attributing trust to a combination of "the trustor's disposition to trust, and the trustee's ability to deal with risks". Tschopp and Ruef [94] support this division, breaking trust in automation down AI-related factors, human-related factors, and environmental factors. Both studies illustrate a scale of trust over time, elucidating that the trust relationship must be sparked by image, user reviews, transparency, and trialability, and must be maintained through usability, reliability, collaboration, security, and interpretability. Rossi [83] echoes these pillars, settling on three primary practically implementable steps towards building trust in AI: 1. Explainability, 2. Bias Awareness and Mitigation, and 3. Trusting AI Producers. Rossi also stresses the importance of collaborating with policymakers and regulators. Thus, trust is complex and nuanced, and buttresses acceptance and subsequently openness to technology adoption. As such, the present study will both incorporate a measure of personal trust into the assessment of system acceptance, and will isolate trust as a factor to study how it is impacted by personality traits.

In Sharan and Romano's recent work [87], they conclude that personality is the primary determinant of trust, as measured by the Locus of Control, and the five dimensions of the Big Five personality Inventory. They found that the Locus of Control represented the greatest influence on trust, holding a strong negative correlation. In addition, the BFI dimensions of Openness and Neuroticism predicted trust, positively and negatively, respectively. Moreover, they state that trust is a critical element of human behavior, and needs to be incorporated into our understanding of personality. This study will further explore the role of trust in system acceptance, and the influence of the BFI and the Locus of Control on trust in facial recognition systems.

Pioneering studies in trait psychology have condensed pillars of human behavior to a number of countable traits. Early work by Cattell [17] identified 35 core traits, and Fiske [24] narrowed these down to emerge five traits that would come to be known as the Big Five. These traits describe personality at their "broadest level of abstraction", and have been repeatedly shown to shape individual differences in behavior and social attitudes across cultures [54, 87]. Table 2 lists an overview of the five dimensions.

A study by Mooradian et al [70] linking personality to trust concluded that the propensity to trust is not caused by agreeableness, but is instead a facet of agreeableness itself. Two studies on trust and trustworthiness in the context of an Investment Game found that extraversion and negative neuroticism were linked to trust, agreeableness and conscientiousness were linked to trustworthiness [23]. Conversely, a study of trust in UK-based cellular providers concluded that the Big Five personality traits did not constitute a major influence on trust, accounting for only 4% of the variability in trust by participants [5].

| Big Five Dimension | Definition |
|---|---|
| **Openness** – Closedness | Curious and seeking new experiences |
| **Conscientiousness** – Lack of direction | Organised, meticulous, and reliable |
| **Extraversion** – Introversion | Energetic, assertive, and seeking excitement |
| **Agreeableness** – Antagonism | Warm, friendly, and helpful |
| **Neuroticism** – Emotional stability | Anxious and moody |

**Table 2. A description of the Big Five dimensions [87]**

Locus of control (LOC) describes a person's "expectancy for reinforcement", or the extent to which one feels in control of the events that influence one's life. As explained by Duttweiler, an individual with an internal locus of control "believes that reinforcement is contingent on his or her own behavior" and champions mastery of one's own life, while an individual with an external locus of control "believes that reinforcement is contingent on luck, chance, or powerful others" and lacks belief in the ability to control their own life [22]. The original scale of measurement of locus of control was Rotter's I-E scale, though the Internal Control Index (ICI) has since come to be considered a more accurate and reliable measure of locus of control [68, 48]. A low score on the ICI denotes internal control, while a higher score denotes external control. Locus of control guides decision making behavior, and extends to decisions of trust as well. In a study on the adoption of agricultural technology in Ethiopia, Abay, et al [1] found that locus of control was a significant determinant in adoption behavior, and that farmers with an internal locus of control showed increased proclivity to adopt new technology compared to those with an external locus of control. Sharan and Romano [87] link an internal locus of control with independent, considered decision making, though note that the link between LOC and trust, particularly among AI and technology, has not yet been widely studied.

## 3. RESEARCH QUESTIONS

The literature recounts a rift in attitudes towards facial recognition technology, driven by apprehension towards numerous risks, and an increasing awareness of data rights and an aversion to a surveillance state. With the rise in uniquity of facial recognition technology comes an urgent need to fill the gaps in research on attitudes towards these systems. The Technology Acceptance Model is a measure commonly used and adapted to study system acceptance, and will form the core of the present study's methodology. In addition, the literature shows that familiarity with technology may breed trust, and that cultural dimensions can play a role in the acceptance of new systems, owing to differences in openness and shared trust. Furthermore, personality traits and locus of control have been linked to trust in technology, most recently in work by Sharan and Romano [87].

In an effort to better understand the contributions of these factors towards the acceptance of new systems and specifically facial-recognition technology, the following three research questions were developed:

Research Question 1: How does the novelty of facial recognition technology impact acceptance of the technology?

Research Question 2: How do cultural dimensions impact acceptance of facial recognition technology?

Research Question 3: How do personality characteristics (as measured by the Big Five personality inventory and the Locus of Control test) impact trust in facial recognition technology?

## 4. METHOD

### 4.1 Participants and Recruitment

A total of 246 participants were recruited for this online study, through University College London student listservs, social media, and word of mouth. Of these 246, 27 participants were designated "Expert" users, as they had experience using the o.vision technology either through working in an office or residing in a student residence currently using the technology as its entry-granting system. All 27 of these participants were from Russia, as the technology is currently in use only in select buildings in Russia. The remainder of the 219 participants were "Naive" users, having no familiarity or experience with the o.vision technology at all.

Participants were given the option to enter a raffle to win one of thirty £10 gift vouchers in compensation for their participation.

Participants were recruited from ten countries in total: Russia, India, Singapore, the United States of America (USA), the United Kingdom (UK), Canada, Australia, New Zealand, Indonesia, and United Arab Emirates (UAE). Due to the low number of participants from Indonesia, Australia, New Zealand, and the UAE, these countries have been considered together as "Other" in all analyses. Of the countries with sufficient sample sizes, the USA, the UK, and Canada are considered individualistic countries, while India, Russia, and Singapore are considered collectivist countries. All participants from Russia completed a translation of the questionnaire in the Russian language (translated by native speakers), while participants from all other countries completed the questionnaire in English, as included in Appendix 1. All open ended questions collected in Russia were translated back to English by native speakers for the analysis process. Table 3 summarizes the sample's demographic profile.

| **Category** | **Number (N)** | **Percent (%)** |
|---|---|---|
| Gender | | |
| Female | 118 | 47.97 |
| Male | 123 | 50.00 |
| Other / Do not want to disclose | 5 | 2.03 |
| Age | | |
| 18-24 | 84 | 34.15 |
| 25-34 | 49 | 19.92 |
| 35-44 | 29 | 11.79 |
| 45-54 | 40 | 16.26 |
| 55-64 | 34 | 13.82 |
| ≥65 | 10 | 4.07 |
| Highest Level of Education Attained | | |
| Less than high school | 5 | 2.03 |
| High school/GED | 9 | 3.66 |
| Some college | 8 | 3.25 |
| 2 year college (Assoc. Degree) | 10 | 4.07 |
| 3/4 year college (BA/BS Degree) | 87 | 35.37 |
| Masters degree | 110 | 44.72 |
| Professional degree (MD, JD, etc.) | 11 | 4.47 |
| Doctoral Degree | 6 | 2.44 |
| Country of Residence | | |
| Australia | 1 | 0.41 |
| Canada | 11 | 4.47 |
| India | 63 | 25.61 |
| Indonesia | 1 | 0.41 |
| New Zealand | 1 | 0.41 |
| Russia | 68 | 27.64 |
| Singapore | 26 | 10.57 |
| United Arab Emirates | 2 | 0.81 |
| United Kingdom of Great Britain and Northern Ireland | 61 | 24.80 |
| United States of America | 12 | 4.88 |
| of which: | | |
| *Designated collectivist* | *157* | *63.82* |
| *Designated individualistic* | *84* | *34.15* |
| *Excluded* | 5 | *2.03* |
| Level of Experience | | |
| Naïve | 219 | 89.02 |
| Expert | 27 | 10.98 |
| **Total** | **246** | **100** |

**Table 3. Demographic information of the sample**

### 4.2 Questionnaire Design

All data for the present study was collected through an online questionnaire administered through the platform Opinio, a web-based survey tool. Participants were limited to one response per person, regulated via device tests and browser cookies. All data was collected between June and July of 2020.

The multi-item questions on the questionnaire fall under eight sections for analysis purposes, each measuring a different dimension of system acceptance, as itemized below. A complete copy of the questionnaire is available for reference in Appendix 1. Of 19 total questions, 7 were open-response, allowing participants to elaborate on their selections in previous questions. The final question (Question 19) asked participants to comment on the ways in which their attitudes towards facial recognition technology may have been affected by the COVID-19 pandemic in 2020, as well as the sudden surge in news reports and legislative decisions regarding facial recognition technology primarily in the USA and UK, as both were particularly prevalent during the time the questionnaire was being administered.

*Demographic Questions*

Questions 1 through 5 collected basic demographic information from participants of their gender, age group, highest level of education attained, occupation, and country of residence. Participants were asked to select a country of residence from a dropdown list, so as to keep responses consistent.

*Personality Test (The Big Five Inventory)*

The sixth question encompassed a 44-item personality test using the Big Five Inventory (BFI). The Big Five Inventory was used to measure personality by Sharan and Romano [87], and is a reliable and comprehensive measure of personality traits that has demonstrated stability across time [20] and validity across geographic region [84]. As in Sharan and Romano, the BFI test used was adapted from John and Srivastava's 1999 book [54], and encompasses a list of 44 statements to be scored on a five points scale of 1 - "I strongly disagree" to 5 - "I strongly agree". Each of the statements measures one of the five dimensions of the BFI - Extraversion, Openness, Agreeableness, Conscientiousness, and Neuroticism. Of the 44 items, 16 were reverse scored.

*Locus of Control testing (The Internal Control Index)*

The seventh question constituted a Locus of Control test, as measured by a 28-item Internal Control Index (ICI). This was derived from Duttweiler's [22] work, and was used in the present study as well as by Sharan and Romano [87] due to its accuracy of measurement of the Locus of Control as compared to other scales [65, 68]. The ICI consists of 28 statements to be scored on a five point scale of frequency, from 1 - "Rarely (Less than 10% of the time)" to 5 - "Usually (More than 90% of the time)". 13 of the 28 items were reverse scored, and the composite score used to calculate a single participant's Locus of Control score.

*Social Priming*

This section of the questionnaire begins with a short description of the o.vision system and technology from the perspective of the user, introducing its basic functionality, instructions for use, and capabilities. This description is accompanied by two pictures of the system and a depiction of it in use, to place participants in the shoes of a user and prime them to imagine the experience of using the system personally. While the system is described accurately and fully, details about its development, corporate ownership, and real world presence are not mentioned, and as such the description could be read as one of a prototype. It is also deliberately not mentioned that the founding corporation is based in Russia. These omissions are precautions against any prejudicial evaluation of the system, and to elicit from participants more generalized views of facial recognition technology as a whole using the o.vision system as a proxy, rather than views on the specific system, company, and optics.

The eight and ninth question prompt participants to reflect on their own experiences with facial recognition technology, to jog existing attitudes and memories. Question 8 asks users to identify any forms of facial recognition technology they may have already used from a list of 5 items, using the scale "Yes", "No", and "Not Sure". Question 9 prompts for any additional examples. These two questions are not incorporated into the quantitative analyses as they are purely for reflection and priming purposes. Similarly, Question 13 (described below) is not included in the analysis as its primary goal is to prompt deeper reflection on similar systems in participant environments.

From this point onwards, the subsequent sections were pooled to measure System Acceptance as a broad measure with the following four subsections:

*Positivity of Beliefs*

Questions 10 and 11 measured general attitudes of acceptance and enjoyment of facial recognition tech, probing for attitudes on ease of use, usefulness, enjoyment, cost, and acceptance to self. Question 10 listed these five dimensions as 5 items, which participants scored on a Likert scale in increasing order of acceptance from 1 to 5. These dimensions were derived from a theoretical framework created by Miltgen et al [69] used to measure individual acceptance of biometric identification technologies. Their model amalgamates primary elements from the Technology Acceptance Model (TAM), diffusion of innovations (DOI) and unified theory of acceptance and use of technology (UTAUT), as well as dimensions from the "trust-privacy research field". Drawing on the user acceptance model for information systems developed by Van der Heijden [37] which includes the factor "perceived enjoyment", the item on enjoyment was added. In addition, the item on cost was added based on Wu & Wang's [99] extension of the TAM as applied to mobile commerce acceptance, which includes "Cost" as a factor. Question 11 asks participants to elaborate on the dimensions above.

*Contexts of Acceptability*

Building further on the assumptions behind the TAM and its extensions in the work cited above, Question 12 queried participants on the contexts in which they find facial recognition technology acceptable using a Likert scale from 1-5 in increasing order of acceptance. 8 items were included, such as "Airports", "Schools", and "Offices". Question 13 asks participants to indicate whether any of 4 common alternatives to facial recognition-based security systems are present in their lives and social circles, such as "Fingerprint-based system" and "Barcode-based system". Question 14 prompts further reflection on their attitudes towards replacing existing security systems (such as the 4 in Question 13) with facial recognition-based technologies.

*Perception of Risks*

Drawing once again on Miltgen et al's [69] model's usage of "perceived risk" and "privacy concerns", Question 15 focuses on attitudes towards perceived risks associated with the facial recognition system. Participants responded on a Likert scale from 1-5 in increasing order of risk (and thus decreasing order of acceptance), rating their concern with 6 named risks, such as "Data security", "Data sharing/privacy", and "Unsure how it works". Question 16 asks participants to list any additional risks they can think of, and Question 17 then prompts them to condense their trust of or distrust towards the system down by expressing their likelihood to recommend the system to a friend. This question draws on Miltgen et al's [69] work as well, specifically incorporating the notion that "The greater the perceived compatibility, the greater the intention to accept the biometric system."

*Measures of Trust*

Question 18 measures trust in the system via an adapted 20-item scale. Participants responded to 20 statements such as "The system is deceptive", "The system can recognize human faces just like a real person", and "I am confident in the system", scoring their responses on a Likert scale of agreement from 1-5. Questions indicating distrust were reverse scored, yielding a composite trust score that greater higher trust with a higher score. This section primarily uses statements developed by Jian, Bisantz, and Drury [52] in measuring trust between humans and automated technologies. The statements are further adapted from statements composed by Forster et al [25], who coined and tested several hypotheses around trust in system performance, process, purpose, and anthropomorphism in evaluation of a system of automated driving. Similar perceptions of attitude were employed by Bettiga and Lamberti [10] to study the perceived value of specific technologies, and also influenced the statements in this question to measure trust and wariness.

All items under the sections Positivity of Beliefs, Contexts of Acceptability, Perception of Risks, and Measures of Trust form the 39 items which will be considered at length to measure System Acceptance in response to the first two research questions.

### 4.3 Study Design

For the first research question, the independent variable was the participant's Level of Experience with the technology - Naive or Expert. The dependent variable was System Acceptance, which was measured by the four aforementioned sections of the questionnaire: Positivity of Beliefs, Contexts of Acceptability, Perception of Risks, and Measures of Trust. Each of the 39 items that fell under these four categories formed our measure of System Acceptance, and items that were reverse scored were duly reversed to match with the others when calculating mean scores.

For the second research question, the independent variable was the participant's Country of Residence, considered individually, as well as under the umbrella of collectivist and individualistic. The dependent variable was System Acceptance, measured in the same manner as stated above.

For the third and final research question, the independent variables were participant scores on the Big Five personality test on each of the five dimensions (scored according to the BFI), as participant scores on the Locus of Control test (scored according to the ICI). The dependent variable was the participant Trust Score, calculated through the 20-item trust scale as a subset of the overall system acceptance questionnaire. These 20 items were averaged, and reverse scored questions balanced to achieve one composite trust score for each participant. Figure 2 summarises all variables and research questions.

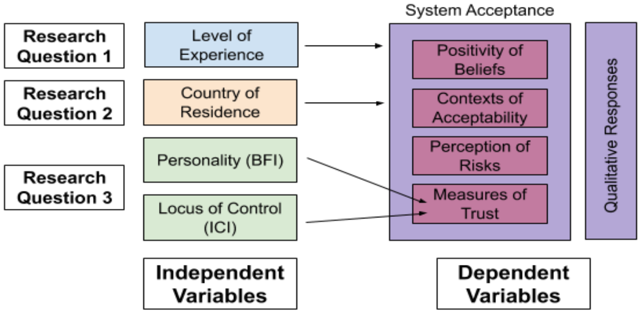

**Figure 2. Variables and Research Questions**

## 5. RESULTS

A reliability analysis was conducted on all quantitative questions of the questionnaire measuring Social Priming, Positivity of Beliefs, Contexts of Acceptability, Perception of Risks, and Measures of Trust - a total of 49 items. A Kolmogorov-Smirnov test was carried out on the applicable variable data, and the data was found to be not normally distributed. As such, non-parametric tests were carried out on the data.

The Big Five personality test (BFI) was scored to achieve five scores for each participant, one for each of the five dimensions: Extraversion, Agreeableness, Conscientiousness, Openness, and Neuroticism. The Locus of Control test (ICI) was scored to achieve a single score for each participant.

### Research Question 1: System Acceptance by Experience Level

A Mann-Whitney U test was conducted on 39 total items under 4 categories of system acceptance: Positivity of Beliefs, Contexts of Acceptability, Perception of Risks, and Measures of Trust, by level of experience. Significant differences in system acceptance by experience level were found on 9 total items, falling under 3 of the 4 categories: Contexts of Acceptability, Perception of Risks, and Measures of Trust. These items are summarized in Table 4.

Means of each significant item were taken and are summarized below in Table 5 by category. Composite means of all items falling under the same category (and thus corresponding to the items listed in Table 4) were also taken and are summarized below in Table 6. Tables 5 and 6 also illustrate color-coded results by level of experience where greener shades indicate greater system acceptance, and redder shades indicate lower system acceptance.

### Research Question 2: System Acceptance by Country

A Kruskal-Wallis H test was conducted on the same 39 total items under 4 categories of system acceptance: Positivity of Beliefs, Contexts of Acceptability, Perception of Risks, and Measures of Trust, by country of residence. Significant differences in system acceptance by country were found on 24 total items, falling under all of the 4 categories. These items are summarized in Table 7.

Means of each significant item were taken and are summarized below in Table 8 by category. Composite means of all items falling under the same category (and thus corresponding to the items listed in Table 7) were also taken and are summarized below in Table 9. Tables 8 and 9 also illustrate color-coded results by level of experience where greener shades indicate greater system acceptance, and redder shades indicate lower system acceptance.

In order to isolate the effects of experience on trust independent of the influence of different cultural dimensions, a Mann-Whitney U test was conducted on Trust by experience level, Expert or Naive using only data from Russia, as Russia is the only country with Expert participants. To yield a single Trust score, the 20-item trust scale from the questionnaire was scored to achieve a single Trust Score for each participant. No significant difference was found between Trust in the system by experience level on data from Russia (U = 411.5, p = .075). These results are detailed in Table 10.

| | **Mann-Whitney *U*** | **Wilcoxon *W*** | **Z** | ***p*** |
|---|---:|---:|---:|---:|
| Acceptability2 | 2089 | 26179 | 2.637 | 0.008** |
| Risks2 | 1826.5 | 2204.5 | 3.385 | 0.001** |
| Risks3 | 2218 | 2596 | 2.168 | 0.03* |
| Risks4 | 1966.5 | 2344.5 | 2.897 | 0.004** |
| Risks5 | 2113 | 2491 | 2.479 | 0.013* |
| Risks6 | 2189.5 | 2567.5 | 2.275 | 0.023* |
| Trust10 | 1723 | 2101 | 3.738 | 0** |
| Trust11 | 1807.5 | 2185.5 | 3.393 | 0.001** |
| Trust20 | 2201 | 2579 | 2.335 | 0.02* |

* significance at the .05 level (2-tailed); **significance at the .01 level (2-tailed).

**Table 4. Mann-Whitney U results**

|  | Naïve |  | Expert |  |
|---|---|---|---|---|
|  | (*N* = 219) |  | (*N* = 27) |  |
|  | ***M*** | *SD* | ***M*** | *SD* |
| Acceptability2: I believe that the o.vision system is acceptable as a building entry system in the context of: Halls of Residence (Student Buildings) | **3.78** | 1.39 | **4.48** | 0.89 |
| Risks2: Data Sharing/Privacy [Lower score is better] | **3.85** | 1.31 | **3.04** | 1.26 |
| Risks3: Fear of mistaken identity in general [Lower score is better] | **3.32** | 1.30 | **2.74** | 1.23 |
| Risks4: Fear of being mistaken for someone else of a similar minority ethnicity/gender [Lower score is better] | **3.07** | 1.42 | **2.22** | 1.31 |
| Risks5: Discomfort with the technology [Lower score is better] | **2.77** | 1.41 | **2.07** | 1.33 |
| Risks6: Unsure how it works [Lower score is better] | **2.48** | 1.35 | **1.93** | 1.36 |
| Trust10: The system seems to be intelligent | **3.87** | 1.06 | **2.93** | 1.36 |
| Trust11: The system can recognize human faces just like a real person | **3.41** | 1.27 | **2.59** | 1.01 |
| Trust20: The system is innovative | **4.20** | 1.02 | **3.78** | 1.09 |

**Table 5. All individual significant items by level of experience with means and standard deviations, color coded to show comparative level of acceptance (from red to green in increasing order of acceptance)**

| **Category of System Acceptance** | Naïve |  | Expert |  |
|---|---|---|---|---|
|  | (*N* = 219) |  | (*N* = 27) |  |
|  | ***M*** | *SD* | ***M*** | *SD* |
| **Contexts of Acceptability** (Higher score indicates more acceptability in each context) | **3.78** | 1.39 | **4.48** | 0.89 |
| **Perception of Risks** (Higher score indicates greater perception of risk) | **3.10** | 1.43 | **2.40** | 1.34 |
| **Measures of Trust** (Higher score indicates greater trust) | **3.83** | 1.17 | **3.10** | 1.25 |

**Table 6. Significant measures of system acceptance by level of experience with means and standard deviations, color coded to show comparative level of acceptance (from red to green in increasing order of acceptance)**

| | **Kruskal-Wallis *H*** | ***df*** | ***p*** |
|---|---:|---:|---:|
| Positivity3 | 35.996 | 9 | 0** |
| Positivity5 | 21.418 | 9 | 0.011* |
| Acceptability2 | 28.678 | 9 | 0.001** |
| Acceptability4 | 34.101 | 9 | 0** |
| Acceptability5 | 28.675 | 9 | 0.001** |
| Acceptability6 | 28.684 | 9 | 0.001** |
| Acceptability7 | 42.147 | 9 | 0** |
| Risks1 | 21.109 | 9 | 0.012* |
| Risks2 | 27.643 | 9 | 0.001** |
| Risks4 | 17.719 | 9 | 0.039* |
| Risks5 | 52.066 | 9 | 0** |
| Trust2 | 46.442 | 9 | 0** |
| Trust3 | 41.641 | 9 | 0** |
| Trust5 | 34.022 | 9 | 0** |
| Trust9 | 21.715 | 9 | 0.01* |
| Trust10 | 22.221 | 9 | 0.008** |
| Trust11 | 47.108 | 9 | 0** |
| Trust12 | 37.333 | 9 | 0** |
| Trust13 | 22.96 | 9 | 0.006** |
| Trust14 | 26.73 | 9 | 0.002** |
| Trust15 | 22.651 | 9 | 0.007** |
| Trust16 | 24.263 | 9 | 0.004** |
| Trust17 | 20.855 | 9 | 0.013* |
| Trust18 | 38.818 | 9 | 0** |

* significance at the .05 level (2-tailed); **significance at the .01 level (2-tailed).

**Table 7. Kruskal-Wallis H results**

|  | Russia |  | India |  | Singapore |  | Canada |  | UK |  | USA |  | Others |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | (*N* = 68) |  | (*N* = 63) |  | (*N* = 26) |  | (*N* = 11) |  | (*N* = 61) |  | (*N* = 12) |  | (*N* = 5) |  |
|  | ***M*** | *SD* | ***M*** | *SD* | ***M*** | *SD* | ***M*** | *SD* | ***M*** | *SD* | ***M*** | *SD* | ***M*** | *SD* |
| Positivity3: I believe that the o.vision system is FUN | **3.59** | 1.42 | **3.76** | 1.09 | **3.42** | 1.17 | **2.64** | 1.36 | **2.75** | 1.29 | **2.25** | 1.06 | **3.00** | 1.58 |
| Positivity5: I believe that the o.vision system is ACCEPTABLE to be used by me | **4.03** | 1.30 | **4.21** | 0.97 | **3.73** | 1.12 | **3.18** | 1.40 | **3.38** | 1.51 | **3.25** | 1.22 | **4.60** | 0.55 |
| Acceptability2: I believe that the o.vision system is acceptable as a building entry system in the following context: Halls of residence (student buildings) | **4.31** | 1.14 | **4.14** | 1.11 | **3.81** | 1.27 | **3.82** | 1.33 | **3.18** | 1.52 | **3.33** | 1.67 | **4.00** | 1.73 |
| Acceptability4: I believe that the o.vision system is acceptable as a building entry system in the following context: Schools | **4.22** | 1.23 | **4.22** | 0.99 | **3.85** | 1.29 | **3.45** | 1.51 | **3.20** | 1.50 | **3.08** | 1.44 | **4.40** | 0.89 |
| Acceptability5: I believe that the o.vision system is acceptable as a building entry system in the following context: Offices | **4.22** | 1.10 | **4.41** | 0.93 | **4.04** | 1.18 | **3.36** | 1.50 | **3.48** | 1.46 | **3.08** | 1.51 | **4.60** | 0.55 |
| Acceptability6: I believe that the o.vision system is acceptable as a building entry system in the following context: Shops | **3.01** | 1.64 | **3.27** | 1.36 | **2.92** | 1.52 | **2.36** | 1.80 | **2.15** | 1.44 | **2.17** | 1.27 | **3.20** | 2.05 |
| Acceptability7: I believe that the o.vision system is acceptable as a building entry system in the following context: Factories | **4.12** | 1.30 | **4.30** | 1.06 | **3.73** | 1.28 | **3.00** | 1.73 | **2.95** | 1.52 | **3.00** | 1.60 | **4.80** | 0.45 |
| Risks1: Data security [Lower score is better] | **3.12** | 1.46 | **3.75** | 1.27 | **3.58** | 1.30 | **3.82** | 1.54 | **4.07** | 1.22 | **3.58** | 1.44 | **3.80** | 1.30 |
| Risks2: Data sharing/privacy [Lower score is better] | **3.16** | 1.39 | **3.81** | 1.20 | **3.88** | 1.18 | **3.73** | 1.62 | **4.23** | 1.17 | **4.00** | 1.41 | **4.40** | 0.89 |
| Risks4: Fear of being mistaken for someone else of a similar minority ethnicity/gender [Lower score is better] | **2.49** | 1.39 | **2.98** | 1.28 | **3.00** | 1.44 | **3.64** | 1.43 | **3.23** | 1.54 | **3.33** | 1.37 | **4.00** | 1.00 |
| Risks5: Discomfort with the technology [Lower score is better] | **2.01** | 1.30 | **2.40** | 1.24 | **2.65** | 1.23 | **3.73** | 1.27 | **3.39** | 1.33 | **3.50** | 1.31 | **3.20** | 2.05 |
| Trust2: The system is dangerous [Reverse scored] | **4.18** | 1.11 | **3.97** | 1.00 | **3.54** | 0.90 | **3.27** | 1.19 | **3.05** | 1.22 | **3.00** | 1.28 | **3.20** | 1.48 |
| Trust3: The system is trustworthy | **3.88** | 1.06 | **3.67** | 0.88 | **3.62** | 0.90 | **2.82** | 1.08 | **2.90** | 1.04 | **2.75** | 1.29 | **2.60** | 1.14 |
| Trust5: I am at the system's mercy [Reverse scored] | **3.71** | 1.40 | **3.02** | 1.41 | **3.00** | 1.26 | **2.36** | 1.21 | **2.67** | 1.29 | **1.92** | 1.00 | **1.80** | 0.84 |
| Trust9: I mistrust the system's purpose [Reverse scored] | **3.97** | 1.20 | **4.03** | 0.97 | **3.88** | 0.82 | **2.91** | 1.22 | **3.41** | 1.42 | **2.92** | 1.51 | **2.80** | 1.48 |
| Trust10: The system seems to be intelligent | **3.54** | 1.32 | **4.24** | 0.69 | **3.92** | 0.89 | **3.45** | 1.29 | **3.61** | 1.20 | **3.42** | 1.08 | **3.60** | 1.67 |
| Trust11: The system can recognize human faces just like a real person | **2.74** | 1.27 | **4.00** | 0.92 | **3.73** | 0.96 | **3.73** | 1.27 | **3.00** | 1.32 | **3.33** | 1.15 | **3.60** | 1.67 |
| Trust12: The system has integrity | **3.76** | 1.12 | **3.60** | 0.87 | **3.50** | 0.95 | **2.91** | 1.30 | **2.74** | 1.15 | **2.58** | 1.16 | **2.20** | 1.30 |
| Trust13: I am wary of the system [Reverse scored] | **3.57** | 1.31 | **3.68** | 1.06 | **3.54** | 1.07 | **2.82** | 1.54 | **2.84** | 1.36 | **2.50** | 1.31 | **3.40** | 1.67 |
| Trust14: I am suspicious of the system's intent, action, or outputs [Reverse scored] | **3.84** | 1.23 | **3.87** | 1.10 | **3.62** | 0.98 | **2.45** | 1.21 | **3.21** | 1.38 | **2.58** | 1.31 | **3.60** | 1.34 |
| Trust15: The system's actions will have a harmful or injurious outcome [Reverse scored] | **3.94** | 1.16 | **3.98** | 1.11 | **3.88** | 0.91 | **3.36** | 1.12 | **3.28** | 1.28 | **3.00** | 1.13 | **3.80** | 1.10 |
| Trust16: I am confident in the system | **3.65** | 1.17 | **3.79** | 0.88 | **3.54** | 0.99 | **2.82** | 1.25 | **3.00** | 1.18 | **3.00** | 1.13 | **3.20** | 1.48 |
| Trust17: The system provides security | **3.94** | 1.12 | **4.11** | 0.86 | **3.92** | 0.89 | **3.55** | 1.21 | **3.54** | 1.01 | **3.58** | 1.16 | **3.60** | 1.67 |
| Trust18: The system is dependable | **2.76** | 1.13 | **3.83** | 0.91 | **3.46** | 0.76 | **2.82** | 1.25 | **3.25** | 0.92 | **3.67** | 0.89 | **3.20** | 1.48 |

**Table 8. All individual significant items by country of residence with means and standard deviations, color coded to show comparative level of acceptance (from red to green in increasing order of acceptance)**

| **Category of System Acceptance** | **Russia** | | **India** | | **Singapore** | | **Canada** | | **UK** | | **USA** | | **Others** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | (*N* = 68) | | (*N* = 63) | | (*N* = 26) | | (*N* = 11) | | (*N* = 61) | | (*N* = 12) | | (*N* = 5) | |
| | ***M*** | *SD* | ***M*** | *SD* | ***M*** | *SDV* | ***M*** | *SD* | ***M*** | *SD* | ***M*** | *SD* | ***M*** | *SD* |
| **Positivity of Beliefs** (Higher score indicates more positive beliefs) | **3.81** | 1.37 | **3.98** | 1.05 | **3.58** | 1.14 | **2.91** | 1.38 | **3.07** | 1.43 | **2.75** | 1.22 | **3.80** | 1.40 |
| **Contexts of Acceptability** (Higher score indicates more acceptability in each context) | **3.98** | 1.38 | **4.07** | 1.17 | **3.67** | 1.35 | **3.20** | 1.60 | **2.99** | 1.55 | **2.93** | 1.51 | **4.20** | 1.32 |
| **Perception of Risks** (Higher score indicates greater perception of risk) | **2.69** | 1.46 | **3.23** | 1.37 | **3.28** | 1.36 | **3.73** | 1.42 | **3.73** | 1.39 | **3.60** | 1.36 | **3.85** | 1.35 |
| **Measures of Trust** (Higher score indicates greater trust) | **3.65** | 1.27 | **3.83** | 1.02 | **3.63** | 0.97 | **3.02** | 1.26 | **3.11** | 1.25 | **2.94** | 1.24 | **3.12** | 1.42 |

**Table 9. Significant measures of system acceptance by country of residence with means and standard deviations, color coded to show comparative level of acceptance (from red to green in increasing order of acceptance)**

**Ranks**

| | **Level of Experience** | **N** | **Mean Rank** | **Sum of Ranks** |
|---|---|---|---|---|
| **Trust_SCORE** | Expert | 27 | 29.24 | 789.5 |
| | Naive | 41 | 37.96 | 1556.5 |
| | **Total** | **68** | | |

**Test Statistics**

| | **Mann-Whitney *U*** | **Wilcoxon *W*** | **Z** | ***p*** |
|---|---|---|---|---|
| **Trust_SCORE** | 411.5 | 789.5 | 1.781 | 0.075 |

Grouping Variable: Expert-Naive

**Table 10. Mann-Whitney U test results on Trust Score using Expert/Naive as a grouping variable on data from only Russia**

### Research Question 3: Trust in the System as a Function of Personality and LOC

As also used above, the 20-item trust scale was scored to achieve a single Trust Score for each participant. A hierarchical multiple regression was carried out to determine the impact of the Big Five Inventory (BFI) and Locus of Control (LOC) on Trust Scores.

First, a regression analysis was conducted to measure the impact of the Big Five personality traits on trust. In step 1, a significant relationship was found between the BFI and the measure of trust on three of the five dimensions: Agreeableness, Neuroticism, and Openness ($F(5, 240) = 4.563$, $p = .001$; agreeableness $\beta = .148$, $p = .041$; neuroticism $\beta = -.166$, $p = .025$; openness $\beta = .133$, $p = .035$). This indicates that as levels of agreeableness and openness increase and levels of neuroticism decrease, trust ratings increase. In addition, a significant relationship was found between LOC and the measure of trust separately ($F(1, 244) = 7.416$, $p = .007$; LOC $\beta = .172$, $p = .007$). This indicates that as levels of LOC increase, trust ratings increase. Results for Step 1 are summarized in Tables 11 and 12.

In step 2, LOC was added to the regression analysis. All six measures together were shown to be a significant predictor of trust ($F(6, 239) = 3.933$, $p = .001$), however when combined with the BFI, LOC was not shown to be a significant predictor (LOC $\beta = .071$, $p = .373$). Thus, Locus of Control was not found to contribute significantly to the predictive algorithm, although individually significant. Results for Step 2 are summarized in Table 13.

In order to isolate the measures that most closely predict trust, a Pearson Correlation was carried out using all measures of the BFI along with LOC. It was found that LOC correlated at a highly significant level with all five measures of the BFI (LOC and Extraversion $r = .226$, $p < 0.001$, LOC and Agreeableness $r = .164$, $p = .010$, LOC and Conscientiousness $r = .484$, $p < 0.001$, LOC and Neuroticism $r = -.429$, $p < 0.001$, LOC and Openness $r = .266$, $p < 0.001$). Findings are summarized in Table 14.

### Qualitative Responses

Through the open ended questions, Expert users readily offered more suggestions for settings to replace existing security systems with a facial recognition system, quoting a variety of settings and explanations of convenience - “In cases of use in large offices - reduces travel time” (Participant number 225, from a collectivist country), and “Universities. Some universities, for example LETI, use a pass system with a card. You can forget them.” (P220, collectivist). Experts identified exactly one additional risk associated with the system - the possibility of twins being confused for one another, and overwhelmingly stated that they would recommend the system to a friend. Most did not identify any links between the technology and COVID-19 situation, with the few who did mentioning that it boosted their sense of safety, and feeling that a temperature scan would be particularly useful in these times. In contrast, Naive participants qualified their suggestions for replacing existing security systems with facial recognition-drive systems by mentioning barriers of cost, privacy, complexity of installation, power failures, and user discomfort. Nearly every suggestion included conditions and issuances of doubt, such as in this response: “I believe facial recognition could feasibly completely replace other access systems in all buildings, however I don't think it is worth the time and effort to do so. Realistically, I believe facial recognition should only be implemented in medium-high security areas, such as airports. Also, I would personally not feel at ease if facial recognition was used everywhere-- it would make me feel that all my movements were being openly recorded, as if I were in some Orwellian dystopia. I am sure I am not the only one with this belief.” (P37, collectivist) Naive participants also identified additional risks associated with the system not previously mentioned on the questionnaire, such as database maintenance costs and storage space, issues with face coverings, over-reliance on technology, difficulty in replacing the system in the case of a hack or breach, and a loss of social contact. Naive participants were overwhelmingly inclined to recommend the system to a friend, but qualified that they would investigate the cost of setup and the level of security available before doing so. Naive participants responded with a variety of thoughts on the state of facial recognition in 2020, noting advantages such as reduced contact and quick access granting as linked to social distancing and fewer health risks. They also expressed some measures of doubt, linking the propensity for facial recognition systems to misidentify people of minority races to the Black Lives Matter protests and renewed cultural awareness around racism taking place at the time, and noting that face coverings and masks can cause the technology to falter.

Many participants from Individualistic countries stressed that their most pressing concern with the system was with cyber security and the loss of privacy, such as in this response: “risk of negative opinion being associated with the organisation using the system. e.g. 'Are they trying to spy on me'” (P191, individualistic). Among these participants, responses relating the system to the climate in 2020 were more likely to mention distrust of facial recognition technology due to issues or racism and discrinination than to mention the opportunity to have a low-contact entry granting system during a pandemic. Participants were also very likely to recommend the system to a friend, but highlighted the need to be familiar with the ins and outs of the system before doing so - “Not until I know more about it myself” (P106, individualistic).

**ANOVA**

| | *df* | *F* | *p* |
|---|---|---|---|
| Regression | 5 | 4.563 | 0.001** |
| Residual | 240 | | |
| Total | 245 | | |

**Coefficients**

| | *β* | *t* | *p* |
|---|---|---|---|
| Extraversion | -0.068 | 1.025 | 0.307 |
| Agreeableness | 0.148 | 2.058 | 0.041* |
| Conscientiousness | 0.028 | 0.407 | 0.685 |
| Neuroticism | -0.166 | 2.261 | 0.025* |
| Openness | 0.133 | 2.125 | 0.035* |

* significance at the .05 level; **significance at the .01 level

**Table 11. Linear Regression results showing the relationship between the BFI and Trust**

**ANOVA**

| | *df* | *F* | *p* |
|---|---|---|---|
| Regression | 1 | 7.416 | .007* |
| Residual | 244 | | |
| Total | 245 | | |

**Coefficients**

| | *β* | *t* | *p* |
|---|---|---|---|
| Locus of Control | 0.172 | 2.723 | 0.007 |

* significance at the .05 level; **significance at the .01 level.

**Table 12. Linear Regression results showing the relationship between LOC and Trust**

**ANOVA**

| | *df* | *F* | *p* |
|---|---|---|---|
| Regression | 6 | 3.933 | 0.001** |
| Residual | 239 | | |
| Total | 245 | | |

**Coefficients**

| | *β* | *t* | *p* |
|---|---|---|---|
| Extraversion | -0.072 | 1.073 | 0.284 |
| Agreeableness | 0.16 | 2.185 | 0.03* |
| Conscientiousness | 0 | 0.004 | 0.997 |
| Neuroticism | -0.14 | 1.783 | 0.076 |
| Openness | 0.115 | 1.74 | 0.083 |
| Locus of Control | 0.071 | 0.893 | 0.373 |

* significance at the .05 level; **significance at the .01 level.

**Table 13. Linear Regression results showing the relationship between the BFI and LOC considered together, and Trust**

**Correlations**

| | *M* | *SD* | Extraversion | Agreeableness | Conscientiousness | Neuroticism | Openness |
|---|---|---|---|---|---|---|---|
| Extraversion | 26.43 | 5.30 | | | | | |
| Agreeableness | 34.19 | 5.26 | .267** | | | | |
| Conscientiousness | 32.74 | 5.54 | .200** | .358** | | | |
| Neuroticism | 21.44 | 6.08 | -.329** | -.449** | -.357** | | |
| Openness | 36.88 | 5.41 | 0.105 | 0.069 | 0.07 | 0.036* | |
| Locus of Control | 99.30 | 11.44 | .226** | .164** | .484** | -.429** | .266** |

* Significance at the .05 level (2-tailed); ** Significance at the .01 level (2-tailed).

**Table 14. Pearson correlations between each of the dimensions of the BFI and the LOC, with means and standard deviations**

Participants from Collectivist countries felt positively about the possibility of switching out an existing security system with a facial recognition-based system, though mentioned aspects of community and larger social structures more often, such as “Difficulty would be depend[e]nt on the country's regulations, whether ownership is public or private” (P31, collectivist), and “This can be done with [a] little bit of convincing the residents” (P25, collectivist). Participants were most concerned about potential failures of the technology, such as power outages and security breaches, as well as the burden of introducing a new system to an existing community - “Visitors entry experience will not be great if they are not used to such systems” (P102, collectivist). Participants were very likely to want to recommend the system to others, responding by predicting their friends’ responses in turn - “I would definitely share the details about O.vision, however, it’s very difficult to change people’s mindset, as this is something new” (P108, collectivist). Participants were very enthusiastic about the role the system can play in the climate of 2020, mentioning various ways in which those working and studying during the COVID-19 pandemic can feel safe with a system that requires no contact and works rapidly.

### Questionnaire Reliability

Cronbach’s Alpha revealed the questionnaire to have acceptable internal consistency, $\alpha = 0.80$. Most items from the questionnaire considered when measuring system acceptance were found to be worthy of retention. All items from questions 8 and 13 were not found to be reliable, but were excluded  nonetheless as their only role was to prompt participant reflection and prime them for the main questions. However four items from the measure of Perception of Risks (Question 15) - Risks1, Risks2, Risks3, and Risks5 - as well as eight items from the Trust scale (Question 18) - Trust2, Trust4, Trust5, Trust7, Trust9, Trust13, Trust14, and Trust15 were found to lower reliability of the overall questionnaire. As the Cronbach’s Alpha was run after the analyses were completed, these items were not removed in the present study, but future analyses may benefit from removing these items.

## 6. DISCUSSION

The results of the study show a marked difference in attitudes by experience with the system, as well as differences in system acceptance by individual countries and patterns along the dimensions of collectivism and individualism. Furthermore, personality traits were shown to be a predictor of trust in the system, and qualitative responses by participants echoed the sentiments displayed in the numbers. In this section, the implications of these results will be more closely examined.

### System Acceptance and Experience

The findings showed a significant difference in perception between the experienced participants and the naive participants on 9 of the 39 statements (23%), under the categories Contexts of Acceptability, Perception of Risks, and Measures of Trust. None under Positivity of Beliefs were found to have a significant difference. Of the 9 that were found to be significant, the results indicate a slight variation in behavior by experience level. Interestingly, experienced users of the technology were more widely accepting of the technology and less concerned with risks, but trusted the system less than naive, completely inexperienced participants did. This is perhaps because expert users are familiar with the system and its workings and thus do not find it as “intelligent” - they do not have any unrealistic expectations. Revisiting the Uncanny Valley model, Gursoy et al [34] and Troshani et al [93] found system acceptance of AI devices to be context dependent, and to rely strongly on perceptions of anthropomorphism and emotion. In their studies, participants based their acceptance of AI on their personal schemas of what they expected in contexts like healthcare and self-service machines, and what they were familiar with and needed from a system. Attitudes of AI acceptance are thus personal choices. It is likely that experienced users of the o.vision system have built familiarity and made peace with the dissonance between the system’s appearance and function, and have experienced firsthand the effectiveness and convenience of its usage. They are familiar with its presence in their vicinity, finding it more acceptable as a security system in a student residence than naive participants did. This is perhaps explained in part by the fact that a large proportion of the expert users surveyed are students living in residences where the o.vision system is currently in use.

Of the risks mentioned in the questionnaire that showed a difference in perception between experienced and naive participants, the greatest distinction was found for the risk “Unsure how it works”, easily explained by the knowledge gap between a current user and an individual who has never encountered the system. Experienced users were less concerned than naive participants with a “Fear of mistaken identity in general” and “Fear of being mistaken for someone else of a similar minority ethnicity/gender”, likely due to having already used the system and being aware of its success rate. This likely also reflects the ethnic makeup of Russia - the present study did not collect information regarding participant ethnicity, but Russia’s ethnic makeup is fairly homogeneous, and this may explain the lack of concern for the latter risk. This is notable, as the literature lists a number of risks that remain prevalent with nearly any facial recognition system, as displayed most notably with tests on Microsoft, IBM, and Google’s systems by Barsan [9]. The o.vision system states a success rate of nearly 100%, and it is possible that since it only conducts simple identity management as opposed to complex facial feature parsing, its users do not associate a number of primary risk factors with this system. Both naive participants and experienced users showed low "Discomfort with the technology", with experienced users being slightly less concerned than naive participants - this suggests a baseline openness to the technology among those sampled. Interestingly, both naive and experienced users were concerned about the risk of "Data Sharing/Privacy", though experienced users were less concerned than naive users. Naive users are likely concerned about this risk as it applies to facial recognition technology in general, while experienced users are likely more concerned in practice, as their data is already in use to make the system function.

On the Trust scale, experienced users found the system less "intelligent" and less capable of "recognizing human faces just like a real person". Both groups found the system innovative, more so with the naive users. This displays a vote of confidence for the system, with both groups finding the technology effective in theory and in practice, but the experienced users harboring no false expectations regarding its functioning, having actually used it and grown accustomed to it.

A large number of items on the questionnaire were not found to have a significant difference in perception by experience, including four other Contexts of Acceptability (Offices, Airports, Personal Device Security, and Residential Security), one Risk (Data Security), and a number of items on the measure of Trust. In addition, there was no significant difference found at all on any items representing Positivity of Beliefs, including finding the system "Fun", "Useful", "Expensive", "Easy to use" and "Acceptable to be used by me". Most notably among the items that did not indicate a significant difference are a large number of items on the Trust scale, including "The system is trustworthy", "The system is a reliable access granting system", and "The system has integrity". It appears that experience using a facial recognition system does not dispel all worries about its trustworthiness.

A significant difference between groups on 23% of the items considered as variables represents a fairly weak difference between the groups overall, though the items that showed a difference were decisive in their distinction. Thus experience using a facial recognition system impacts some aspects of system acceptance by reducing concerns about most risks except for Data Security, being seen as acceptable in the context of use, and finding the system innovative. However, experienced users are still not quick to trust the system overall, and display more wariness in some areas than users with no experience using the system at all.

### Variation by Country of Residence

The findings showed a significant difference in perception between the experienced participants and the naive participants on 24 of the 39 statements (61.5%), under all 4 categories considered: Positivity of Beliefs, Contexts of Acceptability, Perception of Risks, and Measures of Trust. Of the 24 that were found to be significant, the results indicate a prominent variation in behavior by country of residence. The trend overall points to a clear distinction between attitudes reported by collectivist countries (India, Russia, Singapore) and those reported by individualist countries (the USA, the UK, and Canada). Collectivist countries were more accepting of the system on the whole than individualist countries, with Singapore being slightly less accepting than India and Russia. The collectivist countries were more positive towards the system than the individualist ones, finding it more "Fun" and still more "Acceptable to be used by me". The individualist countries were also fairly positive towards the system on the latter, with scores above 3 on all counts. A significant difference was not found on the items "Useful", "Easy to Use", and Expensive". Thus, issues of practicality around cost and usefulness once installed were not considered heavily by the groups of countries, while issues of openness and acceptance were significantly - all participants were reasonably interested in the system and felt open to use it, though participants from collectivist countries expressed greater openness and acceptance. This difference is likely due to the cultural difference in societal attitudes, with collectivist countries being more collaborative and open to group experiences and systems that can benefit the group [43].

Among Contexts of Acceptability, most items showed a significant difference between countries - "Student Residences", "Schools", "Offices", "Shops", and "Factories". Three items did not show a significant difference: "Airports", "Homes", and "Secure buildings". Collectivist countries once again scored higher on each of the items, with Singapore scoring slightly lower than Russia and India. Overall, participants from all countries overwhelmingly found shops to be the least acceptable context for facial recognition technology, likely due to the low need for a security-based system in such a public area, and the discomfort with large numbers of entrants being scanned without explicit consent. Once again, it is likely that participants from collectivist countries felt more open to facial recognition systems as security systems in a number of contexts as they would serve the larger group as a security system that works for all, despite any personal discomfort. Participants from individualistic countries were likely more concerned with their own comfort and approval, and marked each option as so [43]. It is notable that there was no significant difference between the groups of countries on using facial recognition in airport settings or in the home.

In line with the pattern thus far, participants from collectivist countries were less concerned with a variety of risks than were those from individualistic countries. Across both groups, there was concern with the risks of "Data Security" and "Data Sharing/Privacy" than there was for "Fear of being mistaken for someone else of a similar minority ethnicity/gender" and "Discomfort with the technology". No significant differences between groups were found for the risks "Fear of mistaken identity in general" and "Unsure how it works". Interestingly, the countries of Singapore, the USA, the UK, and Canada were more concerned with "Fear of being mistaken for someone else of a similar minority ethnicity/gender" than were India and Russia, with scores above 3 versus scores below 3. This could likely be attributed to the relative ethnic homogeneity of Russia and India as compared to the other 4 countries. The USA and the UK were most concerned about Data Security and Data Sharing, scoring each of the two at or near 4 out of 5 points. This is likely due to the recent discussions surrounding data rights and privacy in both of these countries that have since become a global talking point. As individualistic societies, concerns regarding personal security and self-preservation would be weighed higher than such concerns in collectivist countries, where the needs of the group are put in front of those of the individual. 13 of the 20 items of the Trust measure were found to have a significant difference by country, including "The system is dangerous" (reverse scored), "The system seems to be intelligent", and "The system provides security". The items that did not show a significant difference include "The system's mode of operation is obscure", "The system is reliable", and "The system is innovative". Of the 13 items, India was the most trusting of the system of the countries, and the USA was the least trusting. This pattern holds throughout the significant items, with India showing the greatest system acceptance overall, and the USA showing the lowest system acceptance. In addition to the differences in individualism between the two countries, this is likely also due to the information technology-heavy economy and culture in India weighed against the racial diversity and concern with technological privacy and security in the United States.

A significant difference between groups of countries on 61.5% of the items considered as variables represents a fairly strong difference between the groups overall, with the distinctions between collectivist and individualistic countries being decisive as well. With minor variation on specific items among countries within groups, overall collectivist countries were more open and accepting of the system, being open to more contexts of use and being less concerned about common risks and trusting the system more than did participants from collectivist countries. This is in line with the literature, particularly with Hornik and Tupchiy's [47] findings that collectivist countries prioritize benevolence and conformity (and thus see the system for what it can offer) and that individualistic countries prioritize individual self-direction and power (and thus are hesitant to quickly trust a strange system without an opportunity to form their own detailed opinions). Overall, India was the most accepting, and the USA was the least accepting. Certain items across the scale of system acceptance stood out across all considered countries, including a lack of acceptance of facial recognition technology in shops, a collective concern regarding data security and data privacy, and the sense of feeling "at the system's mercy". These illustrate concerns with system acceptance that shatter divisions between cultures, pointing to global attitudes that should be paid attention to. On the whole, collectivist cultures were more accepting of facial recognition technology, likely due to their tendencies towards strong in-group ties and loyalty towards their own. The system offers an opportunity to safeguard buildings and communities, and in the light of such protection and efficiency, personal concerns and risks fall by the wayside. In contrast, individualistic cultures are less trusting to begin with, and trained to protect themselves first. As such, concerns with risks become more salient when they threaten the individual, and trust and acceptance fall. In addition, the cultural conversation in the year 2020 heavily criticizing facial recognition technology has undoubtedly played a part in shaping the attitudes of most respondents, and would be most likely to impact the responses by those from individualistic countries who feel permitted to express these.

When data from Russia was isolated, and trust in the system compared by experience level (Expert and Naive), no significant difference was found between the groups. This is noteworthy, as it suggests that the influence of culture and country impacts the proclivity for trusting a system more heavily than experience with the system itself does. These results are useful in offsetting the fact that the sample only includes Expert data from Russia (as it is the only country in which the system is currently in use), and that in cross-cultural comparisons, Russian data was the only one to include Experts in the sample. As no significant difference was found on trust, it suggests that the cross-cultural tests conducted hold true, without much loss in validity from this distinction. However, these results must be taken with a grain of salt, as the sample size is fairly small (with a total of 68 Russian participants), and the Expert and Naive samples being quite uneven (27 and 41 participants, respectively). In addition, these results only measured a difference in Trust and not on system acceptance as a whole, and only considered data from Russia. It plants a seed for future research in this vein comparing data on experience by country for a variety of countries.

### Personality Traits and LOC on Trust

The findings showed a significant influence of personality on trust in the system, on three of the five dimensions of the

BFI: Agreeableness, Neuroticism, Openness. Agreeableness and Openness positively predict trust, while Neuroticism negatively predicts trust. Thus, high levels of curiosity and willingness to try new experiences, as well having a more amiable, pleasant, and considerate personality causes one to trust the system more. It follows that individuals who would readily try something unfamiliar and are open to the benefits that the system could provide would be more trustful. High levels of neuroticism suggest increased anxiety, worry, stress, a decreased ability to deal with frustrations, and a tendency against delayed gratification. It thus follows as well that these tensions would obfuscate any benefits of the system and lay bare the potential for things to go wrong. As a result, high levels of neuroticism predict lower trust in the system. Interesting, conscientiousness and extraversion were not found to impact trust.

In addition, the Locus of Control (as measured by the ICI) was found to be a significant predictor of trust as well. Individuals with a higher score on the ICI (and thus a more internal locus of control) positively predicted trust in the system. An internal locus of control signifies that an individual believes that their life is within their control, and that they have power over the happenings around them. Individuals with a more external locus of control would be inclined to think the worst of the system, believing that anything may go wrong with its operation and negatively serve themselves and the people around them. In contrast, individuals with a more internal locus of control would be aware of the risks, but conscious of their own power over the systen's usage and their ability to evade any sticky situations. It thus follows that this would lead to greater trust in the system.

These findings stand in line with Sharan and Romano's findings [87]. They found that the Locus of Control has a strong moderating influence on trust (as measured via reaction time in their study). Similarly, the present study found that the locus of control had a very strong link to trust, stronger still than the influence of the BFI. Sharan and Romano [87] also found that the BFI predicted trust, with neuroticism and extraversion predicting trust. This study found a link between neuroticism and trust as well, but did not find a significant link between extraversion and trust. Instead, agreeableness and openness were found to predict trust.

The findings on the influence of personality traits (as measured by the BFI and ICI) on trust being in line with the previous literature reveals construct validity in our measure of the trust. The 20-item trust scale that was adapted from previous research holds strength, and may be adapted further and reused to study trust in technology [52, 25, 10].

Interestingly, when both the dimensions of the Big Five were considered alongside Locus of Control regarding their influence on trust, only Agreeableness was found to significantly predict trust, and locus of control no longer significantly predicted trust. This suggested that there is a level of overlap and close correlation between the two measures, as they are significant predictors separately, but appear to cancel each other out when combined. In order to ascertain this close relationship, a Pearson correlation was carried out and confirmed this theory. Thus, the ICI and the BFI are distinct measures, but are closely correlated and measure traits that align with each other. These may not be similar traits, but are traits that are linked in a manner that causes them both to predict trust in the same direction.

### Limitations

A pronounced limitation of the present study were the numerous disparities in the splits in sample sizes. The population of Expert and Naive participants differed by over a factor of eight, with significantly more Naive than Expert participants. In addition, the sample sizes of participants from each country varied significantly, with many more participants from Russia and India than from Canada. As a result, there were significantly more data points from collectivist countries than from individualist countries This was caused in part due to the fact that the technology is only available in a limited number of settings in Russia, and that data collection was made difficult during the COVID-19 pandemic that limited international travel and in-person interaction. These incongruities affect the external validity of the study, as they may have caused an imbalance in the weightage of the results.

As an extension of this limitation, all Expert participants were conspicuously from Russia. This both affected the data on country of residence from Russia (as it was the only one of the datasets among all countries that included users of the actual technology), and caused all data on experienced users to be necessarily impacted by Russian cultural norms. A study of experience within only the data collected from Russia was conducted to offset this slightly, but this test was subject to small and uneven sample sizes as well. In order to better understand the impact of experience on system acceptance, it would be prudent to collect data from current users from different countries once the technology has been installed outside of Russia. Another consequence of the global nature of the sample was that Russian participants completed a Russian translation of the questionnaire, and there is always a possibility of mistranslations and misunderstandings when language is concerned, particularly with complex sentences such as "I am at the system's mercy". All other participants having to be fluent English speakers also precludes inclusion of a truly global sample.

In the present study, the Naive participants were not actually exposed to the system in person at all. Seeing a picture of facial recognition technology through a screen may not be an impactful enough experience to elicit a realistic reaction towards the system. More powerful responses in the measurement of system acceptance could be elicited from an in-person study or a simulation-based study that sets participants up to use facial recognition technology for some time before responding to attitudinal measures for a more accurate impression of values. Self-report measures hold limited viability, and the entirety of the present method relied on a self-reported questionnaire. This markedly affects the internal validity of system acceptance, and each of the measures under the umbrella of acceptance: Positivity of Beliefs, Contexts of Acceptability, Perception of Risks, and Measures of Trust. The fully digital nature of this study was another consequence of the COVID-19 ecosystem, and impacts the ecological validity of the results.

Finally, Cronbach's Alpha for the questionnaire was conducted after analyses were completed, and several items included in the analysis were shown to lower reliability of the scale. These items were exclusively from the scales measuring Perception of Risks and Trust, and several of these items were found to be significant in the present study. This study could benefit from a repeat of the analyses that excludes these items from the dataset.

### Implications for the Design of Facial Recognition Technologies

The results of this study hold implications for both psychology and design. An increased understanding of some of the predictors of trust and system acceptance offer us a window into how the o.vision system and facial recognition technology more widely are perceived. The results suggest that experience using a system is helpful in warming up to it, though trust may actually be adversely affected by experience. Several elements of personality impact attitudes towards such technology, and the dimensions of one's country of residence and cultural background strongly impact how such technology is seen and the general openness towards it.

The present study was conducted with the help of the o.vision company, which has established its technology in certain settings in Russia, but is in the process of expanding its operations to the United Kingdom and trialing entry systems that may be adopted by large, multinational corporations and public services in large metropolitan areas. In addition, other companies developing systems in the space of facial recognition technology are increasingly expanding into airports and private developments around the world [2]. There is thus an urgency of need to practically understand how to mitigate risks and address public concerns in a manner that encourages acceptance. This would enable issue-free installation, should the development of the technology and the legal processes allow for it. The findings of the present study suggest a few starting points. To combat dissonance as described in the Uncanny Valley model, designers could make minor changes to make the system appear "friendlier", perhaps incorporating a different forward facing appearance, and a UI with an animated avatar that "welcomes" the user. Less clinical and "watchful" appearances could be trialed in a design study to better understand attitudes towards the physical appearance of the system. For example, RoMa - a Robotic Mannequin developed for the fashion merchandising industry was designed to closely mimic an appealing human appearance in order to "promote customer appeal" [4]. In homes, small robotic appliances are being designed to make use of human emotions and simulated facial expressions and body language that their users will recognize in order to facilitate a closer bond with their users [89]. In urban environments, sensors designed to be anthropomorphic and zoomorphic inspired greater trust and engagement, while more robotic or less visible designs created anxiety and caused rejection [51]. In video games, this principle is often used for the opposite, with characters intended to be scary missing common human features such as eyes and noses [91].

In a social context, it appears useful to draw on social circles and larger communities when piloting such systems. A better understanding of the primary personality traits in a particular industry or location would be helpful in understanding how marketing materials and introductory teachings could be adapted to facilitate maximum trust. In collectivist societies, it may be helpful to establish a wide network of use in order to create and strengthen collective trust in the technology. Experience using the system is helpful, and thus having the system present somewhere in a user's environment increases the likelihood of them being comfortable with it elsewhere, and recommending it in place of other security technology. In order to maintain trust over time, knowledge and transparency is helpful. An attempt to educate users about the system's workings and be open about data privacy and security may go a long way in fostering system acceptance and encouraging positivity of attitudes.

### Recommendations for Future Research

The findings of the present study represent a starting point for further research on the impact of experience, culture, and personality on attitudes towards facial recognition technology specifically. Future research could explore other cultural dimensions as proposed by Hofstede's [43] in addition to Individualism, including the Power distance index, Uncertainty avoidance, and Long-term orientation vs. Short-term orientation. These could impact attitudes towards city-wide deployment of entry systems that are biometric and facial recognition-based. In a cultural context, it would also be prudent to compare expert users in multiple countries to better understand how expertise and novelty affect trust, and any interaction effects or interplay of cultural norms with experience. These would be particularly interesting to study in a long-term context, to view the effects of time on system acceptance and trust. Considering that the present study involves Expert users solely from Russia, a companion study involving participants from an individualistic country would be interesting to compare. As an extension, it would be compelling to directly compare system acceptance by country AND personality at the same time, and measure the interaction between the two. Perhaps the differences by country as found in the present study may be explained by the personality traits of residents of the country.

As mentioned in the previous section, in-depth interviews with naive and expert users may be conducted and analyzed, geared towards a design study that addresses the look and feel of facial recognition technology. It may be useful to employ the present findings to propose adaptations to the appearance, functionality, and perhaps education and perhaps more educational and encouraging marketing around the system, and measure changes towards attitudes. It would also be critical to study "expert" users of different facial recognition systems other than solely the o.vision Face Gate, to understand more generalized attitudes towards facial recognition technology as a whole, and control for any specific reactions to the o.vision technology's design and functionality.

The present study proposes a scale measuring trust in technology adapted from elements of previous scales based on extensions of the TAM. This novel scale encompasses a number of dimensions of trust isolated from previous studies, and was shown to be a strong measure of trust specifically when applied to facial recognition systems. This scale may be reused and further adapted in future work measuring system acceptance. In particular, items on the trust scale that were found to lower reliability through Crinbach's Alpha can be removed to further strengthen the measure.

As was briefly visited in the present study, it would captivating as well to study specifically the impact of COVID-19, and how it has shaped system acceptance. A few participants stated that the pandemic caused them to view the system in a more useful light, and found its ability to conduct temperature checks a positive influence on public health. Alongside these positive attitudes were those concerned with masks serving as obstacles to the technology, and the potential for widespread use of facial recognition to become too acceptable too quickly due to a public health scare. Such issues may be studied more closely to better understand how the events of 2020 have shaped our collective attitudes towards facial recognition technology moving forward.

## 7. CONCLUSION

This study set out to understand the impact of experience, culture, and personality traits on system acceptance of a facial recognition system. A measure of system acceptance was developed that studied a number of factors that influence acceptance, including trust. Studying users of the o.vision Face Gate system alongside non-users from a number of countries, it was found that experience positively impacts some aspects of system acceptance, though it adversely affects system trust. The cultural dimensions of an individual's country of residence plays a significant role in determining system acceptance, as individuals from collectivist countries are more likely to be open to the system and less preoccupied by risks, while individuals from individualistic countries are more wary of the system, and less likely to openly accept its usage. It appears that culture more strongly affects acceptance than does experience using the technology.

Moreover, it was found that personality traits (as determined by the three dimensions of the Big Five personality inventory as well as locus of control) are predictive of trust in the system. Moving forward, the interplay between culture and personality may be studied to better understand the roots of system acceptance, as well as perhaps a longitudinal look at experience and its developing impacts on system acceptance and trust.

With the o.vision technology's impending expansion into a number of facilities, and the increased ubiquity of facial recognition technology worldwide, these insights into system acceptance hold a valuable key towards understanding large-scale public reactions towards facial recognition systems. A closer examination of adaptations to the design of these systems and the ways in which they are presented and their data used may provide sage guidelines for discussing and implementing facial recognition technology between the creators of these technologies, legislators, and the public as a whole.

## ACKNOWLEDGMENTS

I would like to sincerely thank my supervisor, Daniela Romano, for her tireless guidance and teachings throughout the course of this study. I would also like to thank Daniel Sozonov, without whom this study would not have had legs that carried us all the way to Russia and back, and Priscilla Wong, who guided me through the thick and thin of writing. I am grateful to all those who participated in my questionnaire, and would like to finally thank my family and friends for their support and constancy throughout my MSc research.

## REFERENCES

1. Kibrom A. Abay, Garrick Blalock, and Guush Berhane. 2017. Locus of control and technology adoption in developing country agriculture: Evidence from Ethiopia. Journal of Economic Behavior & Organization 143, (November 2017), 98–115. DOI:https://doi.org/10.1016/j.jebo.2017.09.012
2. Ada Lovelace Institute. 2019. Beyond face value: public attitudes to facial recognition technology. Ada Lovelace Institute. Retrieved August 18, 2020 from https://www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology/
3. Icek Ajzen and Martin Fishbein. 1980. Understanding Attitudes and Predicting Social Behavior. Prentice-Hall.
4. Minoo Alemi, Ali Meghdari, Ehsan Saffari, Ahmad Zibafar, Leila Faryan, ALi Ghorbandaei Pour, Amin RezaSoltani, and Alireza Taheri. 2017. RoMa: A Hi-tech Robotic Mannequin for the Fashion Industry. In Social Robotics (Lecture Notes in Computer Science), Springer International Publishing, Cham, 209–219. DOI:https://doi.org/10.1007/978-3-319-70022-9_21
5. Bander A. Alsajjan. 2010. How The Big Five Personality Dimensions Influence Customers Trust In UK Cellular Providers? International Journal of Global Business 3, 1 (June 2010), 102–116.
6. Mark Andrejevic and Neil Selwyn. 2020. Facial recognition technology in schools: critical questions and concerns. Learning, Media and Technology 45, 2 (April 2020), 115–128. DOI:https://doi.org/10.1080/17439884.2020.1686014
7. Payal Arora. 2019. Benign dataveillance? Examining novel data-driven governance systems in India and China. First Monday (April 2019). DOI:https://doi.org/10.5210/fm.v24i4.9840
8. Nora Balfe, Sarah Sharples, and John R. Wilson. 2018. Understanding Is Key: An Analysis of Factors Pertaining to Trust in a Real-World Automation System. Hum Factors 60, 4 (June 2018), 477–495. DOI:https://doi.org/10.1177/0018720818761256
9. Ilinca Barsan. 2020. Research Reveals Inherent AI Gender Bias. Wunderman Thompson. Retrieved August 18, 2020 from https://www.wundermanthompson.com/insight/ai-and-gender-bias
10. Debora Bettiga and Lucio Lamberti. 2017. Exploring the adoption process of personal technologies: A cognitive-affective approach. The Journal of High Technology Management Research 28, 2 (January 2017), 179–187. DOI:https://doi.org/10.1016/j.hitech.2017.10.002
11. Zach Blas. 2013. Escaping the Face: Biometric Facial Recognition and the Facial Weaponization Suite. NMC Media-N (July 2013). Retrieved August 18, 2020 from http://median.newmediacaucus.org/caa-conference-edition-2013/escaping-the-face-biometric-facial-recognition-and-the-facial-weaponization-suite/
12. Nicolas Boyon. 2019. Global Citizens OK with Government Use of AI and Facial Recognition… Within Limits. Ipsos. Retrieved August 18, 2020 from https://www.ipsos.com/en-us/news/polls/WEF-govt-use-facial-recognition-ai
13. Ben Bradford, Julia A. Yesberg, Jonathan Jackson, and Paul Dawson. Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology. Br J Criminol. DOI:https://doi.org/10.1093/bjc/azaa032
14. Cheryl L. Brown. 2012. Health-Care Data Protection and Biometric Authentication Policies: Comparative Culture and Technology Acceptance in China and in the United States. Review of Policy Research 29, 1 (2012), 141–159. DOI:https://doi.org/10.1111/j.1541-1338.2011.00546.x
15. Joy Buolamwini and Timnit Gebru. 2018. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In Conference on Fairness, Accountability and Transparency, PMLR, 77–91. Retrieved August 18, 2020 from http://proceedings.mlr.press/v81/buolamwini18a.html
16. J. Alberto Castañeda, Francisco Muñoz-Leiva, and Teodoro Luque. 2007. Web Acceptance Model (WAM): Moderating effects of user experience. Information & Management 44, 4 (June 2007), 384–396. DOI:https://doi.org/10.1016/j.im.2007.02.003
17. Raymond B. Cattell. 1943. The description of personality: basic traits resolved into clusters. The Journal of Abnormal and Social Psychology 38, 4 (1943), 476–506. DOI:https://doi.org/10.1037/h0054116

18. Shih-Yi Chien, Katia Sycara, Jyi-Shane Liu, and Asiye Kumru. 2016. Relation between Trust Attitudes Toward Automation, Hofstede's Cultural Dimensions, and Big Five Personality Traits. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 60, 1 (September 2016), 841–845. DOI:https://doi.org/10.1177/1541931213601192

19. Mohammad Chuttur. Overview of the Technology Acceptance Model: Origins, Developments and Future Directions. 23.

20. Deborah A. Cobb-Clark and Stefanie Schurer. 2012. The stability of big-five personality traits. Economics Letters 115, 1 (April 2012), 11–15. DOI:https://doi.org/10.1016/j.econlet.2011.11.015

21. F. D. Davis. 1986. A technology acceptance model for empirically testing new end-user information systems : Theory and results. Ph. D. dissertation, Massachusetts Institute of Technology (1986). Retrieved August 18, 2020 from https://ci.nii.ac.jp/naid/20001062454/

22. Patricia C. Duttweiler. 2016. The Internal Control Index: A Newly Developed Measure of Locus of Control: Educational and Psychological Measurement (September 2016). DOI:https://doi.org/10.1177/0013164484442004

23. Anthony M. Evans and William Revelle. 2008. Survey and behavioral measurements of interpersonal trust. Journal of Research in Personality 42, 6 (December 2008), 1585–1593. DOI:https://doi.org/10.1016/j.jrp.2008.07.011

24. Donald W. Fiske. 1949. Consistency of the factorial structures of personality ratings from different sources. The Journal of Abnormal and Social Psychology 44, 3 (1949), 329–344. DOI:https://doi.org/10.1037/h0057198

25. Yannick Forster, Frederik Naujoks, and Alexandra Neukum. 2017. Increasing anthropomorphism and trust in automated driving functions by adding speech output. In 2017 IEEE Intelligent Vehicles Symposium (IV), 365–372. DOI:https://doi.org/10.1109/IVS.2017.7995746

26. Connie Fossi and Phil Prazan. Miami Police Used Facial Recognition Technology in Protester's Arrest. NBC 6 South Florida. Retrieved August 23, 2020 from https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/

27. Geoffrey A. Fowler. 2020. Perspective | Black Lives Matter could change facial recognition forever — if Big Tech doesn't stand in the way. Washington Post. Retrieved August 18, 2020 from https://www.washingtonpost.com/technology/2020/06/12/facial-recognition-ban/

28. Jennifer Fujawa. 2005. Privacy made public: will national security be the end of individualism? ACM SIGCAS Computers and Society 35, (March 2005), 4–4. DOI:https://doi.org/10.1145/1111640.1111644

29. Brian Fung. Tech companies push for nationwide facial recognition law. Now comes the hard part. CNN. Retrieved August 18, 2020 from https://www.cnn.com/2020/06/13/tech/facial-recognition-policy/index.html

30. Pete Fussey and Daragh Murray. 2019. Metropolitan police live facial recognition trial concerns | University of Essex. University of Essex Human Rights Centre. Retrieved August 18, 2020 from https://www.essex.ac.uk/news/2019/07/03/met-police-live-facial-recognition-trial-concerns

31. Kelly Gates. 2004. The past perfect promise of facial recognition technology. (June 2004). Retrieved August 18, 2020 from https://www.ideals.illinois.edu/handle/2142/38

32. Kelly A. Gates. 2011. Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. NYU Press.

33. F.C. Gee, W.N. Browne, and K. Kawamura. 2005. Uncanny valley revisited. In ROMAN 2005. IEEE International Workshop on Robot and Human Interactive Communication, 2005., 151–157. DOI:https://doi.org/10.1109/ROMAN.2005.1513772

34. Dogan Gursoy, Oscar Hengxuan Chi, Lu Lu, and Robin Nunkoo. 2019. Consumers acceptance of artificially intelligent (AI) device use in service delivery. International Journal of Information Management 49, (December 2019), 157–169. DOI:https://doi.org/10.1016/j.ijinfomgt.2019.03.008

35. Karen Hao. 2020. The two-year fight to stop Amazon from selling face recognition to the police. MIT Technology Review. Retrieved August 18, 2020 from https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/

36. Fahad AL Harby, Rami Qahwajim, and Mumtaz Kamala. 2010. Towards an Understanding of User Acceptance to Use Biometrics Authentication Systems in E-commerce: Using an Extension of the Technology Acceptance Model. International

Journal of E-Business Research (IJEBR) 3 (July 2010). Retrieved August 18, 2020 from www.igi-global.com/article/towards-understanding-user-acceptance-use/45005

37. Hans van der Heijden. 2004. User Acceptance of Hedonic Information Systems. MIS Quarterly 28, 4 (2004), 695–704. DOI:https://doi.org/10.2307/25148660

38. Rebecca Heilweil. 2020. Masks can fool facial recognition systems, but the algorithms are learning fast. Vox. Retrieved August 18, 2020 from https://www.vox.com/recode/2020/7/28/21340674/face-masks-facial-recognition-surveillance-nist

39. Rebecca Heilweil. 2020. The dystopian tech that companies are selling to help schools reopen sooner. Vox. Retrieved August 18, 2020 from https://www.vox.com/recode/2020/8/14/21365300/artificial-intelligence-ai-school-reopening-technology-covid-19

40. Kashmir Hill. 2020. Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich. The New York Times. Retrieved August 18, 2020 from https://www.nytimes.com/2020/03/05/technology/clearview-investors.html

41. Lauren Hirsch. 2020. IBM gets out of facial recognition business, calls on Congress to advance policies tackling racial injustice. CNBC. Retrieved August 18, 2020 from https://www.cnbc.com/2020/06/08/ibm-gets-out-of-facial-recognition-business-calls-on-congress-to-advance-policies-tackling-racial-injustice.html

42. Kevin Anthony Hoff and Masooda Bashir. 2015. Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. Hum Factors 57, 3 (May 2015), 407–434. DOI:https://doi.org/10.1177/0018720814547570

43. Geert Hofstede. 2001. Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations. SAGE Publications.

44. Geert Hofstede. 2007. Mexico - Mexican Geert Hofstede Cultural Dimensions Explained. (2007), 3.

45. Geert Hofstede and Jean-Claude Usunier (Eds.). 2003. International business negotiations, Chapter 6 (2nd ed ed.). Pergamon, Amsterdam ; Boston.

46. Richard J. Holden and Ben-Tzion Karsh. 2010. The Technology Acceptance Model: Its past and its future in health care. Journal of Biomedical Informatics 43, 1 (February 2010), 159–172. DOI:https://doi.org/10.1016/j.jbi.2009.07.002

47. Steven Hornik and Anna Tupchiy. 2006. Culture's Impact on Technology Mediated Learning: The Role of Horizontal and Vertical Individualism and Collectivism. Journal of Global Information Management (JGIM) 4 (October 2006). Retrieved August 18, 2020 from www.igi-global.com/article/journal-global-information-management-jgim/3644

48. Keith W. Jacobs. 1993. Psychometric Properties of the Internal Control Index. Psychol Rep 73, 1 (August 1993), 251–255. DOI:https://doi.org/10.2466/pr0.1993.73.1.251

49. Rabia Jafri and Hamid R. Arabnia. 2009. A Survey of Face Recognition Techniques. Journal of Information Processing Systems 5, 2 (2009), 41–68. DOI:https://doi.org/10.3745/JIPS.2009.5.2.041

50. Charlotte Jee. 2020. A new US bill would ban the police use of facial recognition. MIT Technology Review. Retrieved August 18, 2020 from https://www.technologyreview.com/2020/06/26/1004500/a-new-us-bill-would-ban-the-police-use-of-facial-recognition/

51. Hans-Christian Jetter, Sarah Gallacher, Vaiva Kalnikaite, and Yvonne Rogers. 2014. Suspicious boxes and friendly aliens: exploring the physical design of urban sensing technology. In Proceedings of the First International Conference on IoT in Urban Space (URB-IOT '14), ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, 68–73. DOI:https://doi.org/10.4108/icst.urb-iot.2014.257307

52. Jiun-Yin Jian, Ann M. Bisantz, and Colin G. Drury. 2000. Foundations for an Empirically Determined Scale of Trust in Automated Systems. International Journal of Cognitive Ergonomics 4, 1 (March 2000), 53–71. DOI:https://doi.org/10.1207/S15327566IJCE0401_04

53. Oliver P. John, Richard W. Robins, and Lawrence A. Pervin. 2008. Handbook of Personality, Third Edition: Theory and Research. Guilford Press.

54. Oliver P. John and Sanjay Srivastava. 1999. The Big Five Trait taxonomy: History, measurement, and theoretical perspectives. In Handbook of personality: Theory and research, 2nd ed. Guilford Press, New York, NY, US, 102–138.

55. Elena Karahanna, Ritu Agarwal, and Corey M. Angst. 2006. Reconceptualizing Compatibility Beliefs in Technology Acceptance Research. MIS Quarterly 30, 4 (2006), 781–804. DOI:https://doi.org/10.2307/25148754

56. William R. King and Jun He. 2006. A meta-analysis of the technology acceptance model. Information & Management 43, 6 (September 2006), 740–755. DOI:https://doi.org/10.1016/j.im.2006.05.003

57. Michael Koch, Kai von Luck, Jan Schwarzer, and Susanne Draheim. 2018. The Novelty Effect in Large Display Deployments – Experiences and Lessons-Learned for Evaluating Prototypes. (2018). DOI:https://doi.org/10.18420/ecscw2018_3

58. K.S. Krishnapriya, Kushal Vangara, Michael C. King, Vitor Albiero, and Kevin Bowyer. 2019. Characterizing the Variability in Face Recognition Accuracy Relative to Race. 0–0. Retrieved August 18, 2020 from https://openaccess.thecvf.com/content_CVPRW_2019/html/BEFA/S_Characterizing_the_Variability_in_Face_Recognition_Accuracy_Relative_to_Race_CVPRW_2019_paper.html

59. John D. Lee and Katrina A. See. 2004. Trust in Automation: Designing for Appropriate Reliance. Hum Factors 46, 1 (March 2004), 50–80. DOI:https://doi.org/10.1518/hfes.46.1.50_30392

60. Younghwa Lee, Kenneth A. Kozar, and Kai R.T. Larsen. 2003. The Technology Acceptance Model: Past, Present, and Future. CAIS 12, (2003). DOI:https://doi.org/10.17705/1CAIS.01250

61. Ari Levy. 2020. Microsoft says it won't sell facial recognition software to police until there's a national law "grounded in human rights." CNBC. Retrieved August 18, 2020 from https://www.cnbc.com/2020/06/11/microsoft-says-will-not-sell-facial-recognition-software-to-police.html

62. J. C. Lin and Hsing-Chi Chang. 2011. The role of technology readiness in self-service technology acceptance. (2011). DOI:https://doi.org/10.1108/09604521111146289

63. Joseph B. Lyons, Charlene K. Stokes, Kevin J. Eschleman, Gene M. Alarcon, and Alex J. Barelka. 2011. Trustworthiness and IT Suspicion: An Evaluation of the Nomological Network. Hum Factors 53, 3 (June 2011), 219–229. DOI:https://doi.org/10.1177/0018720811406726

64. Kim Lyons. 2020. ICE just signed a contract with facial recognition company Clearview AI. The Verge. Retrieved August 18, 2020 from https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration

65. John Maltby and Clare Diane Cope. 1996. Reliability Estimates of the Internal Control Index among UK Samples. Psychol Rep 79, 2 (October 1996), 595–598. DOI:https://doi.org/10.2466/pr0.1996.79.2.595

66. V. D. Mamontov, T. M. Kozhevnikova, and Y. Y. Radyukova. 2014. Collectivism and individualism in modern Russia. Asian Social Science 10, 23 (2014). DOI:https://doi.org/10.5539/ass.v10n23p199

67. Monique Mann and Marcus Smith. 2017. Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. U.N.S.W.L.J. 40, 1 (2017), 121–145.

68. Lawrence S. Meyers and Dennis T. Wong. 1988. Validation of a New Test of Locus of Control: The Internal Control Index. Educational and Psychological Measurement 48, 3 (September 1988), 753–761. DOI:https://doi.org/10.1177/0013164488483024

69. Caroline Lancelot Miltgen, Aleš Popovič, and Tiago Oliveira. 2013. Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. Decision Support Systems 56, (December 2013), 103–114. DOI:https://doi.org/10.1016/j.dss.2013.05.010

70. Todd Mooradian, Birgit Renzl, and Kurt Matzler. 2006. Who Trusts? Personality, Trust and Knowledge Sharing. Management Learning 37, 4 (December 2006), 523–540. DOI:https://doi.org/10.1177/1350507606073424

71. Masahiro Mori. 1970. The Uncanny Valley. Energy, 7(4), 33-35.

72. Cristian Morosan. 2011. Customers' Adoption of Biometric Systems in Restaurants: An Extension of the Technology Acceptance Model. Journal of Hospitality Marketing & Management 20, 6 (August 2011), 661–690. DOI:https://doi.org/10.1080/19368623.2011.570645

73. Cristian Morosan. 2012. Theoretical and Empirical Considerations of Guests' Perceptions of Biometric Systems in Hotels: Extending the Technology Acceptance Model. Journal of Hospitality & Tourism Research 36, 1 (February 2012), 52–84. DOI:https://doi.org/10.1177/1096348010380601

74. Farzaneh Nasirian, Mohsen Ahmadian, and One-Ki (Daniel) Lee. 2017. AI-Based Voice Assistant Systems: Evaluating from the Interaction and Trust Perspectives. AMCIS 2017 Proceedings (August 2017). Retrieved from https://aisel.aisnet.org/amcis2017/AdoptionIT/Presentations/27

75. O.Vision. 2020. O.Vision. O.vision. Retrieved August 18, 2020 from https://o.vision/o-gate#how-it-works

76. Sung Youl Park. 2009. An Analysis of the Technology Acceptance Model in Understanding University Students' Behavioral Intention to Use e-Learning. Journal of Educational Technology & Society 12, 3 (2009), 150–162.

77. Tero Pikkarainen, Kari Pikkarainen, Heikki Karjaluoto, and Seppo Pahnila. 2004. Consumer acceptance of online banking: an extension of the technology acceptance model. Internet Research 14, 3 (January 2004), 224–235. DOI:https://doi.org/10.1108/10662240410542652

78. Frank E. Pollick. 2010. In Search of the Uncanny Valley. In User Centric Media, Petros Daras and Oscar Mayora Ibarra (eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 69–78. DOI:https://doi.org/10.1007/978-3-642-12630-7_8

79. Joe Purshouse and Liz Campbell. 2019. Privacy, Crime Control and Police Use of Automated Facial Recognition Technology. Criminal Law Review 2019, 3 (2019), 188–204.

80. Karen Mui-Teng Quek and Carmen Knudson-Martin. 2006. A Push Toward Equality: Processes Among Dual-Career Newlywed Couples in Collectivist Culture. Journal of Marriage and Family 68, 1 (2006), 56–69. DOI:https://doi.org/10.1111/j.1741-3737.2006.00233.x

81. Rupak Rauniar, Greg Rawski, Jei Yang, and Ben Johnson. 2014. Technology acceptance model (TAM) and social media usage: an empirical study on Facebook. Journal of Enterprise Information Management 27, 1 (January 2014), 6–30. DOI:https://doi.org/10.1108/JEIM-04-2012-0011

82. Chris Riley, Kathy Buckner, Graham Johnson, and David Benyon. 2009. Culture & biometrics: regional differences in the perception of biometric authentication technologies. AI & Soc 24, 3 (October 2009), 295–306. DOI:https://doi.org/10.1007/s00146-009-0218-1

83. Francesca Rossi. 2018. BUILDING TRUST IN ARTIFICIAL INTELLIGENCE. Journal of International Affairs 72, 1 (2018), 127–134. DOI:https://doi.org/10.2307/26588348

84. David P. Schmitt, Jüri Allik, Robert R. McCrae, and Verónica Benet-Martínez. 2007. The Geographic Distribution of Big Five Personality Traits: Patterns and Profiles of Human Self-Description Across 56 Nations. Journal of Cross-Cultural Psychology 38, 2 (March 2007), 173–212. DOI:https://doi.org/10.1177/0022022106297299

85. Arathi Sethumadhavan. 2019. Trust in Artificial Intelligence. Ergonomics in Design 27, 2 (April 2019), 34–34. DOI:https://doi.org/10.1177/1064804618818592

86. Keng Siau and Weiyu Wang. 2018. Building Trust in Artificial Intelligence, Machine Learning, and Robotics. Cutter Business Technology Journal 31, (March 2018), 47–53.

87. Navya Nishith Sharan and Daniela Maria Romano. 2020. The effects of personality and locus of control on trust in humans versus artificial intelligence. Heliyon 6, 8 (August 2020), e04572. DOI:https://doi.org/10.1016/j.heliyon.2020.e04572

88. Nick Statt. 2020. Amazon bans police from using its facial recognition technology for the next year - The Verge. The Verge. Retrieved August 18, 2020 from https://www.theverge.com/2020/6/10/21287101/amazon-rekognition-facial-recognition-police-ban-one-year-ai-racial-bias

89. John P. Sullins. 2008. Friends by Design: A Design Philosophy for Personal Robotics Technology. In Philosophy and Design: From Engineering to Architecture, Peter Kroes, Pieter E. Vermaas, Andrew Light and Steven A. Moore (eds.). Springer Netherlands, Dordrecht, 143–157. DOI:https://doi.org/10.1007/978-1-4020-6591-0_11

90. Bernadette Szajna. 1996. Empirical Evaluation of the Revised Technology Acceptance Model. Management Science 42, 1 (January 1996), 85–92. DOI:https://doi.org/10.1287/mnsc.42.1.85

91. Angela Tinwell. 2014. The Uncanny Valley in Games and Animation. CRC Press.

92. Rupert Kinglake Tower, Caroline Kelly, and Anne Richards. 1997. Individualism, collectivism and reward allocation: A cross-cultural study in Russia and Britain. British Journal of Social Psychology 36, 3 (1997), 331–345. DOI:https://doi.org/10.1111/j.2044-8309.1997.tb01135.x

93. Indrit Troshani, Sally Rao Hill, Claire Sherman, and Damien Arthur. 2020. Do We Trust in AI? Role of Anthropomorphism and Intelligence. Journal of Computer Information Systems 0, 0 (August 2020), 1–11. DOI:https://doi.org/10.1080/08874417.2020.1788473

94. Marisa Tschopp and Marc Ruef. 2018. On Trust in AI - A Systemic Approach. 5.

95. Jeng-Yi Tzeng. 2011. Perceived values and prospective users' acceptance of prospective technology: The case of a career eportfolio system. Computers & Education 56, 1 (January 2011), 157–165. DOI:https://doi.org/10.1016/j.compedu.2010.08.010

96. Meredith Van Natta, Paul Chen, Savannah Herbek, Rishabh Jain, Nicole Kastelic, Evan Katz, Micalyn Struble, Vineel Vanam, and Niharika Vattikonda. 2020. The Rise and Regulation of Thermal Facial Recognition Technology during the COVID-19 Pandemic. J Law Biosci (June 2020). DOI:https://doi.org/10.1093/jlb/lsaa038

97. Olivia Varley-Winter. 2020. The overlooked governance issues raised by facial recognition. Biometric Technology Today 2020, 5 (May 2020), 5–8. DOI:https://doi.org/10.1016/S0969-4765(20)30061-8

98. Zhongyuan Wang, Guangcheng Wang, Baojin Huang, Zhangyang Xiong, Qi Hong, Hao Wu, Peng Yi, Kui Jiang, Nanxi Wang, Yingjiao Pei, Heling Chen, Yu Miao, Zhibing Huang, and Jinbi Liang. 2020. Masked Face Recognition Dataset and Application. arXiv:2003.09093 [cs] (March 2020). Retrieved August 18, 2020 from http://arxiv.org/abs/2003.09093

99. Jen-Her Wu and Shu-Ching Wang. 2005. What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model. Information & Management 42, 5 (July 2005), 719–729. DOI:https://doi.org/10.1016/j.im.2004.07.001

100. M. I. Zarkasyi, M. R. Hidayatullah, and E. M. Zamzami. 2020. Literature Review : Implementation of Facial Recognition in Society. J. Phys.: Conf. Ser. 1566, (June 2020), 012069. DOI:https://doi.org/10.1088/1742-6596/1566/1/012069

101. Yi Zeng, Enmeng Lu, Yinqian Sun, and Ruochen Tian. 2019. Responsible Facial Recognition and Beyond. arXiv:1909.12935 [cs] (September 2019). Retrieved August 18, 2020 from http://arxiv.org/abs/1909.12935

## APPENDIX 1: QUESTIONNAIRE

Questions marked with a * are required.

**Page 1/4**

1. Please indicate your gender: *
○ Female
○ Male
○ Other / Do not want to disclose

2. Please indicate your age: *
○ 18-24
○ 25-34
○ 35-44
○ 45-54
○ 55-64
○ ≥65

3. Please indicate your highest level of education attained: *
○ Less than high school
○ High school/GED
○ Some college
○ 2 year college (Assoc. Degree)
○ 3/4 year college (BA/BS Degree)
○ Masters degree
○ Doctoral Degree
○ Professional degree (MD, JD, etc.)

4. Please enter your occupation: *

5. Please select your country of residence: *

Please select a country ▼

**Page 2/4**

Please indicate the extent to which you agree with each of the following statements, on a 1 (strongly disagree) to 5 (strongly agree) scale:

6. I see myself as someone who… *

| | 1 (Completely Disagree) | 2 | 3 | 4 | 5 (Completely Agree) |
|---|---|---|---|---|---|
| Is talkative | ○ | ○ | ○ | ○ | ○ |
| Tends to find fault with others | ○ | ○ | ○ | ○ | ○ |
| Does a thorough job | ○ | ○ | ○ | ○ | ○ |
| Is depressed, blue | ○ | ○ | ○ | ○ | ○ |
| Is original, comes up with new ideas | ○ | ○ | ○ | ○ | ○ |
| Is reserved | ○ | ○ | ○ | ○ | ○ |
| Is helpful and unselfish with others | ○ | ○ | ○ | ○ | ○ |
| Can be somewhat careless | ○ | ○ | ○ | ○ | ○ |
| Is relaxed, handles stress well | ○ | ○ | ○ | ○ | ○ |
| Is curious about many different things | ○ | ○ | ○ | ○ | ○ |
| Is full of energy | ○ | ○ | ○ | ○ | ○ |
| Starts quarrels with others | ○ | ○ | ○ | ○ | ○ |
| Is a reliable worker | ○ | ○ | ○ | ○ | ○ |
| Can be tense | ○ | ○ | ○ | ○ | ○ |
| Is ingenious, a deep thinker | ○ | ○ | ○ | ○ | ○ |
| Generates a lot of enthusiasm | ○ | ○ | ○ | ○ | ○ |
| Has a forgiving nature | ○ | ○ | ○ | ○ | ○ |
| Tends to be disorganized | ○ | ○ | ○ | ○ | ○ |
| Worries a lot | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| Has an active imagination | ○ | ○ | ○ | ○ | ○ |
| Tends to be quiet | ○ | ○ | ○ | ○ | ○ |
| Is generally trusting | ○ | ○ | ○ | ○ | ○ |
| Tends to be lazy | ○ | ○ | ○ | ○ | ○ |
| Is emotionally stable, not easily upset | ○ | ○ | ○ | ○ | ○ |
| Is inventive | ○ | ○ | ○ | ○ | ○ |
| Has an assertive personality | ○ | ○ | ○ | ○ | ○ |
| Can be cold and aloof | ○ | ○ | ○ | ○ | ○ |
| Perseveres until the task is finished | ○ | ○ | ○ | ○ | ○ |
| Can be moody | ○ | ○ | ○ | ○ | ○ |
| Values artistic, aesthetic experiences | ○ | ○ | ○ | ○ | ○ |
| Is sometimes shy, inhibited | ○ | ○ | ○ | ○ | ○ |
| Is considerate and kind to almost everyone | ○ | ○ | ○ | ○ | ○ |
| Does things efficiently | ○ | ○ | ○ | ○ | ○ |
| Remains calm in tense situations | ○ | ○ | ○ | ○ | ○ |
| Prefers work that is routine | ○ | ○ | ○ | ○ | ○ |
| Is outgoing, sociable | ○ | ○ | ○ | ○ | ○ |
| Is sometimes rude to others | ○ | ○ | ○ | ○ | ○ |
| Makes plans and follows through with them | ○ | ○ | ○ | ○ | ○ |
| Gets nervous easily | ○ | ○ | ○ | ○ | ○ |
| Likes to reflect, play with ideas | ○ | ○ | ○ | ○ | ○ |
| Has few artistic interests | ○ | ○ | ○ | ○ | ○ |
| Likes to cooperate with others | ○ | ○ | ○ | ○ | ○ |
| Is easily distracted | ○ | ○ | ○ | ○ | ○ |
| Is sophisticated in art, music, or literature | ○ | ○ | ○ | ○ | ○ |

**Page 3/4**

7. Please indicate how you would answer the questions below, using the following scale: *

| | |
|---|---|
| Rarely | Less than 10 % of the time |
| Occasionally | 30% of the time |
| Sometimes | 50% of the time |
| Frequently | 70% of time |
| Usually | +90% of time |

| | Rarely | Occasionally | Sometimes | Frequently | Usually |
|---|---|---|---|---|---|
| When faced with a problem, I try to forget it. | ○ | ○ | ○ | ○ | ○ |
| I need frequent encouragement from others for me to keep working at a difficult task. | ○ | ○ | ○ | ○ | ○ |
| I like jobs where I can make decisions and be responsible for my own work. | ○ | ○ | ○ | ○ | ○ |
| I change my opinion when someone I admire disagrees with me. | ○ | ○ | ○ | ○ | ○ |
| If I want something, I work hard to get it. | ○ | ○ | ○ | ○ | ○ |
| I prefer to learn the facts about something from someone else rather than having to dig them out for myself. | ○ | ○ | ○ | ○ | ○ |
| I will accept jobs that require me to supervise others. | ○ | ○ | ○ | ○ | ○ |
| I have a hard time saying 'no' when someone tries to sell me something I don't want. | ○ | ○ | ○ | ○ | ○ |
| I like to have a say in any decisions made by any group I am in. | ○ | ○ | ○ | ○ | ○ |
| I consider the different sides of an issue before making any decisions. | ○ | ○ | ○ | ○ | ○ |
| What other people think has a great influence on my behaviour. | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| Whenever something good happens to me, I feel it is because I have earned it. | ○ | ○ | ○ | ○ | ○ |
| I enjoy being in a position of leadership. | ○ | ○ | ○ | ○ | ○ |
| I need someone else to praise my work before I am satisfied with what I have done. | ○ | ○ | ○ | ○ | ○ |
| I am sure enough of my opinions to try and influence others. | ○ | ○ | ○ | ○ | ○ |
| When something is going to affect me, I learn as much about it as I can. | ○ | ○ | ○ | ○ | ○ |
| I decide to do things in the spur of the moment. | ○ | ○ | ○ | ○ | ○ |
| For me, knowing I have done something well is more important than being praised by someone else. | ○ | ○ | ○ | ○ | ○ |
| I let other people's demands keep me from doing things I want to do. | ○ | ○ | ○ | ○ | ○ |
| I stick to my opinions when someone disagrees with me. | ○ | ○ | ○ | ○ | ○ |
| I do what I feel like doing not what other people think I ought to do. | ○ | ○ | ○ | ○ | ○ |
| I get discouraged when doing something that takes a long time to achieve results. | ○ | ○ | ○ | ○ | ○ |
| When part of a group, I prefer to let other people make all the decisions. | ○ | ○ | ○ | ○ | ○ |
| When I have a problem, I follow the advice of friends and relatives. | ○ | ○ | ○ | ○ | ○ |
| I enjoy trying to do difficult tasks more than I enjoy trying to do easy tasks. | ○ | ○ | ○ | ○ | ○ |
| I prefer situations where I can depend on someone else's ability rather than just my own. | ○ | ○ | ○ | ○ | ○ |
| Having someone important tell me I did a good job is more important to me than feeling that I have done a good job. | ○ | ○ | ○ | ○ | ○ |
| When I am involved in something I try to find out all I can about what is going on even when someone else is in charge | ○ | ○ | ○ | ○ | ○ |

**Page 4/4**

Please study the description and pictures of the system below, and then answer all the following questions with this information in mind:

The o.vision system is a facial recognition-based security system for offices, schools, and similar buildings that you might use a keycard to gain entry to. Using algorithms and a neural network, the device reads a person's face in front of a turnstile 4 times per second with an accuracy of 99.5%. It can admit more than 40 people per minute. In ⅕ of a second, the system goes through 5 stages before opening the door: It finds all faces in sight, it determines the nearest person, it runs an anti-spoofing check to ascertain that a real person is in front of the camera, it searches for the person in the database, and then decides to open the turnstile and grant entry if a match is confirmed.

As the entrant, you do not have to stop moving or face the camera directly, the recognition is instant and from a distance as you approach the turnstile. It will recognise you with a hat and glasses on as well. Recent advancements in the technology also allow it to conduct a temperature scan, which is applicable to the COVID-19 ecosystem.

8. Have you ever used facial recognition technology in any of the following contexts? *

| | Yes | No | Not Sure |
|---|---|---|---|
| Personal Device Security (Eg. Face ID to unlock your phone) | ○ | ○ | ○ |
| Office Security | ○ | ○ | ○ |
| Airport Security | ○ | ○ | ○ |
| Home/Personal Residence Security | ○ | ○ | ○ |
| Student Accommodation Security | ○ | ○ | ○ |

9. Have you ever used facial recognition technology in any context not listed above? If so, please specify:

10. Please rate the extent to which you agree/disagree with the following statements. *

I believe that the o.vision system is….

| | 1 (Completely Disagree) | 2 | 3 | 4 | 5 (Completely Agree) |
|---|---|---|---|---|---|
| Useful | ○ | ○ | ○ | ○ | ○ |
| Easy to use | ○ | ○ | ○ | ○ | ○ |
| Fun | ○ | ○ | ○ | ○ | ○ |
| Expensive | ○ | ○ | ○ | ○ | ○ |
| Acceptable to be used by me | ○ | ○ | ○ | ○ | ○ |

11. In which situations/contexts do you find the above to be true of the o.vision system? *

12. I believe that the o.vision system is acceptable as a building entry system in the following contexts: *

| | 1 (Completely Disagree) | 2 | 3 | 4 | 5 (Completely Agree) |
|---|---|---|---|---|---|
| Airports | ○ | ○ | ○ | ○ | ○ |
| Halls of residence (student buildings) | ○ | ○ | ○ | ○ | ○ |
| Homes or residential buildings | ○ | ○ | ○ | ○ | ○ |
| Schools | ○ | ○ | ○ | ○ | ○ |
| Offices | ○ | ○ | ○ | ○ | ○ |
| Shops | ○ | ○ | ○ | ○ | ○ |
| Factories | ○ | ○ | ○ | ○ | ○ |
| Secure buildings (e.g. government buildings, banks, labs...) | ○ | ○ | ○ | ○ | ○ |

13. Are you aware of anyone in your social circle or any building in which any of the following systems is in use? Please select all that apply.
□ Facial recognition
□ Card-based system
□ Fingerprint-based system
□ Barcode-based system
□ Other (Please specify)

14. To what extent do you think it would be possible to swap out a current security system with a facial recognition system in any of the buildings above? Please explain. *

15. To what extent do you associate each of the following risks with the o.vision system? *

| | 1 (Very Low) | 2 | 3 | 4 | 5 (Very High) |
|---|---|---|---|---|---|
| Data security | ○ | ○ | ○ | ○ | ○ |
| Data sharing/privacy | ○ | ○ | ○ | ○ | ○ |
| Fear of mistaken identity in general | ○ | ○ | ○ | ○ | ○ |
| Fear of being mistaken for someone else of a similar minority ethnicity/gender | ○ | ○ | ○ | ○ | ○ |
| Discomfort with the technology | ○ | ○ | ○ | ○ | ○ |
| Unsure how it works | ○ | ○ | ○ | ○ | ○ |

16. Are there any additional risks you associate with the system? Please specify below:

17. Would you recommend the o.vision system to a friend? Please explain. *

18. Please rate the extent to which you agree with the following statements: *

| | 1 (Completely Disagree) | 2 | 3 | 4 | 5 (Completely Agree) |
|---|---|---|---|---|---|
| The system provides safety | ○ | ○ | ○ | ○ | ○ |
| The system is dangerous | ○ | ○ | ○ | ○ | ○ |
| The system is trustworthy | ○ | ○ | ○ | ○ | ○ |
| The system's mode of operation is obscure | ○ | ○ | ○ | ○ | ○ |
| I am at the system's mercy | ○ | ○ | ○ | ○ | ○ |
| I suppose the system works accurately | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| The system is deceptive | ○ | ○ | ○ | ○ | ○ |
| The system is a reliable access granting system | ○ | ○ | ○ | ○ | ○ |
| I mistrust the system’s purpose | ○ | ○ | ○ | ○ | ○ |
| The system seems to be intelligent | ○ | ○ | ○ | ○ | ○ |
| The system can recognize human faces just like a real person | ○ | ○ | ○ | ○ | ○ |
| The system has integrity | ○ | ○ | ○ | ○ | ○ |
| I am wary of the system | ○ | ○ | ○ | ○ | ○ |
| I am suspicious of the system’s intent, action, or outputs | ○ | ○ | ○ | ○ | ○ |
| The system’s actions will have a harmful or injurious outcome | ○ | ○ | ○ | ○ | ○ |
| I am confident in the system | ○ | ○ | ○ | ○ | ○ |
| The system provides security | ○ | ○ | ○ | ○ | ○ |
| The system is dependable | ○ | ○ | ○ | ○ | ○ |
| The system is reliable | ○ | ○ | ○ | ○ | ○ |
| The system is innovative | ○ | ○ | ○ | ○ | ○ |

19. How have the COVID-19 pandemic and current events affected your perception of this system? *

**END OF SURVEY**