Assignment 1a - Individual Problem Statement

CpE 190/EEE 193A

Name: Xavier Howell

Problem Description: (Short and brief - 250 words or less)

One of the biggest societal problems we face today are issues revolving around privacy. Society is rapidly growing and technology itself is growing even faster. More now than ever privacy has become a big concern especially as a majority of information goes digital. Almost 60% of users who use the internment today log on to “find information”, and with so much information out there protecting the valuable bits becomes a huge concern. Possibly the biggest concern today is the entrusting of your personal data. Websites, companies, and just about everything you can think of requires some sort of personal data. When you fork over this information you entrust that they will protect it. We know all too often this is not the case. One problem we face today is that personal data has gotten even more personal. The key reasoning is facial recognition software has become insanely good. What you may have believed to only be a thing in spy movies and advanced government agencies is now in the palms of your hand and used to do things as simple as unlock your phone. This begs the question of how can we protect the simplest form of identification (your face) from being identified from those who you may not want watching?

Additional Details of the proposed Problem: details with specific numbers, charts, graphs and quantifiable support data. About three pages in length.

Lack of consent—A basic principle of any data privacy laws is that organizations must let users know what biometric data they are collecting and receive their consent to do so. The most significant privacy implication of FRT is the use of the technology to identify individuals without their consent. This includes using applications such as real-time public surveillance or an aggregation of databases that are not lawfully constructed.

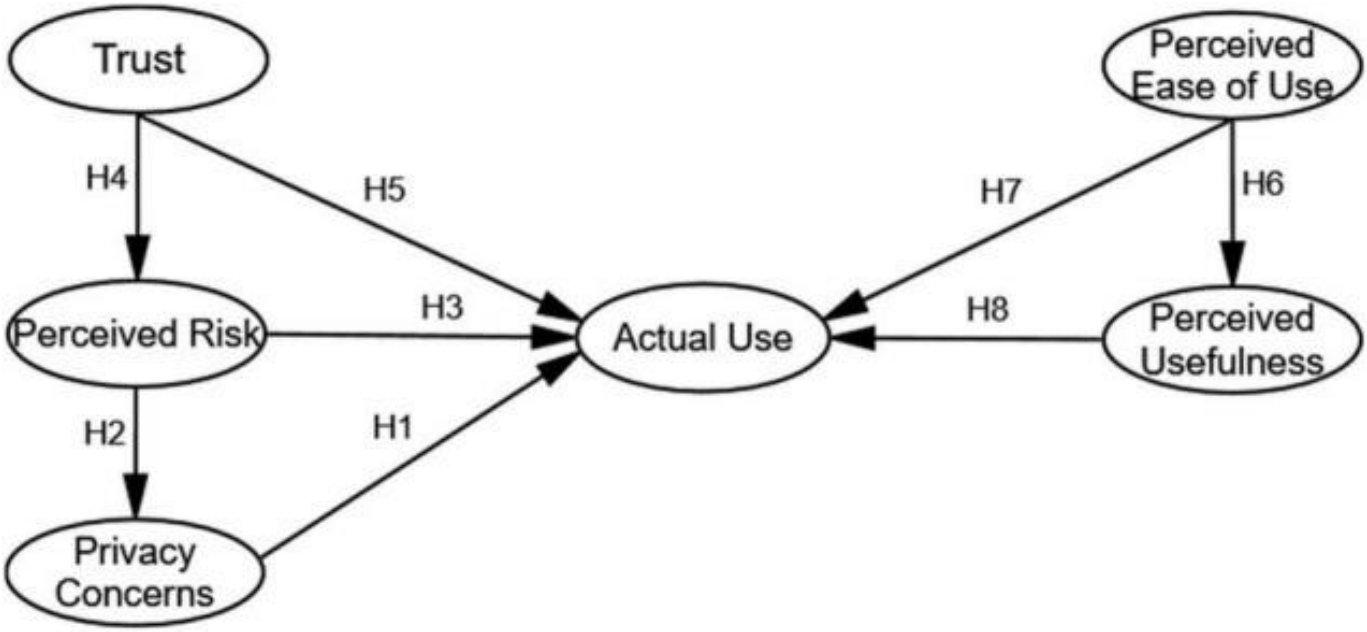
Unencrypted faces—Faces are becoming easier to capture from remote distances and cheaper to collect and store. Unlike many other forms of data, faces cannot be encrypted. Data breaches involving facial recognition data increase the potential for identity theft, stalking, and harassment because, unlike passwords and credit card information, faces cannot easily be changed.

Lack of transparency—Using FRT to identify individuals without their knowledge or consent raises privacy concerns, especially since biometrics are unique to an individual. Furthermore, it poses additional concerns because, unlike other biometrics (e.g., fingerprints), facial scans can be captured easily, remotely and secretly.

Technical vulnerabilities—With FRT, it may be possible to spoof a system (i.e., masquerade as a victim) by using pictures or three-dimensional (3D) masks created from imagery of a victim. In addition, FRT can be prone to presentation attacks or the use of physical or digital spoofs, such as masks or deepfakes, respectively.

Inaccuracy—Inaccuracy is another common critique of FRT. A captured facial scan that misidentifies someone could have long-term consequences. Moreover, accuracy varies by demographic, with false positive rates being highest among women and people of color, that can lead to unjust arrests in the criminal context.

[Hypothesis model]



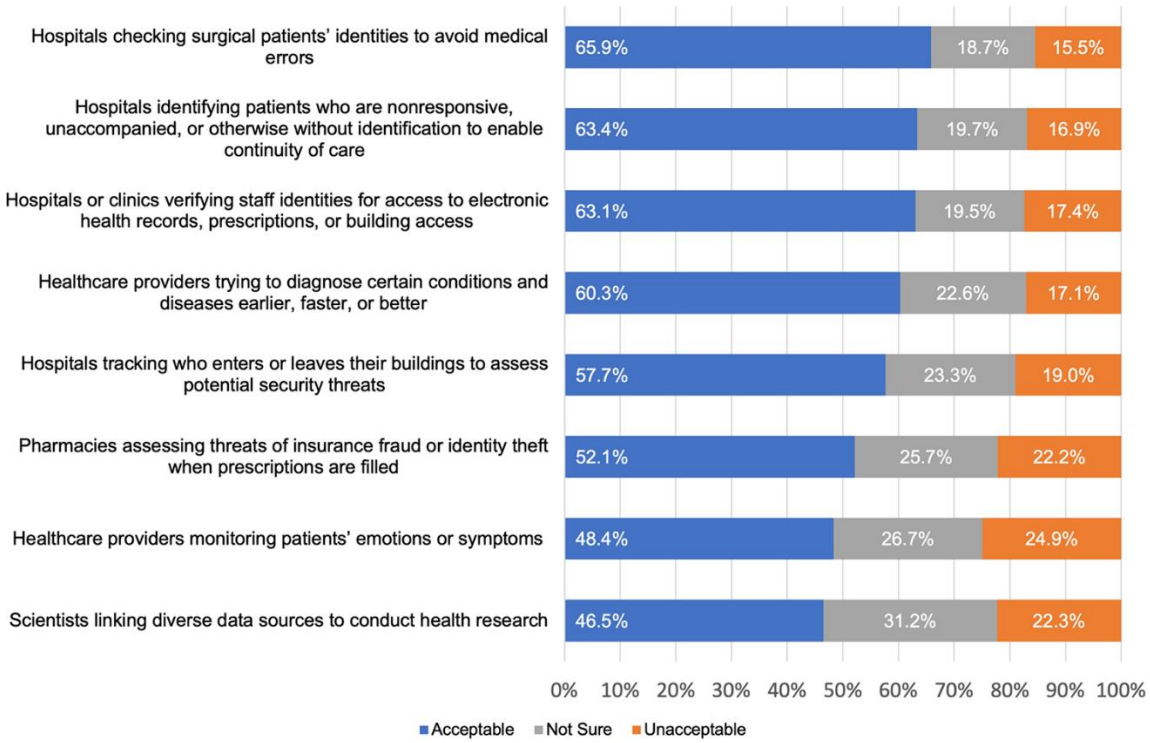
Perceived usefulness refers to the extent to which users believe that using a specific system will improve their job performance. Perceived ease of use refers to the ease with which users think a particular system can be used, which also affects their perceived usefulness of technology (Davis, 1989). The easier it is to use face recognition, the more useful it is considered be. For the purpose of this study, face recognition aims to realize multiple functions, such as providing efficient and convenient services. Therefore, the definition of perceived usefulness should be extended to users think face recognition can improve the degree of convenience and service. In this paper, the ease of using a face recognition application refers to users' perceived ease of use of the technology. Previously, Davis (1989) conducted an empirical study on the e-mail system and concluded that perceived ease of use has a positive impact on the use of applications. In a study on the adoption and use of information systems in the workplace, Venkatesh and Davis (2000) demonstrated that perceived usefulness has a positive impact on people's usage behavior. With the extensive application of the TAM in the information system, the face recognition technology studied in this paper also comprises intelligent media. Perceived usefulness is an important variable that affects the use of face recognition. Thus, the following hypotheses are proposed:

Hypothesis 6: Perceived ease of use has a positive impact on perceived usefulness.

Hypothesis 7: Perceived ease of use has a positive influence on the actual use of face recognition.

Hypothesis 8: Perceived usefulness has a positive impact on the actual use of face recognition.

	M	SD	Privacy concerns	Perceived risk	Perceived ease of use	Perceived usefulness	Trust	Actual use
Privacy concerns	3.986	0.708	1					
Perceived risk	4.070	0.745	0.687**	1				
Perceived ease of use	3.981	0.675	0.237**	0.244**	1			
Perceived usefulness	3.814	0.702	0.129**	0.158**	0.590**	1		
Trust	3.032	0.695	−0.228**	−0.220**	0.084	0.264**	1	
Actual use	3.180	0.743	−0.158**	−0.158**	0.292**	0.494**	0.608**	1



Facial recognition technologies were considered acceptable by a majority of respondents in our survey in six of the eight scenarios (as shown in Fig 2). In fact, 19.8% (800/4048) of respondents considered FRT to be acceptable in all eight of the scenarios we posed, and 53.2% (2154/4048) considered it acceptable in five of the eight scenarios. The two scenarios that failed to elicit a majority acceptance were, notably,

healthcare providers monitoring patients' emotions or symptoms (48.4%, 1879/3883 reported as acceptable) and scientists linking diverse data sources to conduct health research (46.5%, 1793/3855 reported as acceptable). Demographic factors had small or no effects on acceptability of FRT in the eight scenarios.

Propose Design Approach: (Short and brief - 250 words or less)

One way we could protect ourselves from facial recognition is by digitally hiding our faces. Creating a form of facial encryption. This could be done using adversarial patches. Adversarial patches are created to fool machine learning models. Ultimately making it difficult for computer vision and seemingly facial id obscured and hard to use in a real world scenario. If these patches could be projected through infrared it could obstruct unwanted facial recognition from outside cameras while remaining unseen by the human eye. VR glasses are starting to become more of a reality and this could be a implementation and useful feature.

References: (Fours peer-reviewed articles)

	Article Title	Journal	Citation (URL and where available)
1	Research on the Privacy Security of Face Recognition Technology	Comput Intell Neurosci	Pang L. Research on the Privacy Security of Face Recognition Technology. Comput Intell Neurosci. 2022 Jan 25;2022:7882294. doi: 10.1155/2022/7882294. PMID: 35126498; PMCID: PMC8808232.
2	Research on Face Recognition and Privacy in China—	Front Psychol	Liu T, Yang B, Geng Y, Du S. Research on Face Recognition and Privacy in China-Based on Social Cognition and Cultural Psychology. Front Psychol.

	Based on Social Cognition and Cultural Psychology		2021 Dec 24;12:809736. doi: 10.3389/fpsyg.2021.809736. PMID: 35002901; PMCID: PMC8739079.
3	A survey of U.S. public perspectives on facial recognition technology and facial imaging data practices in health and research contexts	PLOS ONE	The PLOS ONE Staff (2021) Correction: A survey of U.S. public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. PLoS ONE 16(12): e0261738. https://doi.org/10.1371/journal.pone.0261738
4	Adversarial Patch	Computer Vision and Pattern Recognition	https://arxiv.org/abs/1712.09665