**Group 5**

**Contemporary Issues in Computer Science & Software Engineering**

Assignment #4

CSE 4314-001 Professional Practices

7/22/2019

Bimal Shrestha 4981

Deion Nwaefulu 6334

Jerry Olds 3643

Meghan Tennant 8625

Mohamed Sawan 0036

Sandhya Sharma 4656

This Assignment is submitted towards and in support of the partial completion of the requirements for the Professional Practices Course

**Table of Contents**

**Introduction1**

**Facial Recognition Devices1**

**Advantages of Facial Recognition Devices2**

**Risks3**

**Conclusion4**

**References6**

**Academic Integrity Form7**

**Introduction**

On May 14, 2019, San Francisco became the first major city in the United States to ban facial recognition devices (Conger, Kate, et al). As facial recognition software advances, so does the range of its applications. While having great potential to facilitate human activity and make data collection and processing more efficient, it can also be used as a tool for malicious actors and encroach into the private lives of its citizens. It is imperative for us as a society to balance these questions and evaluate how such a technology should be allowed to proliferate in the public space, if it should at all. Such an analysis necessitates an understanding of how facial recognition devices operate, their advantages, and the threats they pose to privacy and security.  This article is important to discuss because engineers should understand how these technologies function as well as remain keen on how they impact people's lives and the civic order. This discussion will further discuss the advantages of facial recognition devices, what the risks of using them are, and why San Francisco deemed that the risks they pose to society were too dangerous to be utilized by its departments.

**Facial Recognition Devices**

A facial recognition device is a biometric software application that uniquely identifies the person by comparing and analyzing patterns based on the person's facial contours. It records the geometry of our face such as the distance between the eyes, the length of the face from forehead to chin, facial landmarks, skin color and the retina of the eyes. This is considered our facial signature which can be compared to a database of known faces. Facial recognition devices are capable of identifying and verifying a person from a digital image or video frame. Most devices are designed to scan faces as far as 50 to 100 feet depending on the camera quality and application (Symanovich, Steve). At least 117 million American have images of their face in one or more police databases. According to a May 2018 report, the FBI has had access to 412 million facial images for searches (Rayome, Alison DeNisco).

**Advantages of Facial Recognition Devices**

The advantages of facial recognition include higher security, higher identification

accuracy, and provides efficiency in everyday life. Facial recognition helps to implement higher security features in the devices which will be difficult to attack. It is very uncommon for two people to have the same facial structure. Therefore, security devices can authorize only the person authorized for access (Solutions, TecSynt). For instance, if someone tries to break inside a company’s building, the facial recognition system will alert the authority about the trespass.  
 Recent facial recognition devices are used with infrared cameras and updated with 3D views which helps achieve higher accuracy in security. It is unlikely to fool the system which has such advanced features. This accuracy will help to reduce misidentifications that result from manual recognition. Also, facial recognition ensures that human manpower is not needed to monitor cameras all day (Solutions, TecSynt).

Another important advantage of using the facial recognition feature is that it provides greater efficiency in everyday life. In this busy world, seconds are very important in life (Solutions, TecSynt). For example, it might take twenty seconds for us to unlock a phone using a security password on our mobile devices. Facial recognition allows consumers to unlock a smartphone within a couple of seconds. If we calculate the two seconds saved for a million people, it would be two million seconds saved.

**Risks**

Facial recognition is a relatively new technology that many companies are implementing. Facebook uses it to make tag suggestions in pictures and to crack down on fraudulent accounts, Apple incorporated it as a way to unlock the iPhones, and United States border security implements Microsoft’s facial recognition software.  Like any new technology, the laws have not caught up to cover standards or regulations that cover privacy concerns and also pose risks to security.  
 Facial recognition software uses algorithms that can analyze pictures in order to identify someone.  At the 2001 Super Bowl in Tampa, Florida, police used this technology to scan the attendees in order to find criminals or terrorists.  This could be seen to violate the fourth amendment. In 2018, the US Supreme Court ruled that historical cell phone data was covered under the fourth amendment because it could reveal a person’s movements or physical location.  Using that same precedent, facial recognition in a surveillance agenda would violate the fourth amendment in the same way (Hamann, Kristine, and Rachel Smith).   
 In order for entities to use facial recognition, they have to collect data. Facebook uses this technology to crack down on fraudulent accounts and to make tagging suggestions for pictures. All the data is stored in databases and there are no standards or regulations on how long they can store that data.  Even “compiling data across various databases (whether public or private), throughout multiple locations over a long period, may also implicate the Fourth Amendment.” (Hamann , Kristine, and Rachel Smith). Even though this data was taken publicly, it could reveal intimate details that would only be found with a fourth amendment search.  
 There are very few policies or regulations that address facial recognition. After the protests surrounding Freddie Gray’s death, a study issued by Georgetown Center of Privacy and Technology showed that out of fifty-two agencies, only one had a policy that prohibited the use of technology when it comes to tracking people who engaged in protected speech. Also, most agencies do not require a warrant or even require law enforcement to suspect a crime before using their facial recognition to identify them (“Face Recognition”).

In addition to privacy concerns, Facial recognition also has security flaws. Like traditional security measures, such as a pin, pattern, or password, it can be hacked by sophisticated methods which puts consumer security at risk. Biometric scanning is secure because our DNA never lies. However, faces are not completely free from deception. In 2017, when Apple announced that Face ID would be the newest feature for the iPhone X. It made access to a phone easier, but studies have found a flaw. By adjusting a few pixels at the corner of a person’s eyes or mouth, it would be unrecognizable to the facial recognition technology. Apple took a step further to correct this flaw, but other devices could not handle certain tests to protect a person’s security. The Dutch Organization Consumentenbond conducted a study that resulted in 42 out of 110 devices being unlocked by a photo of their owners which proved a security flaw in Samsung, LG, and Blackberry devices (ZiziMar, Martin).

**Conclusion**

When considering passing a piece of legislation like this that forbids the use of a certain technology, legislators must consider the good and the potential damages that the technology can bring. San Francisco legislators believed that the potential consequences would far outweigh any good that this technology could bring (Conger, Kate, et al). Legislators must also consider what changes to society will occur when banning certain technology. The internet provides an extraordinary amount of services to people but is also abused every day and is the instrument that brings a lot of harm to people. If congress were to ban the internet, it would cause massive economic and social damages that would be too severe for congress to even consider it. In the case of facial recognition devices, the changes to society are minimal and most people in San Francisco will not be affected by this new law.

It is important for the government to consider the worst-case scenarios going forward as new technologies are being developed. If the worst-case scenario is not one hundred percent preventable and if it severely outweighs any good that the technology can provide, then it should not be used in society. Facial recognition devices can be used in a tyrannical way by the government to track people and it introduces a serious threat to people’s safety if it is used by the wrong people. San Francisco legislators believed that these threats were too great for its departments to continue utilizing these devices (Conger, Kate, et al).

**References**

Conger, Kate, et al. “San Francisco Bans Facial Recognition Technology.” *The New York Times*,  
 The New York Times, 14 May 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

“Face Recognition.” *Electronic Frontier Foundation*, Electronic Frontier Foundation, 29 May   
 2019, www.eff.org/pages/face-recognition.

Hamann, Kristine, and Rachel Smith. “Facial Recognition Technology: Where Will It Take Us?”   
 American Bar Association, American Bar Association, 2019,   
 www.americanbar.org/groups/criminal\_justice/publications/criminal-justice-magazine/  
 2019/spring/facial-recognition-technology/.

Rayome, Alison DeNisco. “US Police Storing Facial Image Data of 117 Million Americans,  
 Report Says.” *TechRepublic*, www.techrepublic.com/article/half-of-us-adults-are-in-an-  
 unregulated-police-face-recognition-system-report-says/.

Solutions, TecSynt. “Pros and Cons of Facial Recognition Technology For Your Business.”  
 Upwork, 25 Sept. 2018,[https://www.upwork.com/hiring/for-clients/pros-cons-facial-  
 recognition-technology-business/](https://www.upwork.com/hiring/for-clients/pros-cons-facial-recognition-technology-business/).

Symanovich, Steve. “How Does Facial Recognition Work?” *How Does Facial Recognition  
 Work?*, Symantec Corporation, us.norton.com/internetsecurity-iot-how-facial-recognition  
 -software-works.html.

ZiziMar, Martin. “The Flaws and Dangers of Facial Recognition.” *Security Today*,   
 securitytoday.com/articles/2019/03/01/the-flaws-and-dangers-of-facial-recognition.aspx#.

**CSE - 4314**

**Professional Practices**

**Academic Integrity**

**In order for your Assignment/Homework/Project to be accepted you must read the following, sign this form and attach it to your papers (as the last page of your assignment).**

**Academic Integrity: Students enrolled in this course are expected to adhere to the UT Arlington Honor Code:**

***I pledge, on my honor, to uphold UT Arlington’s tradition of academic integrity, a tradition that values hard work and honest effort in the pursuit of academic excellence.***

***I promise that I will submit only work that I personally create or contribute to group collaborations, and I will appropriately reference any work from other sources. I will follow the highest standards of integrity and uphold the spirit of the Honor Code.***

**Student Signature:**

**Student Id Number: 1001544981           Student Id Number:1000748625**

**Student Id Number: 1001226334                       Student Id Number: 1001554656**

**Student Id Number: 1001533643                     Student Id Number: 1001470036**

***Note: Must be read, signed and attached (stapled) as last page of homework or assignment. If it is a team assignment then all team members must read, sign and attach a single copy of the Academic Integrity form to the team’s paper as the last page. If not properly attached as last page a 2 point penalty will be assessed after grade assigned.***