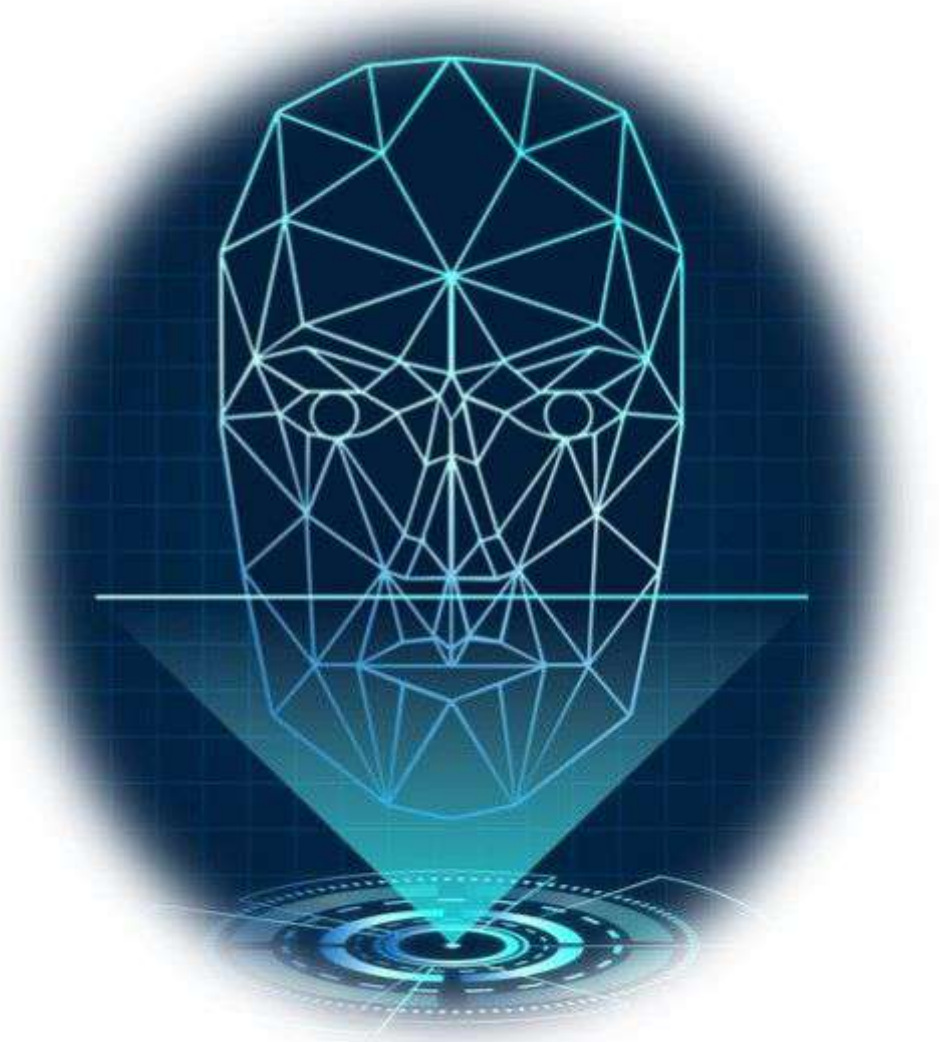

Figure 1: Abstract
Source: Adapted from [1]

Facial Recognition Technology and Ethics

Facial Recognition Recommendation Report

Jake Carlson
Ethan Johnsrud
Calvin Wilcox

November 26, 2019

TABLE OF CONTENTS

Executive Summary 3

Abstract 4

Big Data 5

Biometrics 6

Facial Recognition 7

Legal Issues 8

Privacy Concerns 9

Application 10

Conclusion 11

Recommendation 12

References 14

EXECUTIVE SUMMARY

With developing technologies arises new challenges to overcome. Facial recognition technology is no longer a fantasy from sci-fi movies. It has become a very real, accessible, and applicable solution for many industries. Our motivation in our research is to identify common practices in these technologies, discuss the ethics, and privacy issues that may stem from such methods.

The main areas where facial recognition could be used include law enforcement, border security, social media, data security, and use in stores. In our research, we have concluded that all of these sectors would benefit from implementing facial recognition software but that could come at the cost of risking the general public's data security, and privacy. In some cases, facial recognition needs to be implemented, but new laws and regulations are necessary for every user to abide.

Facial recognition is a rapidly developing tool that has abundant potential for effective application in many areas. Many governments and businesses have expressed interest in using it for various tasks, and some have already started its implementation. With this new development in technology it's applications and uses largely remain unknown. Many industry experts perceive facial recognition technology will revolutionize security, while others envision business and marketing opportunities. Numerous progressive developments will benefit organizations public and private alike. However the opportunity for unintended consequences that could develop as a result of using facial recognition is a serious concern to address. There are many positive effects but there are also many possible unintended consequences that could develop as a result of using facial recognition. This report will lay out many of the possible applications, describe the pros and cons for each application, and propose some possible recommendations of how businesses and the government should proceed with using this software responsibly.

ABSTRACT

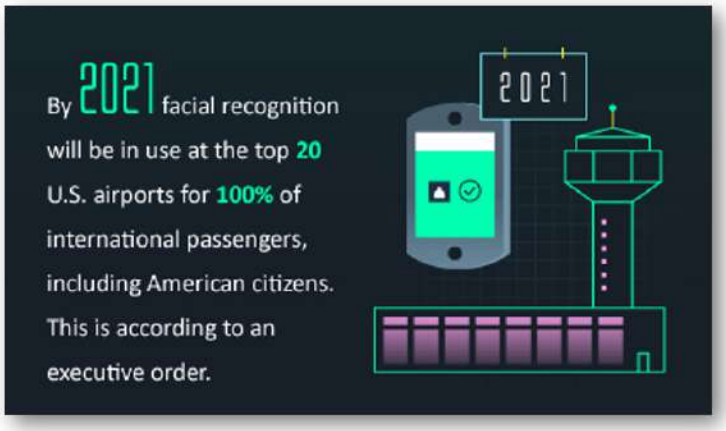

Figure 2: US Facial Recognition in Airports
Source: Adapted from [17]

Facial recognition is a field of biometrics, which strives to identify a person based on their unique physical characteristics. Other forms of biometrics include fingerprint reading, iris scanning, and voice matching. For the past few decades great strides in understanding the unique makeup of a face has been made, this in large part through the cooperation of Psychologists and Computer Scientists. Yet it is only recently that the processing power of modern computers have evolved to make effective facial recognition from a database possible in the not so distant future [2]. Facial recognition software is proving to be highly accurate. DeepFace that is used by Facebook was 97.25 percent accurate in 2014 and FaceNet that is used by Google was 99 percent accurate in 2015 [3]. Now with this developing technology, there is the ethical dilemma of how it will be deployed. Governments have an interest in using it for finding criminals or lost persons, and retailers are interested in using it for marketing or deterring shoplifters.

Due to its user-friendly nature, the automatic face recognition offers a wide range of utilizations ranging from commercial, civilian and forensic applications [2]. Facial recognition software is being used in elections, criminal investigations, and to secure your personal computers. It's greatest rising application is to be used in law enforcement and security surveillance to aid in eliminating voter fraud, check-cashing identity verification, and computer security; areas that remain unsolved through traditional methods [4]. In a security situation, such as a bank, if a camera could quickly and accurately identify an individual, id's and pins would no longer be needed [5].

BIG DATA

In this digital age, the amount of information we give to companies now is colossal compared to what they had to work with in the past. Social media, search engines, proprietary software, and advertisers are collecting and analyzing massive amounts of information from their clients. This type of knowledge is often referred to as Big Data, which leads to new issues that raise many ethical concerns. Including: whether the benefit is worth the cost for people to be giving out valuable information about themselves; and if companies trading this data are working in people's best interest. Although this technology has benefits that could potentially make many systems more effective, there is also the question if this application invades on basic privacy.

A big part of most people's digital footprint originates from social media. When creating an online account, users are required to fill out personal information, and agree to privacy terms and conditions, or decline to use the service in its entirety. Due to outlets' free nature, users are the product technology companies are profiting. The nature of free technology has incentivizes platforms to encourage engagement from their users, and in turn often gain advertisement revenue [6]. However, in many cases these companies do not keep their promises, and users are insufficiently informed about what they're agreeing to.

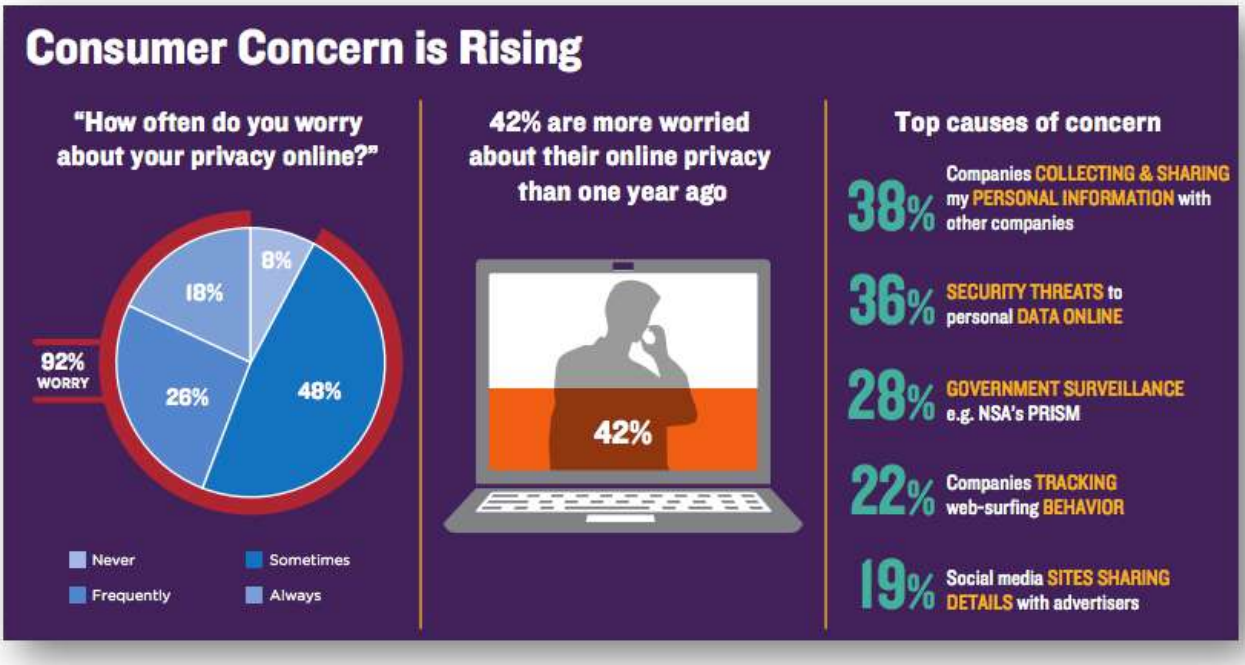

Figure 3: Consumer Privacy Concern
Source: Adapted from [19]

With deep statistical analysis of the information provided by social media networks, companies are able to place targeted advertisements, tailoring both the content and time of day to get a reaction out of users [7]. Advertisers can seize the perfect moment to influence users with messages that have worked on other people, based off similar traits and similar situations. Since there's such massive amounts of data, it is easy for third-parties to cluster individuals with algorithms, predicting stimuli to initiate profitable reactions. This draws a very thin line between enhanced advertising and behavior modification.

Since companies have access to users' behavioral patterns, they can determine the willingness of customers to pay for a service. For example, a person who has quit smoking after twenty years may have a stronger desire and need for health insurance; as they are more prone to health risks. This can lead to perfect price discrimination, where suppliers maximize profit by determining the maximum price an individual will pay. This inevitably leads to loss of consumer surplus [8]. Additionally, refusing insurance on the basis of sensitive information may be prohibited due to anti-discrimination laws. In some cases, perfect price discrimination is illegal; but even in markets where it is legal, the concern arises whether anyone would want to lose surplus based on their online presence. Also, in many situations there is the possibility for companies to mask their intentions with data, via the fine details in terms and conditions of contracts.

BIOMETRICS

Biometrics is an area of science and technology of identifying one person from another by transforming a reading of the human body into a unique identification code. The most proficient and accepted form of biometrics in the market today is fingerprint scanning [4]. A major difference is fingerprints generally require the active participation of the person to be recognized. A technique such as face recognition could, at least in principle, be used to recognize people "passively," without their knowledge or cooperation. There has been an enormous amount of research on data structures and algorithms for use in matching facial images. In general, the matching algorithm will produce a similarity score for each measured element. A threshold can be set so that a match is reported to the

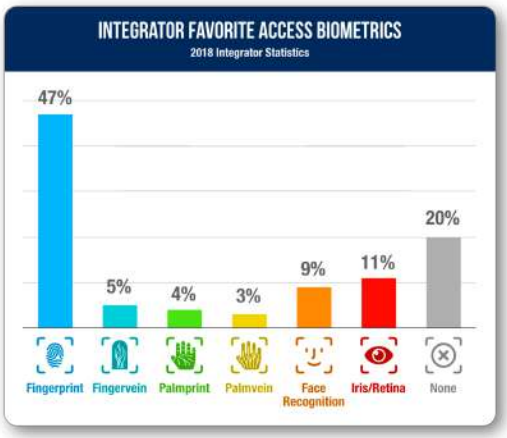

Figure 4: Favorite Biometrics
Source: Adapted from [18]

operator only when the confidence exceeds the threshold. If more than one image generates an above-threshold match, those images can be ranked according to the similarity score. This threshold value can be raised or lowered to adjust the sensitivity of the system [5].

FACIAL RECOGNITION

Facial Recognition Software geometrically identifies disguisable landmarks of the human face. There are about eighty common peaks and valleys that make up the different facial features. Common landmarks measured include the distance between: the eyes, width of nose, depth of eye sockets, cheekbones, jawline, and chin dimensions. The extraction of different landmarks and creating an adaptable template into an automated system that even adapts for a variety of expressions is an arduous goal [9]. When a facial recognition system is running over a video surveillance system it goes through a few steps before that match is made. Once a face is detected in view, the system will determine the head's position, size, and pose. For most systems, a face needs to be turned at least 35 degrees to register. Following is a process called normalization; in which the face is reframed and rotated to match a template. The landmarks in the face are then read into a unique proprietary code that can be quickly compared against a database for matches [4]. Facial recognition methods can be classified in two groups that include appearance-based methods and model-based methods. Former methods use holistic texture features that are applied to either whole-face or specific regions in a face image whereas latter methods employ shape and texture of the face [2]. There are four major methods for facial recognition. Knowledge-based method is a hierarchy of rules, such as the color intensity of the eye area. Challenges with this approach appear with exceptions. If the rules are too general there could be many false positives, and too many false negatives if rules are too specific.

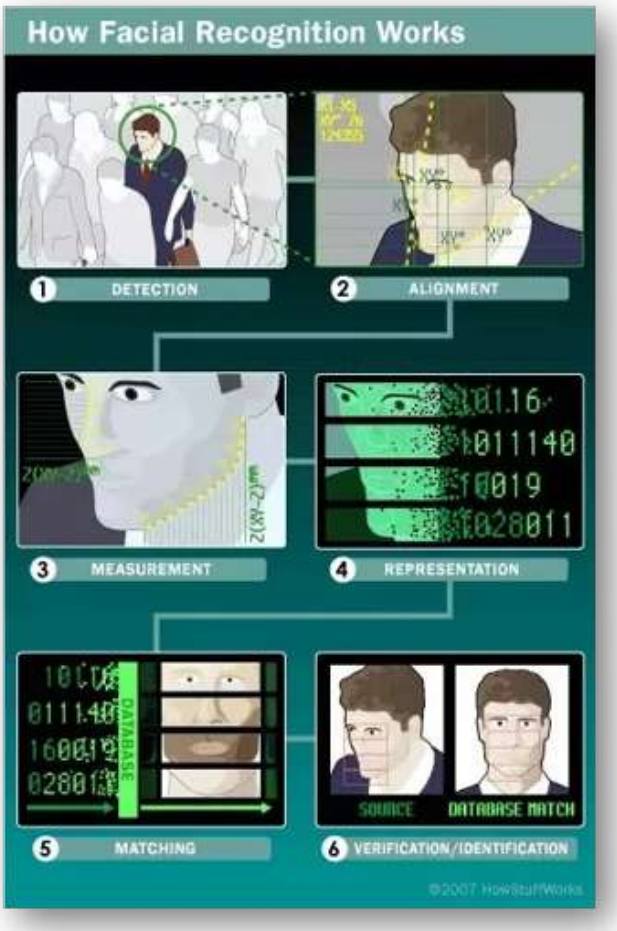

Figure 5: How Facial Recognition Works
Source: Adapted from [16]

Feature-invariant method try to find invariant features of a face despite its angle or position. Specifically, in micro measurements between the eyes, length of nose, and angle of the jaw. Template matching method try to define a face as a function, by matching to a standard template and defining different features independently. Limitations are with variations in pose, scale, and shape; since they rely on a front perspective. Lastly, Appearance-based methods rely on techniques from statistical analysis and machine learning to find the relevant characteristics of face images.

One common algorithm is the Eigenface Principle Components Algorithm. Known as "Eigen faces", because they are the eigenvectors that don't necessarily correspond to the features such as eyes, ears, and noses; but rather characterizes an individual face by a weighted sum of the Eigen faces features. Another algorithm is the Fisher's Discriminant Analysis Distribution Algorithm, that also doubles as a dimensionality reduction technique. It highlights the differences in a given set by maximizing the between class scattering matrix measure while minimizes the within class scatter matrix measure, which makes it more reliable for classification [10].

LEGAL ISSUES

Video surveillance and face recognition systems have become the subject of increased interest and controversy, gaining in popularity following the September 11th, 2001 terrorist attacks on the United States. In favor of face recognition technology, there is the lure of a powerful tool to aid national security. On the negative side, there are fears of an overwhelming invasion of privacy. The most fundamental argument against government use of facial recognition technology in public spaces is that it is a violation of the constitutional right to privacy. Essentially all legal commentators agree that use of face recognition systems in public spaces cannot be considered a "search" for constitutional purposes. The Supreme Court has explained that government action constitutes a search when it invades a person's reasonable expectation of privacy. But the court has also found that a person does not have a reasonable expectation of privacy with regard to physical characteristics that are constantly exposed to the public; such as one's facial features, voice, and handwriting. However,

Figure 6: Facial Recognition usage in Airports
Source: Adapted from [17]

this interpretation of the right to privacy was formulated before it was technically conceivable that a system could automatically match the face of every person entering a public space against a gallery of images of people wanted by authorities [5].

Additionally, there aren't as many solidified limits on who can be identified using the software. In contrast, someone must have committed a crime to be put into the fingerprint database, yet almost everyone is in some sort of facial recognition database due to common services provided by technology companies, such as Facebook and Google, as well as many governmental agencies. These practices have essentially enrolled a majority of citizens into an identifying database which has never been done before and could potentially have dangerous consequences. Among other factors, the personal data becomes valuable and a target for hackers to use in unintended ways.

The collaboration of social media networks and marketing industry leaders is apparent. Companies like Facebook have a massive database of people's photos and the ability to identify a person with over 90% accuracy [11]. The opportunity for deals in the future with walk in retail stores and online companies has expanded rapidly. Facebook can now supply a retailer with their facial recognition technology to identify potential buyers and direct their market more efficiently. To the extreme, someone may walk down the street surrounded by electronic displays showed only to people of similar age, gender, and race. Luckily, privacy concerns like this are being addressed by government organizations like the Nation Telecommunications and Information Administration Agency (NTIA). Currently NTIA is proposing a policy that would require individuals to opt-in voluntarily for their photos to be stored in facial recognition databases.

PRIVACY CONCERNS

Another concern is simply whether citizens should be notified when they enter a public space where video surveillance is being used. For example, given the level of screening already in place for passengers boarding an airplane, posing for a picture for a face recognition system would seem to be a rather minimal added inconvenience. There is also a policy question regarding the decision to add a person's image to the watch list. It seems clear that if there is an arrest warrant for a person, then the person's image could be put in the watch list. But what if a person is only wanted for questioning or if authorities only want to keep track of where a person goes and who they meet. Whether approval from a judge should be required in order to place a person's image in the watch list, perhaps is a process like the requirement for a telephone wiretap. Also, if a

permanent record should be kept of when an individual is entered into the watch list and at whose request. Clearly some level of official procedure is required in order to guard against abuse. If no approval is required for an individual law enforcement officer to enter images into the watch list, it is easy to imagine scenarios for abuse [5].

Facial recognition technology is being developed and tested today. Technology that allows someone to be picked out of a crowd of people and then identified as someone who committed a crime. An instance of this happening is when a man was identified in real time and arrested at a concert in China, surrounded by 50,000 other attendees [12]. While this sounds like it could help society, there are those that worry authoritarian governments would abuse this power in cruel and unusual ways.

APPLICATION

At this time, facial recognition systems have only been implemented in smaller applications; while the public perspective forms and technology continues to develop. The Tampa Police Department tested a software called FaceIt on a one-year trial. While there were no direct arrests made, the network of 36 cameras have allowed police to keep a watchful eye on general activities. One of the most innovative uses of facial recognition is being employed by the Mexican government, which is using the technology to weed out duplicate voter registration [4]. Another way of evaluating how well facial recognition technology works is to look at how it has been adopted by private commercial users. A supplier of face recognition technology claims to have installed fifty systems in casinos, where the technology "is used by surveillance operators to identify cheaters and other casino undesirables, as well as casino VIPs." Casino owners are presumably evaluating the technology on a cost effectiveness basis and judging whether it will allow them to increase their overall profit [5].

Facial recognition is becoming a "NOW" technology, meaning that its performance is reaching efficiency in applications. The ability to identify properties of a person based on their photo is not a new idea. The ability to do it quickly and accurately is just becoming attainable. Professor Alessandro Acquiro of Heinz College at Carnegie Mellon University has been able to conduct experiments where they were not only were able to identify a person from a photo taken from a webcam based off their public Facebook profile picture, but to then also successfully guess that person's Social Security Number [11]. This is a concerning testimony as the consequences of a data breach could be catastrophic.

As technology advances, our policies and practices need to continue to develop. Many of the concerns regarding privacy have yet to be recognized by legislators. As part of an experiment, researchers were able to identify children based on their contextual data from a Smart TV. Facial recognition from the camera, audio from the microphone, and proximity readings from sensors on the device, were all used in their analysis [13]. This allows effective applications, such as enabling an administrator or parent to disable settings or restricting content.

Advantages of facial recognition include benefits towards: law enforcement, data specialists, public safety, accurate identification, and effective marketing tactics [14]. Criminal investigators could potentially locate and arrest a criminal with the use of the criminal database and facial recognition technology. Airlines and public venues could be safer by flagging identified individual entering the facility. Passwords and keycards can be replaced by facial recognition which is more secure and more convenient. Finally, advertisements could be tailored to fit the consumer which could potentially lead to more sales and a better customer experience for everyone.

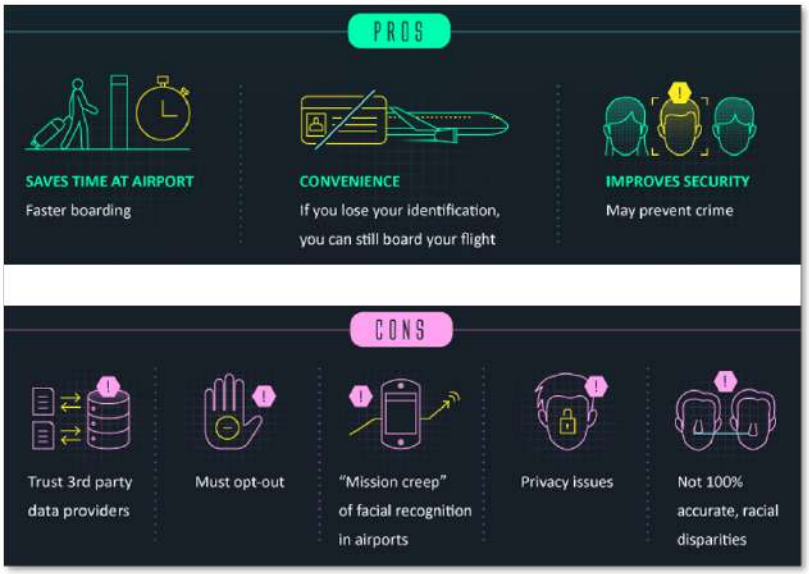

Figure 2: Pros and Cons of Facial Recognition
Source: Adapted from [17]

CONCLUSION

Law enforcement agencies will be one of the first organizations to implement facial recognition technology for a number of reasons. The technology enables live active tracking and identifying of individuals, which will vastly optimize their investigations and ability to catch criminals. Ideally this technology can tell anyone everywhere you've gone and most particularly exactly where you are at any given moment. This is accomplished from the inevitable merged database and camera network of street cameras, traffic cameras, and shopping centers. This all sounds good and well, until you are the wanted individual. While you may not have committed a felony, you may have an unresolved issue

with the IRS, or not spoken well of a politician recently. There is a great opportunity for misuse of this technology, especially by Dictator forms of government. Which is why it is crucial we protect our privacy and trust in government entities through necessary regulation.

The other leading application of facial recognition is with retailers and shopping centers. Unlike online sales, where customers identity and shopping preferences are recorded and analyzed, brick and mortar stores have been unable to gather the same level of detailed information. Digital platforms are able to customize the sales experience to the customer and often this results in more sales. This is not necessarily bad for customers. The algorithms may have identified a better product, an additional item they didn't know they needed, or an unnecessary purchase they'll regret tomorrow. Currently stores are able to track credit card numbers, but this doesn't account for items that were put back on the shelf and targeted demographics. Particularly in malls, where it is easier for a customer to walk in and not find what there looking for, without this data being collected the store doesn't recognize the need to improve their selection or market display. All of this data comes at the cost of privacy, but may outweigh the concern with beneficial opportunities.

RECOMMENDATION

The collection of 'Big Data,' or any personal information, especially identifying data raises numerous privacy concerns. A major necessity is to ensure users and customers are made aware of the information being collected and the purpose for its collection. This allows customers to make an informed decision before using a service that comes at the cost of their personal information. In May 2018, the European Union's General Data Protection Regulation Act went into effect requiring companies to acquire direct consent as well as give consumers control over personal information that is acquired. The U.S. expects similar regulation soon with congress's questioning of Facebook's CEO, Mark Zuckerberg [15]. Particularly with facial recognition, we don't think databases should be allowed to store full pictures of people, but rather only the landmark measurements needed by the software. This will drastically reduce required storage by recognition systems, and more importantly eliminate the opportunity for images to be shared with unintended consequences. Also, decisions on how the data can be shared between companies and databases will require much debate. We believe it is in the best interest of consumers and their privacy to limit sharing; however, this becomes tricky with business ownership styles and methods.

Probably the most dominant and adaptable use of facial recognition technology is in the field of law enforcement agencies. Since this will be the greatest network in any country, we're proposing strict control and accountability over the watchlist. Recognizing the watchlist may not be able to be made public for effectiveness reasons; however, a warrant shall be required to add someone to the watchlist, similar to the practice of telephone tapping. Records also need to be maintained on whom requested the addition and for what reason. In addition, time limits ought to be implemented on how long someone can stay on the watchlist and how long until any identifying information needs to be deleted from all databases. These regulations keep law enforcement agencies accountable. While also maintaining the trust and expectation for privacy with their citizens.

There are even more concerns with facial recognition technology in the hands of private businesses and corporations. In all fairness, they are also the companies investing and developing the technology, giving them more rights than public entities. Nevertheless, businesses selfish ambitions are the concern of many people; at first, it'll only be present for security purposes, but the potential for marketing will soon be recognized. Laws are needed, prohibiting price discrimination and sale discrimination of any form to ensure equal treatment for everyone. This will essentially allow for data to be collected to improve businesses models, but matching activity to an individual and individually adjusting selling campaigns will be prohibited. Retailers shall also clearly post locations of identifying systems and their intentions with the information gathered. The practice is quite similar to online retailers, yet more personalized and leaves consumers not wanting to participate with nowhere to buy merchandise. With large scale implementation, participation is essentially required, making it quite difficult for citizens to 'opt out' of a security tracking program. For this very reason, regulation ensuring privacy and ethical practices are essential for employing facial recognition technology to establishing a safe and prosperous society .

REFERENCES

[1] freepik (2019). Abstract Flat Face Recognition Background. [image] Available at: https://www.freepik.com/free-vector/abstract-flat-face-recognition-background_4715220.htm.

[2] A. K. Agrawal and Y. N. Singh, "Evaluation of Face Recognition Methods in Unconstrained Environments," *Procedia Computer Science*, vol. 48, pp. 644–651, May 2015.

[3] J. Crelin, "Facial Recognition Technology: An Overview," Points of View: *Facial Recognition Technology*, Jul-2017. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=pwh&AN=124174935&site=pov-live.

[4] K. Bosnor, "How Facial Recognition Systems Work," *Armchair Patriot*. [Online]. Available: http://armchairpatriot.com/How Stuff Works/How Facial Recognition Syst.pdf.

[5] K. W. Bowyer, "Face Recognition Technology: Security versus Privacy," *IEEE Technology And Society Magazine*, 2004.

[6] T. Calders, S. Choenni, B. Custers, *Discrimination and Privacy in the Information Society*, London, SpringerHeidelberg, 2013

[7] J. Lanier, *Ten Arguments for Deleting Your Social Media Accounts Right Now*, 1st ed, New York, NY, U.S.A, Henry Holt and Company, 2018

[8] E.K. Clemons, J.S. Wilson, "Family Preferences Concerning Online Privacy, Data Mining, and Targeted ads: Regulatory Implications", *Journal of Management Information Systems*, vol. 32, no. 2, pp 40-70, Fall 2015, doi: 10.1080/07421222.2015.1063277

[9] L. B. Kirithika, "Facial recognition in education system," *IOP Conference Series: Materials Science and Engineering*, no. 263, 2017.

[10] K. Solanki and P. Pittalia, "Review of Face Recognition Techniques," *International Journal of Computer Applications*, vol. 133, no. 12, pp. 0975–8887, Jan. 2016.

[11] Judiciary Subcommittee on Privacy Technology and The Law. 112th Congress, 2nd session. (2012, July 28). J 112 87, *What Facial Recognition Means for Privacy and Civil Liberties*, [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf

[12] P. O'Dowd, "As Facial Recognition Technology Booms, So Do Privacy Concerns," *As Facial Recognition Technology Booms, So Do Privacy Concerns | Here & Now*, 21-Dec-2018. [Online]. Available: https://www.wbur.org/hereandnow/2018/12/21/facial-recognition-privacy-concerns.

[13] P.C.K Hung, K. Kanev, F. Iqbal, D. Mettrick, L. Rafferty, C.M. Fung, "A Study of Children Facial Recognition for Privacy in Smart TV", in *Computational Modeling of Objects Presented in Images.* Sept. 21-23, 2016, pp 229-240

[14] Alicia Puente Cackley, "FACIAL RECOGNITION TECHNOLOGY Commercial Uses, Privacy Issues, and Applicable Federal Law," GAO, Washington D.C. United States, GAO-15-621, 2015

[15] B. Fung, "Why you're getting flooded with privacy notifications in your email," *The Washington Post*, 25-May-2018.

[16] C, M. (2014). *What is face recognition technology and how does it work.* [online] Quora. Available at: https://www.quora.com/What-is-face-recognition-technology-and-how-does-it-work.

[17] Runaway Suitcase. (2019). *Facial Recognition Statistics in Airports.* [online] Available at: https://www.reservations.com/blog/resources/facial-recognition-airports-survey/.

[18] Rhodes, B. (2019). *Favorite Biometrics 2018.* [online] IPVM. Available at: https://ipvm.com/reports/favorite-biometrics-2018.

[19] Trilli, K. (2015). Data Privacy is a Major Concern for Consumers. [online] TrustArc Blog. Available at: https://www.trustarc.com/blog/2015/01/28/data-privacy-concern-consumers/.