12-2020

Global privacy concerns of facial recognition big data

Myranda Westbrook

University of Tennessee at Chattanooga, rmb662@mocs.utc.edu

“Global Privacy Concerns of Facial Recognition Big Data”

Myranda Westbrook

Departmental Honors Thesis

The University of Tennessee at Chattanooga

Management Department

Examination Date: November 11th, 2020

Mohammad Ahmadi, Ph.D.

Guerry Professor of Management

Thesis Director

Abstract:

Facial recognition technology is a system of automatic acknowledgement that recognizes individuals by categorizing specific features of their facial structure to link the scanned information to stored data. Within the past few decades facial recognition technology has been implemented on a large scale to increase the security measures needed to access personal information. This has been specifically used in surveillance systems, social media platforms, and mobile device access control. The extensive use of facial recognition systems has created challenges as it relates to biometric information control and privacy concerns. This concern raises the cost and benefit analysis of an individual's security versus his/her privacy. Due to the contactless ability of facial recognition identification, the global market of this technology is expected to increase considerably over the next decade. This expansion implies the requirements of additional legal regulations in regard to the use of facial recognition technology. Data privacy laws have been passed in over 80 countries around the world and several states within the United States have created laws that apply to this form of technology. However increased action should be taken on a national level to enact stricter regulations in regard to biometric data collection and use.

Introduction:

Big data is defined as a large volume of real time data that involves structured and unstructured data (Ahmadi et al. 2016). As the world becomes increasingly technology intensive, there will continue to be a focus on big data and its privacy concerns. Currently, billions of data points are generated and collected in real time daily; however, this establishes that sensitive data becomes vulnerable to ~~a~~ privacy breach. These privacy related concerns occur during data communication, aggregation, and mining processes. Privacy is focused on the data owners with the intent to protect their private information while utilizing their data for analytic purposes (Tran et al. 2019).

A biometric recognition system is an automatic method that recognizes individuals by identifying features from human characteristics such as fingerprints, irises, and faces. In the past few decades, facial recognition has been deployed on a massive scale due to the increasing use of automatic recognition and surveillance systems. However, the widespread usage of facial recognition systems has raised challenges in terms of biometric information control and privacy. Face images can be collected and misused without the permission of the owner during the storage and processing of the data (Guo et al. 2019). Facial recognition systems have now become the most common and widely used means of biometric identification (Chowdhury et al. 2017).

Background:

When research into facial recognition began in the mid-1960's by academic professor Woody Bledsoe, the beginning data set was comprised of ten faces. The original development of facial recognition was a purely mathematical process of identifying photographs (2D images). However, they encountered problems in identification between the individuals and their stock photos due to change in hair growth, facial expression, and aging. At times, this technology was stated to be "beyond the state of the art of the present pattern recognition and computer technology at this time." (Raviv 2020)

In 1964, Bledsoe was able to create a form of facial recognition that was based on 11 physical measurements, which included a faces' relationship among its major landmarks: eyes, ears, nose, eyebrows, and lips. This technology was tested in 1967 to help law enforcement agencies quickly search through databases of mug shots for a match. The end computer program was tasked with memorizing one version of a facial image and using it to identify its corresponding image in the database. The program had two shortcuts to match the images. The first, known as group matching, would divide the face by its features and compare the relative distances between them to cultivate a match. The second approach used 22 measurements to make an educated guess about the matching facial image. At the end of the testing both approaches, with similar accuracy, completed the task of matching a subset of 100 faces in about three minutes while a test group of humans were able to complete the task in over six hours. This advancement of speed has allowed facial recognition to become a widely implemented security measure for mobile devices, laptops, passports, and payment apps verification. Throughout this technology's history, there has been an apparent recognition of the potential abuses of its widespread implementation. When identifying sample sets the potential biases are made apparent due to the use of almost entirely white men which creates the possibility for facial recognition to be used in a discriminatory manner (Raviv 2020).

The use of facial recognition systems has become commonplace in social media programs and surveillance systems, which when paired with geolocation data, allows for unprecedented tracking of the data contributors. A serious privacy issue influenced by facial recognition technology is the ability to identify a person covertly using the features extracted from a photograph or video feeds. This allows online behavior and data trends to be linked to a specific user (Loebel 2012). One of the major advantages of facial recognition technology is an assumption of safety and security. This is demonstrated in its widespread use by law enforcement agencies and airports. The U.S. Department of Homeland Security predicts that it will be used by 97 percent of travelers by 2023. However, a large drawback of this technology is the opinion that the use of facial recognition systems may be a threat to an individual's privacy (Marr 2019). In the United States, recent legislation has been implemented to protect the privacy of facial recognition data. For example, Oregon and New Hampshire have banned the use of facial recognition in body cameras for police officers (Martin 2019).

Consumers using the internet often indicate that the privacy of their personal data is their foremost concern with the new technology. Different approaches to data privacy and protection are found in the United States and the European Union. In the United States there is a focus on self-regulation, and in the EU there are strict legal requirements (Steinke 2002). In general, Europe is known for its particularly rigorous privacy laws, specifically Germany, France, and the United Kingdom. The Information and Communication Services Act of 1997, which was passed in Germany, contains the Teleservices Data Protection Act. This act is concerned with the protection of personal data used in telecommunications. The British government enacted the Data Protection Act in 1988, which added protection for manual and electronic data records. In 1995, the European Union enacted the EU Data Protection Directive, which requires an organization to inform individuals about the purposes for which it collects and uses information about them. It additionally requires organizations to offer individuals the opportunity to opt out whether their information can be used for a purpose besides the one for which it was originally gathered. Also, sensitive information such as medical conditions, racial, and ethnic origin must allow for the consumer to specifically choose to opt in before the information is disclosed to a third party. The US relies mostly on self-regulation and limited legislation (Steinke 2002).

Current Trends:

The global facial recognition market is set to expand significantly over the next decade. Specifically, the market size is expected to reach $9.93 billion by 2027. The market is anticipated to expand at a rate of 14.5% from 2020 to 2027 according to the Business Wire. This growth can be attributed to the contactless solution that this biometric system implements. A touchless solution can be easily deployed in customer and consumer devices which allows them to be a convenient option. This convenience and ease of implementation has allowed for the gathering of personal information on a large-scale from which patterns and trends of human behavior emerge.

In the past, facial recognition has been used for security and surveillance applications. It is now being implemented at increasing rates for commercial applications. Many consumers are not aware that facial recognition technology exists in public places and can be used to collect personally identifiable data, which can be shared with undisclosed third parties. This has created a need for facial recognition regulation and transparency for the use of this technology in public places (“Commercial Facial Recognition” 2019).

There has been an increased need in government sectors for virtual identification and this is considered a key driver for the growth in the facial recognition market over the next decade. There have also been technology advancements such as cloud-based services and 3D recognition systems that are increasing the ease of implementation and recognition. The rising demand for data security and personal device usage has driven the adoption of technology across various organizations (“Global Facial Recognition” 2020). Face recognition technology is less prone to security breaches as compared to the traditional authorization methods. This level of security is produced due the challenges of replicating a facial scan. The security of this software has been verified with its implementation in banking and financial institutions as a form of customer identification and verification before accessing personal monetary funds via mobile applications for clients on a global scale.

The use of facial recognition in mobile devices is a method of as annual global mobile biometric market revenues are projected to reach $50.6 billion by 2022, which is up from $26.2 billion in 2019. Facial recognition patents are currently being pursued by companies like IBM and Microsoft, which emphasizes the relevance and longevity of this technology as well as its large scale implementation possibilities, however, it will continue to focus on law enforcement, security, access control, and securing biometric payments in the short term future (Samet 2020).

Clients are able to gain access to their current bank and social media accounts through the use of facial recognition and authentication (“Global Facial Recognition” 2020). Given that security concerns that have become increasingly relevant in 2020, the prospect of identifying criminals and preventing security fraud is particularly attractive to customers and organizations around the globe. Fifty nine percent of U.S. adults surveyed by Pew Research Center said it was acceptable for law enforcement to use facial recognition technology to assess security threats in public spaces, but just 15% said it was acceptable for advertisers to use facial recognition technology to see how people respond to public ad displays (Samet 2020). This raises the question of the legal protections in place for consumers that would minimize their risk of public use and collections of their personal biometric data.

Testing:

The United States Commerce Department has been in the process of providing technological benchmarks and evaluating the accuracy of the facial-recognition algorithms. This could be used to inform contract decisions by policymakers and technology organization evaluators. “They [facial recognition suppliers] generally have no idea how effective their algorithms are relative to somebody else’s,” said Patrick Grother, a biometrics science researcher at the National Institute of Standards and Technology (NIST) who led the testing. “If you’re company X, you don’t know your accuracy relative to company Y.” (Kaye 2019).

Joy Buolamwini, MIT researcher and founder of the Algorithmic Justice League, called the NIST benchmarks “gold standards for the industry”. The NIST testing has been viewed as a gold standard of current testing protocol that provides data results that can have a significant impact on policy decisions. The Chinese technology firm, Yitu, confirmed the importance of the U.S. agency testing by stating “The benchmark results of NIST are well-recognized as the golden standards of global industry for its strictness” (Kaye 2019). This form of testing may be important in the future policy implementation of facial recognition due to the standard of accuracy it may require for U.S. companies to undergo before being used on the public to reduce unfair bias.

The NIST results that were released in November 2018 concluded that the entire industry has improved at a substantial rate. It presented that at least 28 developers’ algorithms now outperform the most accurate algorithm from late 2013, and just 0.2 percent of all searches performed by all algorithms tested failed in 2018, compared with a 4 percent failure rate in 2014 and 5 percent rate in 2010 (Kaye 2019).

The testing used by the NIST has incorporated highly complex neural networks and requires the ability of facial-recognition algorithms to detect identities even when poor quality images are employed. This allows technologist to predict a surge in accuracy as data volumes and rate of computing capacity (within the realm of machine learning and artificial intelligence) increase. This form of testing also measures the system’s ability to match an individual’s photo with a different image of the same person stored in a database that contains millions of sample images. The NIST dataset includes 26.6 million portrait photos of 12.3 million individuals that include data from webcam, photojournalism, video surveillance, and personal photo images (Kaye 2019).

The NIST testing has been criticized for its focus on the algorithm’s overall technical performance and its inability to currently provide insight on how these systems truly impact different demographics in groups of people. There have been instances of poor performing facial recognition technologies incorrectly labeling women as men and falsely identifying people with darker complexions. This brings to attention the social implications of facial recognition’s artificial intelligence and the questions in regard to their potential to be used in a discriminatory fashion (Kaye 2019).

The NIST tests, as of December 2019, have discovered that several of the algorithms tested were 10 to 100 times more likely to inaccurately identify the facial imprint of a black or East Asian face as compared to a white face. The demographic that was incorrectly identified at an increased rate were facial images of black women and women of color (Bushwick 2019).

Security vs Privacy:

The use of facial recognition technology in the form of surveillance has rapidly spread in China as the Chinese government prioritizes public security, promotes the development of artificial intelligence (AI), and works to prevent the spread of COVID-19. In March 2020; facial recognition cameras have been equipped with AI-enabled body temperature detection technology in public places to prevent people who may be infected with COVID-19 from traveling. The number of facial recognition cameras in use in China has grown from 176 million in 2017 to 626 million in 2020. The Chinese government has created some measures to regulate the security of biometric data that has been collected. Biometric data collected in this manner is protected by the Personal Information Security Specifications. This regulation states that collection of personal information should be for "legal, justified, necessary, and specific purposes," which often requires consent and must be kept secure. However, the current reality of the implementation of cameras in public places does not attempt to obtain consent or adhere to appropriate data security protection (Dudley 2020).

In the United States; Facebook has settled a $550 million facial recognition lawsuit which demonstrates the influence and power of an Illinois law, the Illinois Biometric Information Privacy Act (BIPA), which is intended to protect a person's biometric data. This case marks one of the largest monetary settlements as it relates to a privacy lawsuit. The BIPA requires companies to obtain a consumer's explicit consent before collecting or sharing their biometric information, this pertains to facial recognition and fingerprint scans. The plaintiffs in the lawsuit argued that Facebook violated the BIPA due to their failure to gain consent before generating user facial scans that were employed to identify the individuals in photos to recommend tagging suggestions (Germain 2020).

In response to this lawsuit; Facebook has updated their tag suggestions settings to not allow for the application of facial recognition technology to automatically suggest tags of related photos. This feature, in the future, will require the user to switch on the use of a broader set of facial recognition abilities to better protect the users' identity while on the platform ("An Update" 2019). Facebook holds several patents targeted to use facial recognition for directed advertising and other purposes but has stated that it doesn't currently use the technology in those ways. Consumer advocates have argued that biometric data is particularly sensitive personal information due to its innate restriction of its inability to be altered. Unlike a password or username your facial features cannot be easily changed (Germain 2020).

Privacy Laws:

The achievements associated with facial recognition technology produces potential drawbacks to privacy for those who are unwillingly subjected to this technology in a public setting. This potential for public use has been paired with current facial recognition technology and the ability to use large amounts of data made available through the internet and social media platforms. Images can be used as data points from various internet sources that create a powerful and potentially invasive form of uncovering a person's identity, which could include full name, address, and additional interests of an individual through the use of just a single photograph ("The Varying Laws" 2020). Private companies, like Apple, have been on the receiving end of bans but are still selling cell phones and other forms of technology that have facial recognition built into their products. These are usually created as a form of security verification. This application of facial recognition is less controversial to consumers due to the perceived choice of disabling or not using the added feature. However legal and financial cases can be filed if consumers are not properly notified by the company. When law enforcement agencies utilize facial recognition technology, often for security and protection of the general public, they can monitor, scan, and track the public without their knowledge. This has been the catalyst for an increase on regulations for this application of facial recognition. The fear of facial recognition has been linked to thoughts of mass surveillance without cause (Ghaffary 2019). The databases required for the use of facial recognition technology are large-scale and are vulnerable to data breaches and often misuse. Some cities in the United States have banned the use of facial recognition technology by city agencies, including the police department, from using these databases against their citizens. In May 2019, San Francisco became the first city in the United States to ban the use of this technology (Center 2020).

A dual-party effort has created in the United States to introduce rules that would prevent law enforcement agencies from using facial recognition technology to surveil citizens. Four cities that have also banned the use of facial recognition technology are San Francisco and Oakland, California, Somerville and Cambridge, Massachusetts. A new bill on facial recognition in the United Sates could include putting a halt on the federal government's acquisition of new facial recognition technology. A main concern that law makers have about facial recognition technology is its potential to infringe on individual civil liberties which include free speech (Ghaffary 2019). Some cities, similar to the Seattle Police Department, have terminated the use of facial recognition technology amid concerns about biased and inaccurate results. Others, like the Detroit Police Department permit the use of facial recognition technology only under certain conditions, such as when the technology seems reasonably likely to aid the investigation into violent crimes ("The Varying Laws" 2020). The use of facial recognition technology has been credited with the solving of numerous criminal cases which further constructs the controversial nature of using this technology as a form of security measure.

The state of Illinois was the first state to address collection of biometric data by private businesses. Its Biometric Information Privacy Act (BIPA), which was passed in 2008, has placed substantial restrictions on how private entities can collect and use a person's biometric data. The act requires that a business obtain informed consent prior to the collection of biometric data. It also prohibits a business from profiting off biometric data, limits the right of a company to disclose collected data, sets forth data protection requirements for business, and it also creates a right of action for individuals whose data has been wrongfully collected or used in violation of the law. Illinois has been in several class action lawsuits that are based on this law in the decade since the law has been in effect. The biometric laws, of similar origin to those in Illinois, in Texas requires individuals and or companies who collect biometric data to inform individuals before assembling the biometric identifiers. However, unlike the Illinois law, the Texas biometric privacy statute does not require a written release. Both state privacy laws prohibit the sale of biometric information and set restrictions on how such information is stored. Washington State's biometric privacy statute took effect in 2017. This law does not specify that consent to collection of biometric data be in writing nor does it create a private cause of action against violators. The Washington state law carves out an exemption to biometric data collection and storage. Businesses may collect and store such information without providing notice and obtaining consent so long as the information is collection for "security purposes." defined to include collection, storage and use of the information for purposes of preventing shoplifting, fraud and theft. The Washington state law also permits companies to sell biometric information under limited circumstances ("The Varying Laws" 2020).

Global Laws:

Currently, many countries with modern data privacy laws have rules in place for the management of information that can identify or be used to identify an individual. Privacy laws have now been enacted in over 80 countries around the world. Australia's Privacy Principles (APP) is an assembly of 13 principles guiding the control of personal information. These principles have set a standard that you must manage personal information in an open and transparent way, which implies having a clear and up-to-date privacy policy about how you manage your customer's personal information. Privacy policies, according to current Australian law, need to define why and how you collect personal information, the significance for not providing personal information, how customers can access and correct their information, and how individuals can report a breach of the principles. The Office of the Australian Information Commissioner (OAIC) is tasked with investigating any privacy complaints or reports about the management of your personal information. Anyone can file a complaint to the office for free at any time, and the office will investigate as soon as possible. In order to avoid complaints about handling of personal information, it's important to have a clear and accurate privacy policy that includes all the requirements laid out by the APP (“2019 Consumer Data” 2019).

Brazil passed the Brazilian Internet Act in 2014, which interacts with policies on the collection, maintenance, treatment, and use of personal data. Any individual and legal entity must obtain a person’s prior consent before collecting their personal data online. Consent given by those under the age of 16 years old is not considered valid. Those from 16 to 18 years old can give valid consent when in under the supervision of their legal guardian. Therefore, before collecting any information, a Brazilian company must be sure to ask whether the user is over 18 years of age. This policy also places an emphasis on the need for an easily understood privacy policy that explains how the personal data collected will be stored and used (“2019 Consumer Data” 2019).

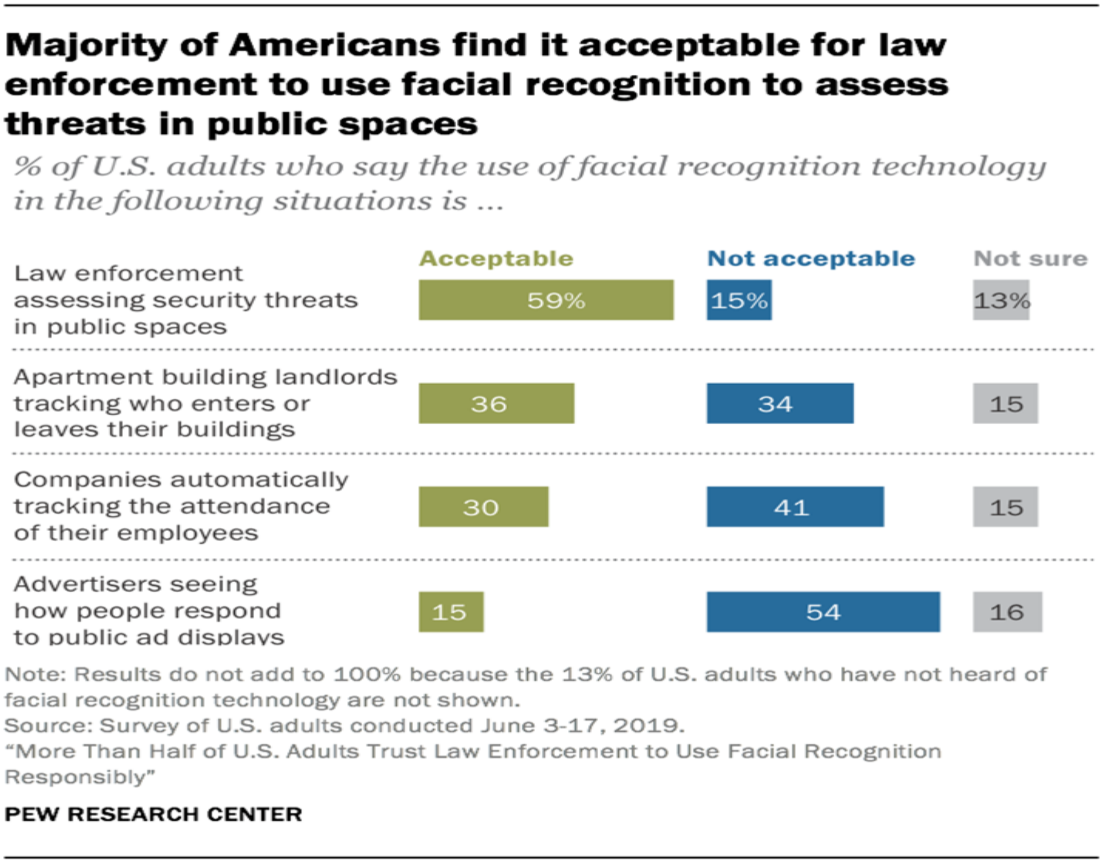
The General Data Protection Regulation (GDPR) created in the European Union (EU) became enforceable in 2018. It is currently the most vigorous privacy protection law in the world. It has since inspired other lawmakers across the world to up their requirements and has inspired the creation of new laws. The purpose of the GDPR is to protect people in the EU from unlawful data collection or processing and works to increase consent requirements, provide enhanced user rights and require a privacy policy that's written with ease and comprehension in mind (“What's Data Privacy” 2019). Concerns about privacy are heightened when breaches, cyberattacks, and illegal sharing of personal information are brought up in the media. The General Data Protection Regulation (GDPR) extended the EU’s jurisdiction beyond those countries. Any global business that sells to or has EU customers is subject to the GDPR, regardless of where that business is based. The GDPR sets forth comprehensive regulations about how companies treat the personal data of EU citizens, including those purchasing U.S. products or services or living in the U.S. (“2019 Consumer Data” 2019).

Future Laws:

United States Senators Roy Blunt and Brian Schatz, who are members of the Senate Committee on Commerce, Science, & Transportation, introduced the Commercial Facial Recognition Privacy Act of 2019. This bipartisan legislation would support and fortify consumer protections by prohibiting commercial users of facial recognition technology from collecting and re-sharing data for identifying or tracking consumers without their consent. “Consumers are increasingly concerned about how their data is being collected and used, including data collected through facial recognition technology,” said Senator Blunt. “That’s why we need guardrails to ensure that, as this technology continues to develop, it is implemented responsibly”. This proposed bill would increase the transparency and choice of consumers by requiring individuals to give informed consent before commercial entities can collect and share data gathered through facial recognition technology (“Commercial Facial Recognition” 2019). Under the bill, companies would be required to notify consumers when facial recognition is being used. It also requires third-party testing and human review of technologies prior to their implementation, this is used to address the accuracy and bias issues in the technology and avoid misuse cases that may result in harm to consumers. The bill restricts rearranging or circulating data to third-party entities without a valid form of consent from the end user. It also clearly explains data controllers and data processors in order to make requirements apparent and rigid for entities that either develop or sell facial recognition products or services, store facial recognition data, or implement these technologies on a physical premise. It would also require facial recognition providers to meet data security, minimization, and retention standards as determined by the Federal Trade Commission and the National Institute of Standards and Technology ("Commercial Facial Recognition" 2019).

Discussion and Implication:

The use of facial recognition technology has become commonplace in the daily lives of the average American. Facial recognition went from being used as a security measure to a source of self-identification. The overwhelming trend of the views of the general public towards the use



Majority of Americans find it acceptable for law enforcement to use facial recognition to assess threats in public spaces

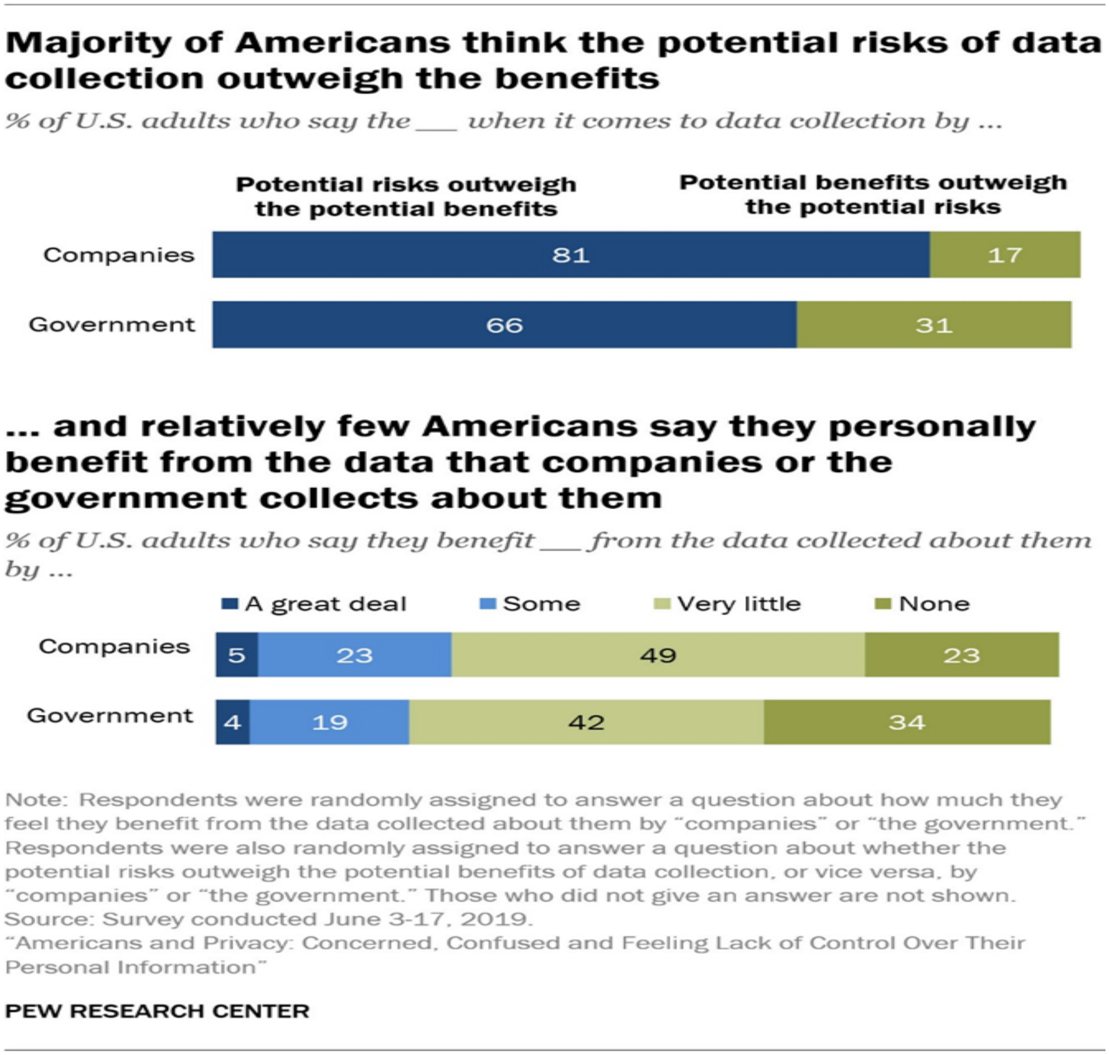
% of U.S. adults who say the use of facial recognition technology in the following situations is ...

Note: Results do not add to 100% because the 13% of U.S. adults who have not heard of facial recognition technology are not shown.
Source: Survey of U.S. adults conducted June 3-17, 2019.
"More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly"

PEW RESEARCH CENTER

of facial recognition is centered around who is using it, are they using it for marketing purposes, and is it being implemented for security reasons? According to a survey by Pew Research Center, as the monitoring bodies of ~~a~~ facial recognition systems move away from being law enforcement and protection services, the lower the approval rating that the implantation of the system will be. Similarly, as the monitoring bodies of a facial recognition system become more focused on marketing purposes the higher the disapproval rating will be.

There is a deep concern on the part of the public on the use of the biometric information that is being collected and how it can be used to personally identify an unsuspecting person in the future. This information can be misused and should be monitored. The security measures put in place to regulate the use of facial recognition technology should be strongly inclusive as to include future uses of the technology. Due to the projected growth of this market and the increased use of different applications of this technology, the longevity of this technology in a public setting is assured. Due to the interest of industry leading companies, like IBM, Facebook, and Amazon, there will be a large-scale implementation of this technology at an increased rate that will be used for security and access purposes. This is especially concerning due to the lack of knowledge and current data protection laws that pertain to facial recognition technology as the general public is concerned. The majority of Americans, according to Pew Research Center, are concerned that the potential risks of biometric data collection outweighs the potential security



Majority of Americans think the potential risks of data collection outweigh the benefits

% of U.S. adults who say the ___ when it comes to data collection by …

… and relatively few Americans say they personally benefit from the data that companies or the government collects about them

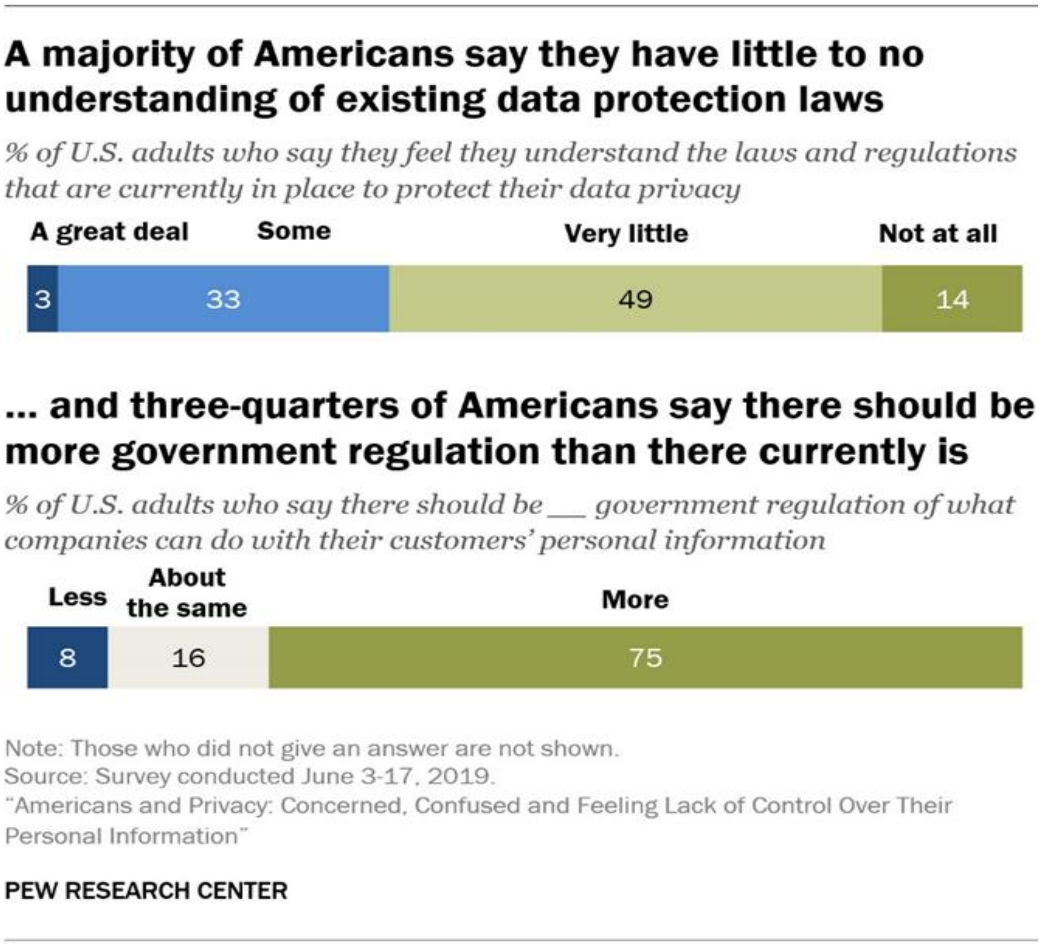
% of U.S. adults who say they benefit ___ from the data collected about them by …

Note: Respondents were randomly assigned to answer a question about how much they feel they benefit from the data collected about them by "companies" or "the government." Respondents were also randomly assigned to answer a question about whether the potential risks outweigh the potential benefits of data collection, or vice versa, by "companies" or "the government." Those who did not give an answer are not shown.
Source: Survey conducted June 3-17, 2019.
"Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information"

PEW RESEARCH CENTER

benefits. There are two main organizational groups that collect data on a large scale. These include companies and government organizations. The overall trend that Pew Research Center was able to determine was that the average adult in the United States (that was surveyed) does not feel the benefit from the data being collected and do not view the potential benefits of data collection as worth the overall risk in the case of both companies and governmental organizations.

There is a lack of understanding and application of current data protection laws in the United States and little to no coverage as it concerns facial recognition technology. This gap in



protection should be addressed due to the increased use of the biometric data collection systems with increased government regulations on the use of customers' personal information. This is echoed in a 2013 Pew Research survey that stated that 75% of adults in the United States would prefer more government regulation around the protection of personal data.

Conclusion:

From its origins in the mid-1960's facial recognition technology has been acknowledged for its potential for misuse when implemented in a national capacity. This can be accredited to its implicit biases for skin color and sex while also recognizing its potential privacy concerns. The use of facial recognition in the consumer sector is set to expand substantially over the next decade through its use by companies that will implement this type of technology to be used by their consumer base for security verification and identification. The databases required for the use of facial recognition technology are large-scale and are susceptible to data breaches and misuse. As demonstrated by the likelihood of a facial image of a black or East Asian person to be misidentified at a rate of 10 to 100 times that of a white face (Bushwick 2019).

Around the world, over 80 countries have created data privacy laws to protect the personal data of their citizens ("2019 Consumer Data" 2019). In Australia; clear and easily understandable privacy policies are required by the Australia's Privacy Principles (APP) to effectively protect users from the unauthorized usage of their personal information. The Brazilian Internet Act of 2014 was enacted to regulate the collection, maintenance, treatment, and use of personal data ("2019 Consumer Data" 2019). The General Data Protection Regulation (GDPR) was created to protect consumers from the illegal and ill-advised processing of personal data ("What's Data Privacy" 2019). In the United States, individual states, like Washington, Illinois, and Texas have ratified laws that prevent the sale of biometric information and have created restrictions on the security at which such information is stored. These individual state laws have also increased the requirements for consent authorized privacy policies for companies collecting personal and biometric information within the bounds of their specific state ("The Varying Laws" 2020). Although these state regulations have increased awareness of the legal implications of data misuse or misidentification, there is an extended need for legal action on the federal level to implement an encompassing measure to protect the personal and biometric data of consumers. The United States should implement a federal personal data privacy law that require a comprehensive and easily understood privacy policy that is accessible to all consumers, a guideline for the collection and use of the personal data collected, and a threat of legal repercussions if these general requirements are violated. Facial recognition technology has the hallmarks of a system that will be consistent in its use and explosive in its expansion of applications. Due to its current trend of longevity of use the need for legal regulations is heightened. Although the use of facial recognition technology provides a level of convenience and security the need to also protect the privacy of users should remain a top priority.

Work Cited

Ahmadi, Mohammad, et al. “A SWOT Analysis of Big Data.” *Journal of Education for Business*, vol. 91, no. 5, 2016, pp. 289–294.

“An Update About Face Recognition on Facebook.” About Facebook, 7 Nov. 2019, about.fb.com/news/2019/09/update-face-recognition/.

Auxier, Brooke, and Lee Rainie. “Key Takeaways on Americans' Views about Privacy, Surveillance and Data-Sharing.” Pew Research Center, Pew Research Center, 17 Aug. 2020, www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/.

Bushwick, Sophie. “How NIST Tested Facial Recognition Algorithms for Racial Bias.” Scientific American, Scientific American, 27 Dec. 2019, www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/.

Center, Electronic Privacy Information. “EPIC - State Facial Recognition Policy.” Electronic Privacy Information Center, epic.org/state-policy/facialrecognition/.

Chen, Lv, et al. “Automatic social signal analysis: Facial expression recognition using difference convolution neural network” Journal of Parallel and Distributed Computing, 131 (2019). pp. 97-102.

Chowdhury, Mozammel, et al. “Biometric Authentication Using Facial Recognition.” *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Security and Privacy in Communication Networks*, 2017, pp. 287–295.

“Commercial Facial Recognition Privacy Act of 2019 Introduced.” Security Magazine RSS, Security Magazine, 8 Apr. 2019, www.securitymagazine.com/articles/90097-commercial-facial-recognition-privacy-act-of-2019-introduced.

Dudley, Lauren "China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash." – The Diplomat, For The Diplomat, 7 Mar. 2020, thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/.

Germain, Thomas. "Facebook Settles $550 Million Facial Recognition Lawsuit." Consumer Reports, 30 Jan. 2020, www.consumerreports.org/lawsuits-settlements/facebook-settles-facial-recognition-lawsuit/.

Ghaffary, Shirin. "How Facial Recognition Became the Most Feared Technology in the US." Vox, Vox, 9 Aug. 2019, www.vox.com/recode/2019/8/9/20799022/facial-recognition-law.

"Global Facial Recognition Market Size, Share & Trends 2020-2027 - Facial Analytics Expected to Portray a Lucrative CAGR of 20.8% Over the Forecast Period - ResearchAndMarkets.com." Business Wire, 9 Apr. 2020, www.businesswire.com/news/home/20200409005340/en/Global-Facial-Recognition-Market-Size-Share-Trends.

Guo, Shangwei, et al. "Towards Efficient Privacy-Preserving Face Recognition in the Cloud." *Signal Processing*, vol. 164, 2019, pp. 320–328.

Kaye, Kate. This Little-Known Facial-Recognition Accuracy Test Has Big Influence, International Association of Privacy Professionals, 7 Jan 2019, iapp.org/news/a/this-little-known-facial-recognition-accuracy-test-has-big-influence/.

Loebel, Jens-Martin. "Is Privacy Dead? – An Inquiry into GPS-Based Geolocation and Facial Recognition Systems." *ICT Critical Infrastructures and Society IFIP Advances in Information and Communication Technology*, 2012, pp. 338–348.

Marr, Bernard. "Facial Recognition Technology: Here Are The Important Pros And Cons." Forbes, Forbes Magazine, 19 Aug. 2019, www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/.

Martin, Nicole. “The Major Concerns Around Facial Recognition Technology.” Forbes, Forbes Magazine, 25 Sept. 2019, www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/.

Raviv, Shaun. “The Secret History of Facial Recognition.” Wired, Conde Nast, 21 Jan. 2020, www.wired.com/story/secret-history-facial-recognition/.

Samet, Alexandra. “Facial Recognition Has Been Championed for Keeping Data Safe - but Some Targeting Practices Are Making Customers Uneasy.” Business Insider, Business Insider, 11 Feb. 2020, www.businessinsider.com/facial-recognition-privacy-safety-trends.

Smith, Aaron. “More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly.” Pew Research Center: Internet, Science &amp; Tech, Pew Research Center, 27 Aug. 2020, www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.

Steinke, Gerhard. “Data Privacy Approaches from US and EU Perspectives.” *Telematics and Informatics*, vol. 19, no. 2, 2002, pp. 193–200.

“The Varying Laws Governing Facial Recognition Technology.” *IPWatchdog.com | Patents & Patent Law*, 27 Jan. 2020, www.ipwatchdog.com/2020/01/28/varying-laws-governing-facial-recognition-technology/id=118240/.

Tran, Hong-Yen, and Jiankun Hu. “Privacy-Preserving Big Data Analytics a Comprehensive Survey.” *Journal of Parallel and Distributed Computing*, vol. 134, 2019, pp. 207–218.

“What's Data Privacy Law In Your Country?” Privacy Policies, www.privacypolicies.com/blog/privacy-law-by-country/.

“2019 Consumer Data Privacy Legislation”, National Conference of State Legislatures, www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.