Huahao Zhou

Professor Feigenbaum

CPSC 610

10 December 2019

Facial Recognition Technology: its Benefits, Risks, and Potential Regulations

Introduction

Facial Recognition Technology (FRT) and its regulation have made many headlines as companies and governments apply it to areas such as surveillance, law enforcement, and business. The United States blacklisted 28 Chinese entities that use FRT to identify Muslim minorities in China on October 7, 2019 (Swanson, and Mozur). Domestically, cities such as San Francisco, Oakland, and Somerville have banned the use of facial recognition technology across local agencies, including transport authority and law enforcement (Metz). In the private sector, on March 14, 2019, a bipartisan bill called the Commercial Facial Recognition Privacy Act, was introduced by senators to offer legislative oversight on the commercial application of facial recognition (Hatmaker). In light of such events, it is evident that there are increasingly more regulations on FRT in both the public and private sectors.

Still, no well-established and unanimous regulations exist in the United States in either the public or private sector; it is imperative to think about possible nationwide effective regulations. How can we protect people's privacy and liberty without disincentivizing business from innovating or hindering governments from using technology for the benefit of its citizens?

We need a set of regulations that balance the protection of people's rights, leave room for beneficial use of FRT, and facilitate technological innovation. I propose that future regulations should encompass the following four categories. First, prohibit facial recognition algorithms with lower than 99% accuracy or proven bias on a particular minority group from entering the market. Second, ban law enforcement from using FRT with body cameras, real-time tracking, and operations related to the investigation of immigrants with FRT. Third, only allow law enforcement's use of FTR with a court order to situations where the benefits far outweigh the risks, such as terrorist attacks. Forth, require both government agencies and private companies to obtain affirmative consent from users and citizens to safeguard the privacy of user and citizens while leaving room for technological innovation and business growth. To show that, I will first explain what is FRT and how it works. I will then unpack the benefits and risks of FRT. With the motivation to amplify the benefits and mitigate the risks, I will look at the current regulations in the US and finally propose four sets of guidelines for future regulations in the United States.

What is FRT? How Does it work?

Facial Recognition Technology is a pattern recognition technology to identify or verify a person through photos or videos (Introna and Nissenb 10). More specifically, it detects a face in an image, estimates personal characteristics, verifies people's identify with face, or identifies an individual by matching an image of an unknown person to a gallery of known people (Gao 4).

FRT consists of four major steps. First, a camera captures an image from its photos or videos. Second, the image is processed by an algorithm to create a facial template (also called face print). A face template uses numerical values to describe some features of a face, such as

color and spatial relationship between different parts of a face (Gao 8). Depending on the numerical representation used, there are three approaches to create a facial template: geometric approach, photometric approach, and skin texture analysis (Gao 8). The geometric approach records the location and spatial relationship between different parts of a face, such as the location of the mouth and its distance to the center of the eyes (Tian 2). The photometric approach tries to decompose a face into a weighted sum of other standard facial templates, and it records those weights and referenced standard templates as the numerical representation of the new facial template (Yang et al. 39). The last approach, skin texture analysis, takes advantage of the fact that various small scale structures in the surface (wrinkles, scars) and the texture can help differentiate human faces. It records parameters associated with these scale structures and texture to identify faces (Pierrard and Vetter 1). These three approaches are used either separately or collectively to build a face template depending on the FRT algorithm. With a constructed face template, the third step is to use machine learning algorithms such as neural networks to match the face template with the existing image in the database. Once the similarity score passes a certain threshold, the FRT will deem there is a match between the targeting face and a face in the existing database (Gao 8).

Benefits

FRT has a wide range of applications, and it could bring benefits to many facets of our lives. I have put these benefits into six categories and listed them in order of their significance. These six categories include 1) improving public security, 2) assisting with more accurate diagnosis and offering better support in medical care, 3) refining errors and improving algorithm

performances with more user feedback and larger training set, 4) verifying identity for security purposes, such as financial transactions, 5) commercial usage to increase the convenience and personalization of service, 6) and incentivizing other creative usage and innovation.

One of the most significant benefits of FRT is its effective protection of public security by identifying wanted criminals and finding missing people. Castro from the Information Technology & Innovation Foundation argues that the current crime investigation model of manually identifying criminals in videos or asking witnesses to provide clues is not only costly but also ineffective (Castro). However, the FRT reduces the cost of searching wanted criminals and increases efficiency and accuracy. Some successful cases have proven Castro's point. For example, FRT helped the Maryland police to scan through the mug shots and identify Jarrod Ramos, a suspect who currently faces five charges for first-degree murder, when he refused to identify himself (Bosman and Kovaleski). Most citizens would likely to be comfortable with this kind of use of facial recognition technology to improve public safety(Bala and Watney). Some private users such as shop owners also use FRT cameras to alter themselves with the appearance of frequent thieves (Chivers). In addition to identifying wanted criminals, FRT's utility in detecting missing people has been exemplified by the case in India. The police in New Delhi identified nearly 3,000 missing children within just four days with help from FRT (Cuthbertson). FRT software has also been developed to help identify human trafficking victims by matching the photos of missing people and those on sex advertisements (Ossola).

FRT could also extend people's ability to perceive things and make more accurate judgments. In the medical field, doctors could use FTR to predict potential genetic diseases from a person's face and recommend preventive solutions. A Boston based startup, Face2Gene, tries to

identify possible genetic diseases from a patient's face pictures. The FRT from them could outperform human doctors in spotting patients with conditions such as Angelman syndrome and Cornelia de Lange (Kaminsky). For people with prosopagnosia (face blindness) and other memory-related conditions, memory support applications with FRT in smartphones could assist them well by confirming the identities and providing the names of family members, friends, and caregivers (Rivolta 344). Therefore, FRT could both help doctors to make diagnoses and patients to extend their perceptive capabilities.

Another significant benefit of using FRT is the potential to refine current errors of this technology, to enlarge the data set enabling smarter learning algorithms, and to incentivize computer scientists and companies to further develop FRT for future potential benefits. Looking back at the development of FRT, facial recognition systems got 20 times better at finding a match in a database of 12m portrait photos between 2014 and 2018 according to the National Institute of Standards and Technology (NIST). These large improvements are closely related to the open space for the FRT application and research. If the technology were banned, technology companies would not have had enough incentive to invest in and research FRT that could bring innovation and business profit. Without enough research and application, we could not have improved the accuracy of FRT and kept refining errors. Therefore, opening enough space for the application and research of FRT stimulates a virtuous cycle for advancing this technology and increasing its benefits for people.

Many other use cases utilize FRT to verify people's identity to avoid identity fraud, protect user's privacy, and ensure the security of data and property. Among the wide range of use cases to verify identity for access, the most significant ones are associated with higher stakes

because they control access to important information and properties. For example, FRT can be used to authorize government employees at high-security facilities (Bala and Watney). Some banks already have Auto Teller Machines (ATM) with FRT to facilitate the money withdraw process; the process with FRT is arguably safer because only knowing the passcode would not help the thieves to withdraw the money (Soo). In the case where people are forced to withdraw money, FRT also provides a chance to record the situation and provide visible evidence for future investigation. Newer fin-tech companies like Alipay has also made the "pay with your face" function available on their app (Ren). Additionally, many smartphones have already implemented FRT as a way to unlock and their phones as an alternative to passwords (Dospinescu and Popa 20).

FRT also brings in personalization and innovation to many other services. Two examples include personalized advertisements in stores with information from FRT cameras, and many social media functions based on FRT. In New York and Chicago, an advertising company called Cooler Screens has already partnered with advertisers like Red Bull, Coca-Cola and Pepsi to change ads on the door of grocery stores depending on the different information from facial scanning various customers (Kuligowski). For example, if the camera captures a cluster of faces of family members together entering the store, the door might recommend newly-designed family packs for different drinks. Many social media use FRT to create an innovative experience and entertain users. For example, FaceApp can capture a person's face to predict what people will look like when they are older, younger, or in different genders (Hoffman and Bates). Facebook also has a function of tagging friends by automatically analyzing who is in the same picture with FRT. Although these applications of FRT could be fun and effective social and

business tools, their benefits are arguably less fundamental compared to previous benefits such as protecting public security. Therefore, we need to put these different levels of benefits in mind when we try to set rules for different use cases.

Risks and Concerns

Although FRT brings many benefits in both public and private use cases, it also leads to two main types of risks. The first type of risk results from the imperfection of the technology, such as an error in identification and biases that arise when identifying people from different identity groups. The second type of risk comes from the impact that FRT, even with a perfect error rate and zero bias, will have on people's privacy and freedom. The risks of this kind include continuously tracking people, infringing on people's freedom of speech and assembly, and disproportionately targeting minority groups, such as undocumented immigrants.

If the police and other law enforcement agencies make decisions to stop or arrest suspects solely based on FRT, the existing errors in this technology could exacerbate the burden of innocent citizens and violate their freedom from unreasonable search, a right protected by the Fourth Amendment. There is still debate on whether the FRT results can constitute a probable cause; current FRT does not have a 100 percent accurate matching rate, and there are many cases of false positives. In these cases, if the police choose to stop or arrest the matched suspect for interrogation, the suspect is bearing more burdens (such as delayed travel time and temporary loss of freedom) than they need to. As previously mentioned, the Fourth Amendment of the Constitution protects citizens from unreasonable searches. Law enforcement agencies need to have a court warrant or probable cause to arrest and search people. Probable cause is commonly

defined as "a reasonable amount of suspicion, supported by circumstances sufficiently strong to justify a prudent and cautious person's belief that certain facts are probably true" (Trainum 65). But the question is, can potentially false results from FRT still constitute a probable cause? Currently, no law explicitly states whether or not FRT could be used as probable cause. One can argue that given that the good FRT algorithm like GaussianFace could achieve an accuracy level of 98.52 percent (Lu and Cao 3811), there is a high chance that the suspect matched with FRT is indeed the criminal in question. Thus, it is reasonable to support the usage of FRT results to search. Being extra cautious with potential criminals and taking actions to stop and search them will also develop community safety. However, statistically speaking, here is still 1.48 percent of the matched people who will be wrongly stopped and the absolute number is not small. If FRT is massively used on all Americans, nearly five million people will be wrongly identified as criminals. If the police are allowed to conduct search on them, their freedom granted by the fourth amendment will be violated. Because any one of us could fall into a victim of the error, we all face the risk of losing the freedom from unreasonable search. Therefore, there is a need for regulations to wisely keep the balance between public safety and individual rights.

Besides the errors in the overall identification success rate, several studies have shown that many FRT algorithms have discriminative accuracy in identifying faces of different ages, genders, and racial groups. In situations where extreme importance is assigned to the facial recognition results, such as in criminal investigations, these biased results will unfairly assign more burdens on groups that have a lower accurate matching rate. Researchers like Timnit Gebru from Microsoft Research and Joy Buolamwini from MIT Media Lab have shown that "facial recognition has greater difficulty differentiating between men and women the darker their skin

tone". Across the FRTs from Microsoft, IBM, and Face++, the error rates of darker-skinned females were as high as 34.7 percent while the maximum error rate for lighter-skinned males was 0.8 percent (Timnit Gebru and Joy Buolamwini 1). Gebru explains that, although about 130 million US adults are already in face recognition databases, the original datasets are mostly white and male. As a result, some algorithms are biased against darker skin types (Wall). Additionally, many facial recognition algorithms are trained on CelebFaces Attributes Dataset (CelebA), a large-scale face attributes dataset with more than 200 thousand celebrity images (celebrity images are relatively easy to get and each image is labeled with 40 attribute annotations in the CelebA (Liu et al.)). Because there are far more white celebrities than those from other ethnic groups, those algorithms also identify the white population more accurately. Given the lower accuracy rate in minority groups, some high-stakes usages of FRT, such as law enforcement, could unfairly assign more burden and lead to discriminatory treatments on minority groups. The discriminatory treatment violates the principle of equality, one of the most fundamental human rights and building blocks of a democratic society.

Even if FRT's accuracy will be improved to nearly 100% in the future, the second type of risk of infringing privacy and increasing surveillance still prevail. FRT gives the government and private companies tremendous power to track individuals, and the lack of transparency in their current data collection and data usage poses a further threat to people's privacy and autonomy. If there are ubiquitous cameras with FRT in both public places and private shops on the street, the government and private entities can just track where people went. If the social media platforms analyze all the tagged photos of a user, they might know who the user is friends with, what activities he or she likes to do, and other private information that the companies would not know

without FRT. If that information is not related to public affairs, either the government or company has the right to attain that piece of information from FRT. What is even worse, we are unaware of other ways in which our privacy is intruded on due to the lack of transparency in data collection and data usage in both government and private entities. For example, Georgetown Law's Center on Privacy and Technology has found from investigation that the FBI use databases with over 400 million photos for face matching, and those photos include driver's license photos and passport application photos (LeBlanc). In other words, the FBI is using people's photo that is merely intended to apply for a driver's license or passport without their consent. In the private sphere, Facebook was alleged by Illinois citizens that "they didn't consent to have their uploaded photos scanned with facial recognition and weren't informed of how long the data would be saved when the mapping started in 2011" (Constine). Both cases suggest that we can see that future regulations need to hold both public and private entities accountable by requiring transparency on their data policies and regulating certain use cases. I will discuss this more in detail in the next section.

The infringement on people's privacy will naturally lead to more surveillance, which threatens the core of a democratic society: freedom of speech and freedom of assembly. The increased surveillance makes even the most minor of crimes unescapable and hurts some of the most vulnerable communities, such as undocumented immigrants. If the police use FRT to identify and track participants in protests, people would become afraid that their presence in protests or speeches on political issues might bear larger ramifications. They will then choose to silence themselves or feel hesitant to go to protests, rather than voicing their opinion vocally. For example, many attendees in LGBTQ-rights protests prefer not to reveal their identity to the

public or government in fear of consequential discrimination and unfair treatment. If the police begin to associate the protestors' faces with their names and other private information, protestors will be heavily disincentivized from openly fighting for LGBTQ rights. In this case, the surveillance supported by FRT encourages citizens to censor themselves, thus hurting democracy and social advancement by not allowing every citizen to fully participate in free expression. If the police utilize FRT on the street, every nook and cranny of cities would be under surveillance. Even a minor jaywalking incident would be caught by the camera and the offender promptly identified. The negative impact is even greater for more vulnerable communities, such as undocumented immigrants. Currently, U.S. Immigration and Customs Enforcement (ICE) uses FRT to identify the parents of undocumented immigrants, allowing them to separate families. Given the large negative consequences of surveillance due to FRT, there is an urgent need for regulations to safeguard its proper use to protect democratic values, freedom in society, and vulnerable minority groups.

Current Policies

On the federal level, while there are pending bills in Congress intending to regulate both federal law enforcement agencies and private entities, there is still no FRT-specific law to regulate either government or companies on the use of FRT. Currently, For FRT-specific regulation on private entities, the Congress is still discussing the newly-introduced bill, *S.847 Commercial Facial Recognition Privacy Act of 2019*. This bill tries to prohibit commercial entities "from using facial recognition technology to identify or track an end-user without obtaining the affirmative consent of the end-user, and for other purposes" (Blunt and Schatz 1).

In other words, users will be asked if they give consent to private companies to collect and use their facial information to provide services with FRT. In terms of the regulations on federal law enforcement agencies, *The Facial Recognition Technology Warrant Act of 2019* was just introduced on November 14, 2019, to "require federal law enforcement to obtain a court order before using facial recognition technology to conduct targeted ongoing public surveillance" (Coons and Lee). This bill is trying to limit the use of FRT to only severe crimes and reduce intrusion on privacy.

On the state and city levels, there are more FRT-specific regulations, but these regulations are far from most effective. The cities of San Francisco, Oakland in California and the city of Somerville in Massachusetts have banned FRT in city agencies (Metz). Detroit only allows FRT to assist in the investigation of violent crimes and home invasions in no real-time. In other words, the police officers cannot use FRT to detect crime in real-time; they can only use it as an aftermath investigation tool (Einhorn). Additionally, California, New Hampshire, and Oregon have banned law enforcement from using FRT in body cameras (Garvie 22). These current regulations have shown that most cities and states do not have a safeguard to use FRT, which highlights the importance of having federal level regulations to effectively contain the risks of FRT on a national scale.

Policy Recommendations

Having understood both the benefits and potential risks of FRT, we need a set of rules that protects the privacy and liberty of people without disincentivizing business from innovating or hindering governments from using the technology for the benefit of its citizens. I propose that

future regulations should encompass the following four categories. First, prohibit facial recognition algorithms with lower than 99% accuracy or proven bias on a particular minority group from entering the market. Second, ban law enforcement from using FRT with body cameras, real-time tracking, and operations related to the investigation of immigrants with FRT. Third, only allow law enforcement's use of FTR with a court order to situations where the benefits far outweigh the risks, such as terrorist attacks. Forth, require both government agencies and private companies to obtain affirmative consent from users and citizens to safeguard their privacy while leaving room for technological innovation and business growth.

Legislators should regard ensuring equity and accuracy in FRT as a priority because these are the cornerstones of applying FRT to benefit humans; equity is one of the most fundamental values in a democratic society, and accuracy makes it possible for us to trust FRT in the first place. I propose that federal laws should prohibit any use of FRT technology with a lower than 99% accuracy in real-life conditions such as poor lighting and disparate biased rates towards groups, including but not limited to different ethnic, gender and age groups. Providers of FRT should pass the accuracy and bias test in NIST (National Institute of Standards and Technology) in order to sell their product to either law enforcement or private entities. The number 99% comes from two reasons. First, the human benchmark of successfully identifying faces is 97.53%, so the FRT needs to perform better than humans to assist us (Chowdhry). Second, right now most companies have not achieved the 99% accuracy rate in real-life conditions (Google's FaceNet has 99.63% success rate and Facebook's Deepface has 97.25% success rate (Gemalto)), so the 99% accuracy rate in real-world condition serves as motivation for companies to develop

more accurate technologies while keeping the error rate arguably lower to 1%. Bias should also be tested alongside the overall success rate to ensure the fairness of the technology.

Although we want to see more accurate technology with less bias, more perfect technology also means more surveillance and a potential threat to privacy. Therefore, we need a second set of rules to regulate massive surveillance. Because citizens and users might not be able to opt-out of FRT in public places or they do not have enough knowledge to informed decisions to opt-out of an FRT-based private service to protect themselves, regulations should ban use cases that bring enormous risk but few benefits to effectively protect users and citizens. These use cases include real-time facial recognition without a court warrant, body cameras with FRT, and the use of FRT to target undocumented immigrants for both law enforcement and private companies. It is an overkill to use real-time facial recognition 24/7 in public to catch criminals because it inherently tracks everyone's behaviors and causes people to censor themselves to participant in free speech and demonstration and only catching criminals could justify the use of massive surveillance at that scale. The portion of severe criminals are low, and they will avoid going to areas with FRT. Therefore, FRT should only serve FRT as an investigation in non-real time with the warrant from the court to help arrest severe criminals and reduce massive surveillance. Similarly, body cameras also drastically increase surveillance without necessarily improving public safety. It breaks the traditionally fixed boundary of surveillance areas and makes citizens feel watched in any place. Additionally, the use of FRT on undocumented immigrants presents serious discriminatory and moral problems. Even with perfect accuracy in the technology itself, law enforcement agencies might still apply this technology more to ethnical minorities because of the unconscious bias of the immigration status of the non-Caucasian

population. FRT could help to separate families and make some politicians more popular without actually improving public safety. In fact, several criminologists in recent research found that "illegal immigrants report engaging in less crime prior to and following their first arrest than legal immigrants and native-born Americans" (Bianca el al.). Although there might be other new future use cases that I might not have discussed, the same principle of weighing its risks and benefits should still be applicable.

Rather than simply banning all usage of FRT in public agencies, like what San Francisco and several other cities have done, leaving some room for cautious and responsible use of FRT under critical circumstances might be extremely beneficial to the public while mitigating risks at a low level. Therefore, the third set of regulations aims to clarify when and how law enforcement could use FTR to maximize the public benefits. The recent pending bill, *The Facial Recognition Technology Warrant Act of 2019*, provides a good framework to the above questions, but there is still controversy on the legal surveillance of fewer than 72 hours, and it still needs to address the problem of using non-consensual data. This bill requires covered court order based on probable cause showing of criminal activity to conduct ongoing public surveillance of an individual exceeding 72 hours; in special circumstances, the law enforcement can use FTR and apply after within 48 hours (Coons and Lee 3). It also requires a human review of the results of FRT before taking further actions and reports from both courts and agencies to reveal the number of court orders applied and granted (Coons and Lee 11). While this bill provides room for law enforcement to use FRT in an accountable manner, I argue that the permission of fewer than 72 hours surveillance is too long of a time period and it should not allow the law enforcement to start using it without a court order or similar procedures in special circumstances. This will help

us to reduce mass surveillance. Moreover, the bill also fails to address the problem of law enforcement agencies like ICE and FBI use non-consensual photos from DMV database (Harwell). This loophole leads to the last set of regulations related to affirmative consent.

As suggested before, the last set of regulations should enforce affirmative consent as the last safeguard for users and citizens to protect themselves while leaving some room for technical innovation and business growth. The pending bill, *Commercial Facial Recognition Privacy Act of 2019*, has set up a good framework of requiring user's affirmative consent to collect and use data for private companies, but it does not regulate government agency. Therefore, regulations should require both private companies and the government to ask for affirmative consent from users and citizens. Affirmative consent means the individual understands the full process of the data collection and data usage and they give voluntary and explicit agreement to this process (Blunt and Schatz 1). This means that individuals should have the right to reject their data being collected without being denied from services; they could also request to delete the data from the database at any time, and the companies should be banned from using data for other purposes than those stated in the original consent (Blunt and Schatz). Because the previous three sets of regulations have banned use cases that could bring detrimental harm such as mass surveillance and imprisonment, the rest use cases have arguably less risk and potentially more benefits. Therefore, the law should give people the freedom to weigh their personal risks and benefits to make their own decisions. For example, the collection of face pictures in order to get a diagnosis from FRT-powered medical acquire the consent from patients. On the other hand, patients also enjoy the right to have the opportunity to seek a diagnosis from FRT. This mutually benefits consent also gives medical software companies incentives to further develop technologies that

could be beneficial to our society. Furthermore, this set of regulations should also apply to government agencies. With the affirmative consent requirement, individuals could reject DMV's sharing photos with ICE and FBI, which gives individual power to protect their own privacy and to hold the government committed to the original consent of how they can use collected data.

Conclusion

FRT has huge potential to improve public security, extend human's ability to detect diseases, secure access to important assets, and stimulate further technological and business innovation. However, it also has potential risks coming from both its "imperfection" and the "perfection". The error rate and biases could exacerbate the burden of innocent citizens and violate the equality principle. The unregulated and massive use of FRT will infringe on people's privacy and liberty.

Although there are some state and city level regulations on FRT, many states still do not have FRT specific regulations and there is no federal law that is specifically dedicated to FRT. In order to effectively promote the benefits and mitigate the risks of FRT on a national level, I have proposed a regulation guideline that consists of four sets of rules that complement each other. On the one hand, we heavily limit the use of FRT. To mitigate the risks of matching errors and identification biases, we need to prohibit facial recognition algorithms with lower than 99% accuracy or proven bias on a particular minority group from entering the market. For use cases that have far more detrimental risks than marginal benefits, the law should ban the use of FRT in those cases to protect individuals who are unable to make informed decisions or protect themselves. On the other hand, we also create room for FRT use to utilize its benefits, encourage

technological innovation, and facilitate business growth. We use the court order to allow law enforcement to use FRT as an investigation tool to improve public safety without mass surveillance. In addition, we should also enforce assertive consent as both a bridge and safeguard - it creates a voluntary contract between users and companies, individuals and governments for the possible use of FRT, business growth, and further technological innovation; it also serves as the last safeguard to protect individual privacy and freedom. Future legislation could follow the above guidelines and fill the details to form a mature FRT regulation system.

Works Cited

"Privacy Act Of 1974; Department Of Homeland Security/United States Customs And Border Protection-016 Nonimmigrant And Immigrant Information System". *Federal Register*, 2019, https://www.federalregister.gov/documents/2015/03/13/2015-05804/privacy-act-of-1974-department-of-homeland-securityunited-states-customs-and-border-protection-016.

Bala, Nila, and Caleb Watney. "What Are The Proper Limits On Police Use Of Facial Recognition?". *Brookings*, 2019.

Bersani, Bianca et al. *Investigating The Offending Histories Of Undocumented Immigrants*. 2019.

Blunt, Roy, and Brian Schatz. "Text - S.847 - 116Th Congress (2019-2020): Commercial Facial Recognition Privacy Act Of 2019". *Congress.Gov*, 2019, https://www.congress.gov/bill/116th-congress/senate-bill/847/text.

Bosman, Julie, and Serge Kovaleski. "Facial Recognition: Dawn Of Dystopia, Or Just The New Fingerprint?". *Nytimes.Com*, 2019, https://www.nytimes.com/2019/05/18/us/facial-recognition-police.html.

Castro, Daniel. "Statement To The House Committee On Oversight And Reform Regarding Facial Recognition And Civil Liberties". *Itif.Org*, 2019,

https://itif.org/publications/2019/05/22/statement-house-committee-oversight-and-reform-regarding-facial-recognition.

Chivers, Tom. "Facial Recognition… Coming To A Supermarket Near You". *The Guardian*, 2019, https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties.

Chowdhry, Amit. "Facebook's Deepface Software Can Match Faces With 97.25% Accuracy". *Forbes.Com*, 2019, https://www.forbes.com/sites/amitchowdhry/2014/03/18/facebooks-deepface-software-can-match-faces-with-97-25-accuracy/#2bea121554fc.

Constine, Josh. "$35B Face Data Lawsuit Against Facebook Will Proceed – Techcrunch". *Techcrunch*, 2019, https://techcrunch.com/2019/10/18/facebook-35-billion-lawsuit/.

Coons, Chris, and Mike Lee. *Coons.Senate.Gov*, 2019, https://www.coons.senate.gov/imo/media/doc/FRTWA%20One-Pager%20FinalFinal.pdf.

Cuthbertson, Anthony. "Police Trace 3,000 Missing Children In Just Four Days Using Facial Recognition Technology". *The Independent*, 2019,

https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html.

Dospinescu, Octavian, and Iulian Popa. "Face Detection And Face Recognition In Android Mobile Applications". *Informatica Economica*, vol 20, no. 1/2016, 2016, pp. 20-28. *ECO-INFOSOC Research Center*, doi:10.12948/issn14531305/20.1.2016.02.

Einhorn, Erin. "Detroit Police Can Keep Using Facial Recognition — With Limits". *NBC News*, 2019, https://www.nbcnews.com/news/us-news/detroit-police-can-keep-using-facial-recognition-limits-n1056706.

Gao, Gao. *Gao.Gov*, 2019, https://www.gao.gov/assets/680/671764.pdf.

Garvie, Clare. *Docs.House.Gov*, 2019, https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-GarvieC-20190522.pdf.

Gemalto, Gemalto. "Facial Recognition In 2020: 7 Trends To Watch | Gemalto". *Gemalto.Com*, 2019, https://www.gemalto.com/govt/biometrics/facial-recognition.

Harwell, Drew. 2019, https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-driver

s-license-photos-are-gold-mine-facial-recognition-searches/. Accessed 21 Dec 2019.

Hatmaker, Taylor. "Bipartisan Bill Proposes Oversight For Commercial Facial Recognition – Techcrunch". *Techcrunch*, 2019, https://techcrunch.com/2019/03/14/facial-recognition-bill-commercial-facial-recognition-privacy-act/.

Hoffman, Ashley, and Josiah Bates. "Https://Time.Com". *Time*, 2019, https://time.com/5628141/face-app-challenge/.

Introna, Lucas, and Helen Nissenbaum. *Nissenbaum.Tech.Cornell.Edu*, 2019, https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf.

Kaminsky, Leah. "The Invisible Warning Signs That Predict Your Future Health". *Bbc.Com*, 2019, https://www.bbc.com/future/article/20190116-the-invisible-warning-signs-that-predict-your-future-health.

Kuligowski, Kiely. "Facial Recognition Advertising Targets Customers". *Business News Daily*, 2019, https://www.businessnewsdaily.com/15213-walgreens-facial-recognition.html.

LeBlanc, Paul. "Washington Post: ICE, FBI Use State Driver's License Photos For Facial-Recognition Scans". *CNN*, 2019,

https://edition.cnn.com/2019/07/08/politics/fbi-ice-driver-license-photos-facial-recognition/index.html.

Liu, Ziwei et al. "Large-Scale Celebfaces Attributes (Celeba) Dataset". *Mmlab.Ie.Cuhk.Edu.Hk*, 2019, http://mmlab.ie.cuhk.edu.hk/projects/CelebA.html.

Lu, Chaochao, and Xiaoou Tang. "Surpassing Human-Level Face Verification Performance On LFW With Gaussianface". *Arxiv.Org*, 2019, https://arxiv.org/abs/1404.3840.

Metz, Rachel. 2019, https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html. Accessed 21 Dec 2019.

NIST, NIST. "NIST Evaluation Shows Advance In Face Recognition Software'S Capabilities". *NIST*, 2019, https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities.

NIST, NIST. "NIST Evaluation Shows Advance In Face Recognition Software'S Capabilities". *NIST*, 2019, https://www.nist.gov/news-events/news/2018/11/nist-evaluation-shows-advance-face-recognition-softwares-capabilities.

Ossola, Alexandra. "AI Tool Helps Law Enforcement Find Victims Of Human Trafficking". *Futurism*, 2019, https://futurism.com/ai-tool-law-enforcement-stop-human-trafficking.

Pierrard, Jean-Sebastien, and Thomas Vetter. *Citeseerx.Ist.Psu.Edu*, 2019, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.154.6540&rep=rep1&type=pdf.

Ren, Rebecca. "Pay With Your Face In China: A Choice Of Convenience Or Security- Pingwest". *Pingwest*, 2019, https://en.pingwest.com/a/2744.

Rivolta, Davide et al. "Covert Face Recognition In Congenital Prosopagnosia: A Group Study". *Cortex*, vol 48, no. 3, 2012, pp. 344-352. *Elsevier BV*, doi:10.1016/j.cortex.2011.01.005.

Soo, Zen. "Bye-Bye Bank Cards? Chinese Lender Launches Atms With Facial Recognition Software In Shenzhen Ahead Of Nationwide Roll-Out". *South China Morning Post*, 2019, https://www.scmp.com/tech/innovation/article/1867831/bye-bye-bank-cards-chinese-lender-launches-atms-facial-recognition.

Swanson, Ana, and Paul Mozur. "U.S. Blacklists 28 Chinese Entities Over Abuses In Xinjiang". *Nytimes.Com*, 2019,

https://www.nytimes.com/2019/10/07/us/politics/us-to-blacklist-28-chinese-entities-over-abuses-in-xinjiang.html.

Tian, Ying-li. "Evaluation Of Face Resolution For Expression Analysis - IEEE Conference Publication". *Ieeexplore.Ieee.Org*, 2019, https://ieeexplore.ieee.org/abstract/document/1384875/.

Trainum, James L. *HOW THE POLICE GENERATE FALSE CONFESSIONS*. ROWMAN & LITTLEFIELD, 2018, p. 65.

Wall, Matthew. "Biased And Wrong? Facial Recognition Tech In The Dock". *BBC News*, 2019, https://www.bbc.com/news/business-48842750.

Yang, Ming-Hsuan et al. "Detecting Faces In Images: A Survey". *Pdfs.Semanticscholar.Org*, 2019, https://pdfs.semanticscholar.org/4a92/251e62be8fc2f4cbdff6e7314305bffdf2c4.pdf.