Intersect, Vol 15, No 2 (2022)

Why the US Needs Federal Law on Facial Recognition Technology

Huseyn Panahov
Georgetown University

Abstract

Since the beginning of the 2000s, Facial Recognition Technology (FRT) has become significantly more accurate and more accessible. Both government and commercial entities use it in increasingly innovative approaches. News agencies use it to spot celebrities at big events. Car companies install it on dashboards to alert drivers falling asleep at the wheel. Governments have used it to track Covid-19 patients' compliance with quarantine regimes, or to reunite missing children with their families. However, as the use of technology has become more widespread, the controversies around it have also grown. The technology offers tremendous opportunities, but there are reasons to be concerned about its impact on privacy and civil liberties, if it is not used properly. In this paper, I make a brief introduction to facial recognition technology, look separately at commercial and government applications of it, and present my argument why the US needs a federal legislation on FRT.

1. The nuts and bolts of FRT

Facial recognition falls under the category of biometric data. The software pinpoints facial landmarks, measures the distance between them, and creates a geometric shape of your face. It is less accurate than other biometric identifiers, such as iris and or fingerprint scanning, because of two reasons. One, facial images are not always of high quality. Two, unlike other biometric identifiers, facial features can change over time, due to aging, plastic surgery, cosmetics, effects of drug abuse or smoking, etc. However, FRT has become a lot more popular, because it can be used remotely and is a lot easier to apply in high traffic places.

Today, facial recognition is used mainly for two reasons. First, **face verification**, also, known as “one-to-one” matching. It is used to verify that you are who you say you are. It is commonly used to unlock a smartphone or replace ID checks. Second, **face identification**, also, known as “one-to-many” matching. Usually used to search for persons of interest, where you start the search with an image of a person you do not know to determine his/her identity.

Another category is facial analysis, where the algorithm analyses facial features to determine “age, gender, ethnicity, emotions, fitness for certain jobs.” For example, McDonald’s has used facial analysis in its Japanese stores to check if the employees are smiling, when assisting the customers. Walmart is working on a facial analysis system that will help to process the shoppers’ mood while they are in a store. There have been numerous reports that China is using facial analysis to track ethnic Uighurs, a largely Muslim group in the western province of Xinjiang. Reportedly, the technology can distinguish “Uighur/non-Uighur attributes”, and allows the Chinese police to track the movements of the minority group. While the reports of the Chinese government crackdown on Uighurs have been confirmed, the credibility of the software distinguishing Uighurs purely on facial features is questionable.

These news stories give us a good idea about how the FRT can evolve in the future, but at this point in time, facial analysis software is mainly in the research and trial phase. So, this paper will keep the focus on facial recognition. The truth is even facial recognition technology is prone to mistakes. On several occasions, police have arrested the wrong person, because of a mistake by the FRT. In June 2020, Detroit Police Chief said that the software they use misidentifies 96% of the time, so they use it only to narrow down their search sample. In 2018, American Civil Liberties Union tested the facial recognition software of Amazon to compare the images of members of Congress with a database of 25000 mugshots of convicted criminals. Amazon’s “Rekognition” software falsely identified 28 members of congress as criminals. (Amazon’s software is available for public use and cost the ACLU only $12.33).

The FRT is more likely to make a mistake with women and people with darker skin tones than with white men. In the ACLU test, 40% of the false matches were African Americans, even though they comprise only

20% of Congress. In 2018, MIT study of gender and skin-type bias in commercial artificial-intelligence systems showed a 34.7% error rate for dark-skinned women, and only 0.8% for light-skinned men. There are two likely explanations for this bias: darker skins do not reflect light as well as fair skin tones; 2. smaller sample size of minorities' images.

However, this is a changing pattern and every year the FRT is getting better at recognizing people of all skin tones. A big reason for this is that both the quantity and the quality of the facial images are going up. According to the National Institute of Standards and Technology (NIST) under the US Department of Commerce, the best face identification algorithm in 2014 had an error rate of 4.1%, while by 2020 the leading algorithm had an error rate of less than 1%.

2. Commercial use of FRT

The market for FRT emerged only around 2001, but it has been dynamically growing ever since. According to various estimates, it is expected to reach somewhere between 7 and 10 billion USD in 2022. More and more organizations are using FRT to replace ID checks. Schools use it to track attendance and/or keep away unwanted people. It is widely used to group and catalog images and video files. We have already mentioned some other innovative ways how FRT can be used. However, it is important to note that not all uses of the technology have equal social impact and the US Congress needs to take action and set legal boundaries for commercial use of the FRT.

If we go back to the two sub-categories of facial recognition we discussed earlier, the main issue in the commercial use of the FRT is around *facial identification*. In the case of facial verification or one-to-one searches, there is a set limit to the database and everyone involved is usually aware that they are part of a certain facial verification system. Usually, facial features of more people are processed to train the algorithm, but that is less problematic since those images are anonymized. In the case of facial identification or one-to-many searches, there is no set limit to the databank and many people are not aware that their information is on a certain database. So, this raises a question about consent.

Can the companies use the images we share on public platforms online to build their database without asking for permission? On November 2, 2021, Facebook announced that it is shutting down its facial recognition system and deleting "more than a billion people's individual facial recognition templates". That is why we no longer see little squares around faces when we scroll over Facebook photos. The decision came 6 months after Facebook had to pay $650 million for violating the Illinois Biometric Information Privacy Act (BIPA), which bans collecting and storing of the facial geometry of Illinois residents. Facebook made an elaborate argument that it inflicted no harm on its users, but still lost the case, since BIPA clearly states that processing the biometric data of Illinois residents without opt-in consent is illegal.

Most big tech companies in the US have or had their own facial recognition software, but following the controversies over the racial bias issue, they have restricted investments in FRT. Within a week in June 2020, IBM announced that it is getting out of the facial recognition business altogether, while Microsoft and Amazon declared a moratorium on selling their facial recognition technology to law enforcement agencies. However, these tech giants are not the biggest in the facial recognition market. Table 1 lists 10 of the biggest companies in the FRT market.

Company	Country	Founded in	Web info
Ayonix	Japan	2007	https://ayonix.com
Clearview AI	USA	2017	https://www.clearview.ai/
Clear Secure	USA	2010	https://www.clearme.com
Cognitec	Germany	2002	https://www.cognitec.com/
iOmniscient	Australia	2001	https://iomni.ai
Kairos	USA	2012	https://www.kairos.com
Megvii	China	2011	https://en.megvii.com
NVISO	Switzerland	2009	https://www.nviso.ai/en
Oosto*	Israel	2015	https://oosto.com
SenseTime	China	2014	https://www.sensetime.com/en

TABLE 1. Some of the biggest companies in the FRT market.

In January 2020, The New York Times investigation revealed that a New York based company Clearview AI built a database of 3 billion images scraped from the internet and is selling its software to 600 law enforcement agencies. A month later, BuzzFeed did a follow-up investigation and found that Clearview "had provided its facial recognition tool to more than 2,200 police departments, government agencies, and companies across 27 countries." Now the company is facing lawsuits in at least 7 countries, including the United States, Canada, Australia, Germany, United Kingdom, France, Italy and Greece. In November 2021, UK government imposed a $23 million fine on Clearview, for violating their national data privacy law. Twitter, Google, and Facebook have also sent cease-and-desist letters requesting it stops using the public information of their users.

When sued under BIPA, Clearview responded that it will delete data of all the residents from Illinois. Currently, on its website Clearview offers an opt-out form for residents of Illinois and California, which also has legislation similar to BIPA. The United States Congress should pass federal law similar to BIPA or California's Consumer Privacy Act that would introduce clearly defined limits for commercial use of the FRT.

However, considering that on the other side of the debate, this technology adds value to the efforts of the security agencies, the federal legislation should not be overly restrictive. An opt-out consent might be a reasonable solution.

We should, also consider that with every passing day, it is becoming easier to build a search engine for photo matching, like Clearview. Two weeks after the attack on the US Capitol on January 6th, 2021, a website named Faces of the Riot appeared online, which catalogued the faces of 6000 individuals who were present during the incident, extracted from 827 videos posted on social media platform, Parler. The author of the website, who self-identified as a student in the Washington DC area, told the journalists that he intended to help the police investigation and that he used only open-source software. Thus, a heavily restricted legal environment might not achieve the intended purpose, but create a lucrative black market for the FRT. The federal law on commercial use of FRT should define feasible legal boundaries and find the right balance between the right to privacy and public security efforts.

3. Government use of FRT

The number of governments using facial recognition is growing every year. They use it mainly for security and traffic control purposes. However, facial recognition technology and the artificial intelligence behind it are very powerful tools that can be used in many different ways that are not always in the public interest. The federal legislative bodies need to intervene and establish certain standards, impose responsibilities and delineate restrictions for the public use of the FRT.

If facial recognition becomes overly pervasive, then independent of the intent, it could lead to constraints on public freedom. It is important for governments to evaluate the potential impact of facial recognition on civil liberties and establish ethical principles and regulatory guidelines before expanding the use of FRT. A privacy impact assessment by The International Justice and Public Safety Network, which is comprised mainly of seasoned law enforcement officers, mentions that “the mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition.” There are various reports that this is happening in China, where facial recognition is very commonplace. German journalist, Kai Stritmatter, who has studied China for more than 30 years writes about the government use of facial recognition in China: “What the Communist Party is doing with all this high-tech surveillance technology now is they're trying to internalize control. ... Once you believe it's true, it's like you don't even need the policemen at the corner anymore, because you're becoming your own policeman.” In order to provide a better context, I present a brief overview of the government uses FRT in China and the European Union.

China

According to one estimate in 2020, there were around 770 million surveillance cameras installed around the world and roughly 54% of those cameras were in China. Based on the number of cameras per 1000 people 16 out of the top 20 most surveilled cities are in China. Facial recognition technology is omnipresent in most parts of the country and is used by both government and private entities. For example, at KFC China you can pay by smiling into a camera. According to new guidelines passed by China's Supreme People's Court, since August 1, 2021, commercial venues, such as hotels, shopping malls, and airports, need to get consent from customers to use facial recognition. The new rules also impose restrictions on the use of the technology and responsibilities for protecting it. The decision of the Supreme People's Court came about a year after residents in Honk-Kong staged mass protests against the ubiquitous facial recognition and toppled 20 lampposts equipped with cameras. However, there are no restrictions on the government use of the FRC and it continues to be an integral part of the social credit score system. If a Chinese citizen decides to jaywalk on a street equipped with facial identification camera, she will receive a private message with a fine and that will impact negatively on her social credit score.

European Union

Two weeks ago, a coalition in the German parliament, led by the ruling Social Democratic Party said they want to ban "biometric recognition in public spaces as well as automated state scoring systems by AI." In April of 2021, European Commission proposed a new regulation titled Harmonized Rules on Artificial Intelligence, which also suggests a ban on facial recognition, absent certain exceptions for security purposes. According to the proposed regulation, the use of "*real time* remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is prohibited unless certain limited exceptions apply." Exceptions include: strictly necessary for a targeted search of potential victims of a crime, prevention of a specific imminent threat to life, or the detection or identification of a perpetrator. The act has already been criticized and various improvements have been offered, but is a great starting point on this very important issue.

The United States

The United States, the world leader in AI industry, does not have a regulation on the fair use of facial recognition either, but the issue is on the agenda of political debates in Congress. In March 2021, National Security Commission on Artificial Intelligence, a bipartisan working group, released its final report, where it recommends the "Congress to require prior risk assessments "for privacy and civil liberties impacts" of AI systems, including facial recognition." In 2020, "Facial Recognition and Biometric Technology Moratorium Act", was proposed, but did not pass. Such a moratorium would give time to improve the accuracy of the facial recognition technology and conduct an assessment of its potential implications.

Conclusion

One of the biggest concerns in the United States has been the bias of the facial recognition software. As discussed earlier facial recognition systems have been biased against minorities, which has led to several wrong arrests by police. For example, in the summer of 2020 Robert Williams, a resident of Michigan was detained and kept in the police station overnight because a facial recognition algorithm made a flawed match. Usually, these cases get resolved within hours, but it creates a tremendous inconvenience for innocent people and their families. The United States needs a national law that sets out the legal framework for public use of the FRT and addresses all the possible side effects. For example, an effective way to address this issue would be to have third-party testing and approval for the facial software used by police. They would use only the software that is certified by an independent agency. It is also important that police do not use low quality images in their queries.

Facial recognition technology is a powerful new tool that requires a comprehensive approach, which takes into account its impact on the economy, national security, and civic life. It presents incredible opportunities, especially in aiding the work of law enforcement agencies, but finding the right balance between security and civil liberties will be one of the biggest challenges. Federal law is required to regulate both commercial and government use of the FRT and establish quality and credibility standards for the facial recognition software. The law should not force the police to work with analog technologies in a digital age, but they should enforce high ethical standards that will minimize the potentially negative impact on civic life.

References

Bischoff, P. (2021, May 17). *Surveillance camera statistics: which cities have the most CCTV cameras?* Comparitech. https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Crawford, K., Dobbe, R., Dryer, T., & Fried, G. (2019, December). *2019 Report*. AI Now Institute. New York University. https://ainowinstitute.org/AI_Now_2019_Report.pdf

Crumpler, W. (2020, April 14). *How Accurate are Facial Recognition Systems – and Why Does It Matter?* Center for Strategic and International Studies. https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter

Davies, D. (2021, January 5). *Facial Recognition And Beyond: Journalist Ventures Inside China's "Surveillance State."* NPR. https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta

Dou, E. (2021, July 30). *China built the world's largest facial recognition system. Now, it's getting camera-shy*. Washington Post. https://www.washingtonpost.com/world/facial-recognition-china-tech-data/2021/07/30/404c2e96-f049-11eb-81b2-9b7061a582d8_story.html

Facial Recognition. (2021, October). INTERPOL. https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition

Fussell, S. (2019, August 30). *Why Hong Kong Protesters Are Cutting Down Lampposts*. The Atlantic. https://www.theatlantic.com/technology/archive/2019/08/why-hong-kong-protesters-are-cutting-down-lampposts/597145/

Garvie, C., & Moy, L. M. (2019, May 16). *America Under Watch | Face Surveillance in the United States*. America Under Watch - Real-Time Facial Recognition in America. https://www.americaunderwatch.com/asd

Greenberg, A. (2021, January 20). *This Site Published Every Face From Parler's Capitol Riot Videos*. Wired. https://www.wired.com/story/faces-of-the-riot-capitol-insurrection-facial-recognition/

Hardesty, L. (2018, February 12). *Study finds gender and skin-type bias in commercial artificial-intelligence systems*. MIT News | Massachusetts Institute of Technology. https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

HARMONISED RULES ON ARTIFICIAL INTELLIGENCE. (2021, April 21). European Union Law. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206

Heikkilä, M. (2021, November 24). *German coalition backs ban on facial recognition in public places*. POLITICO. https://www.politico.eu/article/german-coalition-backs-ban-on-facial-recognition-in-public-places/

Hill, K. (2020, August 3). *Wrongfully Accused by an Algorithm*. The New York Times. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Hill, K. (2021, November 2). *The Secretive Company That Might End Privacy as We Know It*. The New York Times. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Illinois Opt-Out Request Form. (2021). Clearview AI. Retrieved December 9, 2021, from https://clearviewai.typeform.com/to/HDz8tJ?typeform-source=www.clearview.ai

Julia Horowitz, CNN Business. (2020, July 3). *Tech companies are still selling facial recognition tools to the police*. CNN. https://edition.cnn.com/2020/07/03/tech/facial-recognition-police/index.html

Kaspersky. (2021, August 23). *What is Facial Recognition – Definition and Explanation*. Www.Kaspersky.Com. https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition

Keegan, M. (2020, August 14). *The Most Surveilled Cities in the World*. US News. https://www.usnews.com/news/cities/articles/2020-08-14/the-top-10-most-surveilled-cities-in-the-world

Koebler, J. (2020, June 29). *Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time*. Vice. https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time

Mac, R. (2020, May 8). *Clearview AI Says It Will No Longer Provide Facial Recognition To Private Companies*. BuzzFeed News. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies

MacCarthy, M. (2020, August 20). *Who thought it was a good idea to have facial recognition software?* Brookings. https://www.brookings.edu/research/who-thought-it-was-a-good-idea-to-have-facial-recognition-software/

MacCarthy, M. (2021, May 25). *Mandating fairness and accuracy assessments for law enforcement facial recognition systems*. Brookings. https://www.brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-accuracy-assessments-for-law-enforcement-facial-recognition-systems/

Mozur, P. (2019, May 6). *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*. The New York Times. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Nagaraj, A. (2020, February 14). *Indian police use facial recognition app to reunite families with lost children*. Reuters. https://www.reuters.com/article/us-india-crime-children/indian-police-use-facial-recognition-app-to-reunite-families-with-lost-children-idUSKBN2081CU

Nature Editorial, & Castelvecchi, D. (2020, November 18). *Is facial recognition too biased to be let loose?* Nature. https://www.nature.com/articles/d41586-020-03186-4

Nothing personal? How private companies are using facial recognition tech. (2020, June 8). TechHQ. https://techhq.com/2020/06/nothing-personal-how-private-companies-are-using-facial-recognition-tech/

Pesenti, J. (2021, November 3). *An Update On Our Use of Face Recognition*. Meta. https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/

Porter, T. (2019, March 21). *The debate on automatic facial recognition continues*. Surveillance Camera Commissioner's Office. https://videosurveillance.blog.gov.uk/2019/03/21/the-debate-on-automatic-facial-recognition-continues/

Rollet, C. (2019, November 11). *Hikvision Markets Uyghur Ethnicity Analytics, Now Covers Up*. IPVM. https://ipvm.com/reports/hikvision-uyghur

Snow, J. (2018, August 3). *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*. American Civil Liberties Union. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Symanovich, S. (2021, August 20). *What is facial recognition? How facial recognition works*. Norton. https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

Webster, S. (2021, May 27). *Clearview AI Hit With Dozens of Lawsuit in Europe Over Method of Collecting Data*. Tech Times. https://www.techtimes.com/articles/260747/20210527/clearview-ai-hit-dozens-lawsuit-europe-over-method-collecting-data.htm