NOTE FOR NATIONAL DEFENCE:
Public Policy Framework for AI-Powered Facial Recognition Technologies

Authors: M. R. Nematollahi [1] and K. Khorasani[2]

[1] Graduate Student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- Biometrics measures the person's permanent physical characteristics such as fingerprint and eye characteristics, or even behavioral characteristics, which can verify their identity uniquely.
- Facial recognition is a particular application of the computer vision technology to detect, identify, and classify human images based on the human's face biometrics. AI and Facial Recognition systems are complementary technologies. AI-powered facial recognition software is superior in performance and brings new insights into the technology.
- Currently, cameras are becoming ubiquitous and constitute as an inseparable part of our life. This further implies that the required sensory systems for facial recognition systems are becoming available almost everywhere.
- The required datasets for facial recognition systems are also becoming ubiquitous, through our interactions with either the personal or public monitoring cameras and our activities in various social networks.
- Similar to other applications of AI systems, AI-powered facial recognition systems are also subject to debates and concerns as far as privacy, accountability, liabilities, and security are concerned.
- The social networks provide the easiest way of data collection, with the highest data generation rate, and provide enormous amount of data sets containing comprehensive information about different aspects of people's real life. They are also directly subject to many current debates and concerns on privacy breaches, mainly due to using AI-powered facial recognition technologies over these data sets.

- As far as the social networks are concerned, from the early stages of development of these technologies, many researchers had suggested privacy-aware frameworks for use by policymakers. They had addressed the proper conceptualization of the privacy that would cover most of the current concerns and requirements for the laws, social norms, the market, and the infrastructure to be able to force the governing companies to observe the people's privacy in social networks, while they had also considered the available lag in the response time of policymakers.

- After almost a decade from the early versions of the social networks, now, it is the right time to study the people's concerns and intentions in using the social networks, which would further enable us to evaluate how well different frameworks can respond to these concerns, while not blocking and impeding the form of activities that have been formed and developed around these technologies.

CONTEXT

- Facial recognition technologies utilize the face contours as a type of biometrics to identify persons in images or video frames by matching the biometrics to a database of facial features previously created and stored somewhere.

- Biometrics are highly personal and linked to unique information about each person; hence, they are trendy among law enforcement agencies to identify the criminals, yet, once the infrastructure has been established even for good primary intentions, after that, the technology can be easily misused intentionally or even unintentionally.

- Before being used in the critical decision-making processes, facial recognition technologies should have the required performance and accuracy to ensure the safety of the individuals and society, for example, not to identify the wrong person guilty in sensitive situations.

- In using AI-powered facial recognition systems since one depends on the a-prior dataset and AI algorithms, one should ensure that the dataset and algorithms will not result in further discrimination based on skin color, gender, or other discriminative parameters. It is evident that "while technology cannot solve all societal problems, it should not exacerbate them."

- Collected biometrics, the same as other collected datasets, are prone to be hacked. Biometrics are becoming more commonplace, and peoples tend to use them instead of passwords to protect their properties, and this is when in comparison with passwords, one cannot change biometrics commonly. Such high-profile datasets are desirable targets for hackers. On the other hand, as our biometrics becomes ubiquitous, hackers can more easily access that information. Hence, the security of these technologies should be taken into account before they become widespread.

- Nowadays, cameras as the main sensory system for facial recognition systems are becoming ubiquitous and an inseparable part of our life. As contactless sensors, this can raise further privacy concerns, as people may be monitored constantly even without being noticed.

- On the other hand, in previous decades, social networks became ubiquitous as well. Now, human life becomes highly tied to social networks and due to the strong effects of social networks, people recklessly share images, videos, and other types of information related to every aspect of their lives. These make the social networks ideal datasets for developing, testing, and using AI-powered facial recognition systems.

- Most of the currently popular social networks are managed by private companies, most of which do not care enough about users' privacy. On the other side, users also do not have enough knowledge about how their information is collected and may be used by these companies. Therefore, most of them think that the same social norms have been applied and hence, trust in these networks in sharing their information.

- Besides, this fact that the policymakers in responding to the social concerns are always with a lag behind made the situation even more stringent. Despite all concerns, due to no proper response, as statistics show, the number of social network users continues growing, followed by growth in the amount of the data stored by the servers. This increase in peoples' interaction with social networks also brought new insights into the businesses and peoples' lives, making the networking effect more potent than before.

CONSIDERATIONS

- Undoubtedly, for technology with many different applications, from identifying an individual among a bunch of peoples to face authentication in unlocking a mobile phone, one cannot use the same prescription all the times, or one will ruin all the potential advantages along with those potentially harmful purposes to avoid the risks. Therefore, a more use-case familiar scenario is preferable.

- Policies and laws should cover the two main parts of the AI-powered facial recognitions systems i.e., the enrolment phase consists of all data collections and data storage, and matching phase which is related to AI algorithms.

- Especially, the three most important areas of human rights, in which the impact of AI-powered facial recognition technologies should be considered are privacy, equity and due processes.

- Regarding privacy, one should ensure the active consent of peoples for their biometrics being collected and stored for future usages, avenues for objection regarding storing and using the data even after primary consent for doing so, and proper standard for accessibility of the data by third parties.

- Regarding the equity, one should ensure possible bias enrollment in datasets, bias exposures, and the quality standards in the datasets and the required performance.

- Regarding the due processes, one need to inform people about using their data by law enforcement agencies, the possibility of using their data as evidence, or for identification and being used for public consultations.

- One may also need to revisit the conceptualization of social concerns such as privacy, to properly cover type of applications and intervention of facial recognition technologies.

- Regarding privacy, instead of traditional conceptualizations like, “the right of being left alone”, conceptualizations based on intervention in the information flow are more preferable, especially when dealing with social networks.

- Nowadays, Social networks provide the easiest way of data collection, with the highest data generation rate, and provide enormous data set containing comprehensive information about different aspects of peoples' real life.

- From the early stages of development, social networks were a desirable place for designing, testing, and applying the AI-powered facial recognition systems, thanks to ignorance and fewer concerns about users’ privacy and human rights by the companies managing these systems.

- Now with hindsight, in regulating the social networks concerning about privacy and other human rights, in proposing a policy framework, one should take into account the increasing dependency of people’s life to social networks, new forms of interactions, the current infrastructure, and being friendly about the rise of new technologies.

- Four main constraints that can be used for regulation of technologies are law, social norms, market, and infrastructure or architecture.

- One can use law to mandates certain behavior and imposes sanctions on deviate actions, the market to inflict a cost on certain actions and incentivizing the market participants to modify their behavior, while one needs to provide the infrastructure that makes the alternatives desired architectures possible. At the same time, by culture building and raising people awareness about the context one can use the social norm, as a force to companies for changing their behavior in long term.

- When using this force wares, policymakers and lawmakers should take into account the current states of the social networks, the new form of people’s interactions and intentions in using them, the new business models and business insights formed around them, compatibility and transformability of the current infrastructure, international concerns, society trust, and the last but not the least providing enough venues for rising new technologies.

References

- https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology

- Ruhrmann, Henriette. "FACING//THE FUTURE." (2019).

- Welinder, Yana. "A face tells more than a thousand posts: developing face recognition privacy in social networks." Harv. JL & Tech. 26 (2012): 165.

- https://www.statista.com/topics/1164/social-networks/

- https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/