Security-Policy NET Nexus of Emerging Technologies

BRIEFING NOTES

#BN-47-Cyber and space as key enablers-Feb2021

FACIAL RECOGNITION SYSTEMS, SOCIAL NETWORKS AND PRIVACY

Authors: Mohammadreza Nematollahi[1] and Kash 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 measure 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 computer vision to detect, identify, and classify human images based on the human face biometrics. AI and Facial Recognition are complementary technologies. AI-powered facial recognition software is superior in performance and brings new insights into this domain of technology.
- Nowadays, cameras are becoming ubiquitous and are an inseparable part of our life. This further implies that the required sensory components for facial recognition systems are becoming available almost everywhere. The required datasets for facial recognition are also becoming ubiquitous, through our interactions with either personal or public monitoring cameras and our activities in social networks.
- Like other applications of AI, AI-powered facial recognition systems are also subject to debates regarding privacy, accountability, liabilities, and security.
- The social networks provide the easiest way of data collection, with the highest data generation rate, and provide enormous data sets containing comprehensive information about different aspects of peoples' real life.
- They are directly subject to many current debates of privacy breaches, mainly due to using AI-powered facial recognition technologies over these data sets.
- Concerning social networks, from the early stages of development of these technologies, many researchers have suggested privacy-aware frameworks to be used by policymakers. They addressed the proper conceptualization of the privacy that covers most of todays concerns and requirements for laws, social norms, the market, and the infrastructure to be able to force the governing companies to observe the peoples' privacy in social networks, while also considering the available lag in the response of policymakers.
- After almost a decade from the early versions of social networks, now, it is the right time to study the peoples' concerns and intentions in using social networks, which further enable us to evaluate how well different frameworks can respond to their concerns, while not damaging the form of activities that have been formed 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.
- Biometrics are highly personal and linked to unique information about each person; hence, they are trendy among law enforcement agencies to identify criminals, yet, once the infrastructure has been established even for justifiable primary intentions and reasons, after that, the technology can be easily misused intentionally or even unintentionally.

- Before being used in critical decision-making processes, facial recognition technologies should have the required performance and accuracy to ensure safety of individuals and society, as for example not identifying a wrong person guilty under sensitive situations.
- In using AI-powered facial recognition systems given that one depends on the a priori 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 people tend to use them instead of passwords to protect their properties, and this is the case that when in comparison with passwords, one cannot change one’s biometrics. Such high-profile datasets are desirable targets for malicious hackers. On the other hand, as our biometrics become ubiquitous, hackers can more easily access that information. Hence, security guarantees of these technologies should be taken into account before they become widespread.
- Recently, cameras represent as the main sensory system for facial recognition systems and 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 notified.
- On the other hand, in the past two decades, social networks have become ubiquitous as well. Human life has become highly tied to social networks and due to the strong effects of social networks, people recklessly share images, videos, and other types of information as 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 sufficiently focus on users’ privacy. On the other hand, users also do not have sufficient knowledge on how their information is being collected and may be used by these companies. Therefore, most people think that the same social norms have been applied and hence, trust in these networks in sharing their information.
- Besides, the fact that policymakers in responding to social concerns are generally with a lag behind has made the situation even more critical. Despite all many serious concerns, due to no proper responses and as statistics have shown, the number of social network users continues to grow, followed by growth in amount of data that is stored by servers. This increase in people interaction with social networks also has brought new insights into the businesses and people’s lives, making networking effects more potent than before.

CONSIDERATIONS

- Clearly, for a technology with many different applications, from identifying an individual among a group of people to face authentication in unlocking a mobile phone, one cannot use the same criterion all the times, or the potential advantages will be compromised 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 aspects of the AI-powered facial recognitions systems, i.e., the enrollment phase that consists of data collections and data storage, and the matching phase which is related to AI algorithms.
- 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 process.
- Regarding privacy, one should ensure that active consent of people for their biometrics are properly collected and stored for future usage, avenues for objection regarding storing and using data even after primary consent for doing so are available, and proper standards for accessibility of data by third parties are established.
- Regarding equity, one should ensure possible bias enrollment in datasets, bias exposures, and quality standards in datasets and required performance.
- Regarding due process, one needs 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 conceptualization of social concerns such as privacy, to properly cover types of application and intervention of facial recognition technologies.
- Regarding privacy, instead of traditional conceptualizations such as, “the right of being left alone”, conceptualizations based on intervention in information flow are more preferable, especially when dealing with social networks.
- Social networks provide the easiest way for data collection, having the highest data generation rates, and providing enormous data set containing comprehensive information about different aspects of people’s real life.
- From early stages of development, social networks were a desirable place for designing, testing, and applying AI-powered facial recognition systems, thanks to ignorance and fewer concerns about users’ privacy and human rights by companies managing and developing these systems.
- Now with hindsight, in regulating social networks as far as privacy and other human rights are concerned and in proposing a policy framework, one should take into account the increasing dependency of individuals’ 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.
- One can use law to mandates certain behavior and imposes sanctions on deviate actions, the market can 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 alternative desired outcomes possible. At the same time, through cultural building and raising people’s awareness about the context one can use social norms as an instrument of force companies change their behavior in the long term.

- When using the above considerations, policymakers and lawmakers should take into account the current state of social networks, the new forms for people 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, social trust, and the last but not the least providing sufficient venues for supporting the new technologies.

REFERENCES

1. https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology
2. Ruhrmann, Henriette. "FACING//THE FUTURE." (2019).
3. Welinder, Yana. "A face tells more than a thousand posts: developing face recognition privacy in social networks." Harv. JL & Tech. 26 (2012): 165.
4. https://www.statista.com/topics/1164/social-networks/
5. https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/