Security-Policy NET Nexus of Emerging Technologies

BRIEFING NOTES

#BN-45- Cyber and space as key enablers-Feb2021

FAIRNESS AND PRIVACY DILEMMA IN PERSONALIZED AI SENSORY SYSTEMS

Authors: Reza Bahrevar[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

MINDS
MOBILISATION DES IDÉES NOUVELLES EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

Security-Policy
NET Nexus of Emerging Technologies

SUMMARY

- Personalized AI sensory systems, such as face recognition or voice recognition systems, when merged with IoT, can be used to form a powerful computational device, and with the emergence of technologies such as 5G, networks can receive a boost that will ensure and facilitate improved performance of these systems.
- Individuals with special disabilities and limitations can easily use these devices in order to ensure that they improve their livelihood through recognizing voices or faces, given that they could be belonging to their relatives, friends, or employers.

  However, the same technologies and tools also introduce and expose individuals with societal privacy and fairness concerns that need to be carefully investigated and addressed. Appropriate policy protocols and measures have to be introduced to carefully address the associated issues and challenges.

CONTEXT

- AI sensory systems are a type of AI that utilize an image, sound, or other sensors to collect information from an environment and based on the data to render a decision output.
- With recent developments in IoT networks through advent of smart technologies such as edge cloud, 5G, and combination of 5G and edge cloud, there could be an added efficiency in AI sensory systems since they can process larger quantity of data in the same or even less amount of time.
- Recently countries, such as France among others, are using face recognition systems to control masks wearing in view of rise of COVID-19 pandemic. However, it is being claimed that private information are not stored.
- Face recognition or voice recognition systems, with the support of machine learning technologies, can be trained to learn on objects, humans, and the real-world. They can also be utilized to assist people with disabilities.
- Therefore, important questions related to individual and societal responsibilities [1] have been raised. For example, a user, while benefiting from a face recognition system, might be wary of inadvertently sharing personalized sensitive information [1] with unauthorized users.
- On the other hand, it is not fair for individuals with disabilities, such as being deaf or blind, to be denied of the benefits of these systems, such as knocking on doors and recognizing familiar faces [1,2].
- How can individual privacy considerations of those in close contact with these technologies and smart systems be preserved?

CONSIDERATIONS

- If AI sensory systems are employed for personal use how advanced these AI systems should be?
- How to avoid and prevent bias especially towards already marginalized groups [3,4].
- Even a person with a disability can have surveillance and malicious motivation when using AI sensory systems [3].
- In the facial recognition systems case is it desirable to have functionalities to recognize every voice of a celebrity, online friends, or strangers [1]?
- What information should be following as a result of the decision-making processes?
- For example, the concept of a smartwatch for the visually impaired person is discussed in [2], where these individuals can attend a meeting that requires audience silence, and at the same time, they would be able to recognize the speaker and the people present in that meeting without any disruption.
- There are already existing all-party consent laws in place, which could limit the development of such devices.

NEXT STEPS

- One should monitor companies that manufacture the AI sensory systems and devices. Adding security certification based on their provided level of transparency is the first thing that one should implement when dealing with such systems. In this way, one can offer a level of trust to the users.
- Unauthorized access of the AI sensory systems and devices to the cloud databases may need to be prevented.
- One should encourage built-in AI sensory systems for personal use, where access to the internet and global search engines are limited.
- If the AI sensory systems and devices utilize the internet and high-speed technologies such as 5G, then one would recommend that users should be identifiable. For example, a visually impaired person that uses the cloud database should have an identifiable code.
- One should identify and certify what type of information these technologies will store in their databases. Information such as name, age, height, and credit card.
- The AI sensory systems and devices will constantly upload information as they are trying to be assistive to their users. There should be a built-in mechanism that prevents uploading sensitive information such as credit card details since the excess info may become accessible to every collaborating third party companies within the cloud.
- To ensure fairness in data training, one should be able to determine who decides on the inputs and how are they chosen, and what labels would the data will be assigned to [1].
- One should also consider a possibility that a potential user might be an adversary [1] and therefore invest in cyber-security measures that deal with and mitigate adversaries that impersonate as a user.

REFERENCES

[1] Findlater, L., Goodman, S., Zhao, Y., Azenkot, S. and Hanley, M., 2020. Fairness issues in AI systems that augment sensory abilities. *ACM SIGACCESS Accessibility and Computing*, (125), pp.1-1.

[2] Neto, L.D.S.B., Maike, V.R.M.L., Koch, F.L., Baranauskas, M.C.C., de Rezende Rocha, A. and Goldenstein, S.K., 2015, April. A Wearable Face Recognition System Built into a Smartwatch and the Visually Impaired User. In *ICEIS (3)* (pp. 5-12).

[3] Guo, A., Kamar, E., Vaughan, J.W., Wallach, H. and Morris, M.R., 2019. Toward Fairness in AI for People with Disabilities: A Research Roadmap. *arXiv preprint arXiv:1907.02227*.

[4] Keyes, O., 2018. The misgendering machines: Trans/HCI implications of automatic gender recognition. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), pp.1-22.