Ethical Concerns for the Future of Face Recognition Technology and Policy

Kolina Koltai (UT Austin), Claudia Flores-Saviaga (West Virginia University), Megan Rim (University of Michigan)

Regulation of face recognition technology (FRT) has not kept pace with increasingly widespread adoption of face recognition technologies. This has resulted in the unregulated use of FRT by law enforcement in places such as Detroit, Michigan, and Baltimore, Maryland. While several bills have been introduced, there currently exists no comprehensive protections at the federal level against the use of face recognition on citizens. Although, San Francisco, California, Somerville, Massachusetts, and Oakland, California have instituted bans on FRT, some cities have opted instead to pass regulatory policies face recognition to the effect of imposing some restrictions but ultimately legitimizing its use as a policing technology. As some cities have begun implementing real-time face recognition technologies, this has stirred debate about how its use by law enforcement might violate the First Amendment's protections of the right to freedom of assembly, and Fourth Amendment's protections against the unlawful search of private spaces (Hamann and Smith, 2019).

As it stands, we do not anticipate FRT to leave the public space in the near future. We anticipate that more governments and agencies would want to incorporate FRT into monitoring, policing, and military efforts. FRT will be built into the infrastructure of society, physically with cameras, institutionally with policy, and culturally as an accepted norm. We also anticipate there being a lack of separation between FRT data and personal data from other companies and organizations. You can imagine Social Media Platform data and FRT data combining to give a 'catered' experience when you go to different physical locations. While it may seem 'Minority Report'-esqe, we may not be far from a future that has highly integrated FRT into society from shopping and catered ad preferences and consistent monitoring.

FRT biometrically identifies you by matching your unique facial dimensions against huge databases. However, a recent study uncovered large gender and racial bias in commercial Facial recognition software. In the researchers' experiments, the accuracy in determining the gender of light-skinned men were never worse than 0.8 percent. For darker-skinned women, however, the error rates ballooned to 35 percent (Buolamwini, 2018). Afterall, FRT is only as smart as the data used to train it. If the system is trained using faces of many more white men than people of color, then it will be worse at identifying these minorities. This is worrisome as across the U.S, state and local police departments are building their own face recognition systems. But, we know very little about them. i.e. we don't know how they address accuracy problems. As a consequence, we don't know how any of these systems affect racial and ethnic minorities.

Recent research has proposed ways to reduce bias in identifying people in different demographic groups (Amini, 2019), but without regulation, that won't curb the technology's potential for abuse. Ultimately, as accuracy is improved and bias is mitigated, it is expected that law enforcement will want to use FRT for immediate identification. For example, it might soon be possible to scan the faces of people passing by the street using CCTV cameras and determine not just who someone is, but where they've been, where they're going, and whether they have an outstanding warrant, immigration detainer, or unpaid traffic ticket (Kofman, 2017). If FT systems that government and law enforcement agencies use is biased and with low accuracy, there is risk that the face recognition search will lead to an investigation, if not an arrest, of the wrong person (Garvie, 2019).

The main problem is that existing privacy and civil rights laws were mainly designed to limit old-fashioned forms of privacy violation, such as illegal searches or unauthorized revelation of private activities, such as medical records. Currently, there is evidence about how face recognition is being used in police surveillance of protests (Garvie, 2016). This could have an impact on the public and political discourse. For example, past research has found that surveillance practices may create a chilling effect on democratic discourse by stifling the expression of minority political views (Stoycheff, 2016). If the of face recognition technology in public spaces continues to expand, minorities might not choose to participate in activities such as protests, if they know their face could be scanned. In the absence of regulation, the use of face recognition for law enforcement, could lead to serious risks of misidentification. In the absence of transparency, these uses threaten to violate the due process rights of those arrested (Garvie, 2019).

References

Amini, A., Soleimany, A., Schwarting, W., Bhatia, S., & Rus, D. (2019). Uncovering and Mitigating Algorithmic Bias through Learned Latent Structure.

Buolamwini, J., & Gebru, T. (2018, January). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency* (pp. 77-91).

Garvie, C. (March, 2019). Garbage In, Garbage Out: Face Recognition on Flawed Data |Center on Privacy and Technology, Georgetown. https://www.flawedfacedata.com/. (Accessed on 09/22/2019).

Garvie, C. 2016. Bedoya A. Frankle J. (October, 2016). Perpetual Line Up - Unregulated Police Face Recognition in America | |Center on Privacy and Technology, Georgetown. https://www.perpetuallineup.org/.(Accessed on 09/22/2019).

Introna, L., & Nissenbaum, H. (2010). Facial recognition technology a survey of policy and implementation issues.

Kofman, A. (2017, March) Privacy Fears Over Cops Using Real-Time Face Recognition | The Intercept. http://bit.ly/2m7aOku. (Accessed on 09/22/2019)

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring. *Journalism & Mass Communication Quarterly*, *93*(2), 296-311.