Ikhlas Attarwala / LGAI
11-08-2019 / Final Paper

1045 words

Facial Recognition: Identifying a Worried Expression

The United States and Sub-Saharan South Africa have nearly the exact same rates of violent gun deaths per 100,000 people (4.43 vs 4.56)[1]. Opioids account for 66% of all drug overdose deaths in the US[2]. Until recently, sufficient scrutiny never fell over the risk of e-cigarettes due to a lack of clinical research[3]. Each of these epidemics share one thing in common: the absence of swift regulation that, if acted upon earlier, would have reduced their extent of harm. In the case of opioids, pharmaceutical companies wrongly reassured the medical community that there would be no addiction to opioid pain relievers in the 1990s; regulation to halt production until research of the medication became available could have saved some of the 1.7 million people suffering from it per year in the US today. This similar attitude, this lack of caution, now applies to ignoring proper regulation for facial recognition technology. Facial recognition was a gift that emerged from the field of biometrics and artificial intelligence with the capability of identifying and authenticating people from digital images and videos. Regrettably, the impulsive rush to use such an advanced tool without proper data privacy laws in place has already twisted this gift into a menace for some, and is leading us to a more unpromising future. Fortunately, there are ways to correct and foster both innovation and public safety before it's too late.

Facial recognition has been deployed in all manner of services ranging from mobile applications, incl. Snapchat and Facebook, to national security, such as the arrest of wanted criminals and terrorists. Prior to its inception, we had less enhanced security for finding missing children or criminal activists, fewer ways to integrate identity with profiles for commercial use, and even the world of affective computing would be much smaller today (the study of human affect and emotion). Of course, accuracy and algorithmic bias have been recent concerns that needed immediate attention[4], but larger threats such as misidentification, misuse of individual privacy, and the breaching of databases have started to loom overhead. One such example to illustrate the concern for unregulated identification can be seen with FindFace, a mobile application developed in Russia, that was being used to identify and harass women who appeared in pornographic films[5]. People deserve enough freedom to not fear being identified and surveilled without their knowledge, and at the bare minimum, enough freedom to keep their anonymity.

Unlike other biometric systems, facial recognition does not require cooperation of the subject to work. Government and corporate entities have begun installing these in airports, malls, and other public areas where crowds of people exist. You've probably walked past a few every week without realizing; in fact, you may not have noticed the potential concern of your laptop's front-facing camera until now either (even Mark Zuckerberg covers his with tape[6]). This may not seem very concerning, but the misuse potential is quite dangerous. China recently purchased large surveillance and security systems to monitor its people, with most of its attention falling on the northwest Xinjiang region where police use facial recognition eyewear to pick people out of crowds[7]. The Xinjiang region is home to the Uyghur Muslims, a minority group that China has begun placing in internment camps (~1.5 million inmates in capacity). Authorities identifying minority groups is a grave concern, not only for the Uyghur people, but also for anyone who is misidentified by the algorithm. Despite receiving widespread criticism, China is further pushing to

Please note: This paper was granted an
extension until Friday, Nov 8th, 2019, 11:59pm.

have all of this region under total surveillance[8]. India is also setting up a large, centralized facial recognition system[9], but while I agree they are terribly understaffed with police forces, India has a more impulsive and authoritarian nature to address issues, such as shutting down the internet for a week in Kashmir for "peace and tranquility"[10]. The worst part about this is that India has little to no effective data privacy laws for facial recognition.

A large debate over data privacy is how it balances with the need for information, and everyone gets it differently. India is too slow at passing personal data protection laws. China lacks the interest in enforcement. Others that have made strides ended up going too far, such as the EU overregulating with the GDPR and crippling their competitiveness[11,12]. We need to learn from these examples to determine what to balance correctly. My suggestions for the core components of privacy laws are as follows: *They should require a flexible level of transparency.* Some form of rudimentary explanation is necessary to account for what a system's intentions are. It may help to create agencies that are designed to privately test for algorithmic bias and fairness. *There should be a provided right to the data collected.* Data collected on a larger scale should require approval. *All individuals should have the right to opt out whenever they choose.* If information is collected and tagged, you should have the right to remove it. It may be possible to develop an electronic tag that signals a facial recognition system to skip identifying you, acting as an "invisibility cloak". *Any individual governed by an algorithm should have the right to request judgment by a non-automated process.* While explanations for black boxes may not be practical, the alternative, to request a different form of judgment, is. There are numerous other necessities, but there should be an equal amount of attention on what shouldn't be included, such as the GDPR's blanket restriction on "automated decision-making", the little difference it makes between what larger and smaller businesses have to abide by, and its endless consent requirements.

Newer AI applications are developed and deployed constantly, as should the revisioning of data protection laws that govern them. Facial recognition is an invaluable technological marvel, and it should be treated as such. The implications for it and our freedom can be chilling, but there's still time to safely protect our liberty and pace of competitive growth. Repressive rule and overregulation don't have any fine line between them, they're fairly opposite; at the heart of it all, the focus of regulating facial recognition systems should be on its actual uses and impact, rather than its collection and analysis.

Citations:

[1] Aizenman, Nurith, and Marc Silver. "How The U.S. Compares With Other Countries In Deaths From Gun Violence." *NPR*, NPR, 5 Aug. 2019, www.npr.org/sections/goatsandsoda/2019/08/05/743579605/how-the-u-s-compares-to-other-countries-in-deaths-from-gun-violence

[2] National Institute on Drug Abuse. "Overdose Death Rates." *NIDA*, 29 Jan. 2019, www.drugabuse.gov/related-topics/trends-statistics/overdose-death-rates.

[3] "Public Health Law Center." *E*, 24 Apr. 2019, www.publichealthlawcenter.org/topics/commercial-tobacco-control/e-cigarettes.

[4] Editor, Ryan Daws. "Joy Buolamwini: Fighting Algorithmic Bias Needs to Be 'a Priority'." *AI News*, 24 Jan. 2019, artificialintelligence-news.com/2019/01/24/joy-buolamwini-algorithmic-bias-priority/.

[5] Mills, Laura. "Facial Recognition Software Advances Trigger Worries." *The Wall Street Journal*, Dow Jones & Company, 10 Oct. 2016, www.wsj.com/articles/facial-recognition-software-advances-trigger-worries-1476138569.

[6] Olson, Chris. "3 Things about This Photo of Zuck:" *Twitter*, Twitter, 21 June 2016, twitter.com/topherolson/status/745294977064828929.

[7] Simonite, Tom. "Behind the Rise of China's Facial-Recognition Giants." *Wired*, Conde Nast, 4 Sept. 2019, www.wired.com/story/behind-rise-chinas-facial-recognition-giants/.

[8] Hamdi, Pierre. "Videos Show How China Has Installed Facial Recognition Scanners in Uighur Mosques." *The France 24 Observers*, France 24, 13 Sept. 2019, observers.france24.com/en/20190913-videos-show-how-china-has-installed-facial-recognition-scanners-uighur-mosques.

[9] Chaudhary, Archana. "India Is Planning a Huge China-Style Facial Recognition Program." *Bloomberg.com*, Bloomberg, 19 Sept. 2019, www.bloomberg.com/news/articles/2019-09-19/india-seeks-to-adopt-china-style-facial-recognition-in-policing.

[10] Goel, Vindu, et al. "India Shut Down Kashmir's Internet Access. Now, 'We Cannot Do Anything.'." *The New York Times*, The New York Times, 14 Aug. 2019, www.nytimes.com/2019/08/14/technology/india-kashmir-internet.html.

[11] Coos, Posted byAndrada. "GDPR: The Pros and The Cons." *Endpoint Protector Blog*, 14 Dec. 2018, www.endpointprotector.com/blog/gdpr-the-pros-and-the-cons/.

[12] "General Data Protection Regulation - GDPR." *General Data Protection Regulation (GDPR)*, 25 Mar. 2018, gdpr-info.eu/.