Effective Arguments Assignment

Effective Arguments Assignment

Nathan Ketterlinus

March 3, 2024)

Towson University, COSC418-102, Steven Evans

Abstract

This paper attempts to develop three effective arguments that make facial recognition acceptable in society. All these arguments assume that all data collected is handled ethically, and is not used maliciously by any party, whether it be an individual, corporation, or government. The three arguments made are that well-implemented facial recognition promotes convenience for the average person, security for more sensitive systems, and national and international safety. In particular, we consider the convenience Apple’s Face ID technology provides, the security 2FA utilizing facial recognition as a modality provides, and the assistance facial recognition scans can provide to police at key places around the world, such as banks and international airports, in catching known, wanted criminals.

Effective Arguments Assignment

In the 21st century, very few technologies are as polarizing as facial recognition software. What may appear to be nothing but a fancy way to unlock an iPhone to some can be seen as an invasion of privacy to others. Assuming all involved parties treat data collected by facial recognition software ethically and responsibly (that is, with the intent to collect and store only data which is absolutely necessary, and to secure any stored PII from prying eyes as much as possible), facial recognition software has use cases that poise it to be commonplace across the world. Among these are convenience, personal security, and public security.

Convenience

Facial recognition software’s biggest strength to the average person is the amount of convenience and time save it can introduce. As mentioned in the introduction, Apple’s Face ID software uses facial recognition to allow users to not only unlock their devices, but also securely make purchases and sign into downloaded apps, all with a “1 in 1,000,000” probability of a false positive (Mcclellan, 2020). This reduces the number of passwords the average person needs to memorize and saves time that would have otherwise been spent typing in passwords or log-in patterns or the like. In addition, there is a significant population who writes down their passwords, which is a security vulnerability if a malicious actor were to find the password written down somewhere. Facial recognition alleviates this issue for this population by preventing the need for many passwords in the first place.

However, facial recognition in this context does introduce the possibility of an attacker holding a picture of a valid user (or an unconscious user) up to a sensor and gaining unauthorized access to a system. Going back to Apple’s Face ID, these problems have already been solved and implemented. Apple’s sensor uses an IR scanner to make a 3D map that faces must match, which 2D photos cannot (Apple, 2024). In addition, Face ID requires the user to provide eye contact with the sensor, which is very difficult to spoof with someone who’s asleep or otherwise unconscious. Finally, Apple requires the use of passcodes instead of/ in addition to Face ID in certain scenarios, which we will see why it’s such a good idea in the next section. In these respects, apple sets the gold standard for consumer-grade, privacy-considerate facial recognition, and shows that facial recognition has useful applications to the general public.

Personal Security

After looking at the convenience facial recognition can provide, it may seem counterintuitive that it could also enhance personal security. At first glance, it appears that facial recognition shifts the burden of security from a password’s integrity to a sensor’s integrity. However, facial recognition can provide enhanced security across all platforms with two-factor authentication (2FA). 2FA is the use of multiple user validation modalities to confirm someone is truly who they say they are. Current implementations of 2FA may use both a password and a temporary code sent to a registered phone number or email. 2FA by its nature is much more secure than a singular password or face scan alone, as malicious actors need access to both inputs simultaneously, which is exponentially harder to achieve.

2FA using facial recognition software can be implemented everywhere: from banks to self-checkout grocery stores to mobile apps to secure job sites. The main strength of using facial recognition over some other modality is again the speed and convenience it provides. While 2FA through text or email requires a user to wait for their code to be sent to them, navigate to the message containing the code, then copy it into the input prompt, a facial scan takes a fraction of the time and many less unique actions: just show your face to the sensor. As a quick addendum, 2FA is inherently slower (and more inconvenient) than single factor authentication, but many sources are beginning to implement it because the added security it provides far outweighs the slight inconvenience it poses.

Public Security

After looking at facial recognition software’s applications in adding convenience and security to the average citizen, we now look at how facial recognition can be used to improve the safety of all people by detecting wanted criminals. Imagine an international database where known, wanted criminals have their faces stored, much like how we store their fingerprints today. Using facial recognition technology at key places, like airports or banks, police now have a much easier time catching these criminals and dealing with them appropriately. While the implementation of such a system would undoubtedly be quite complex, places like the Helsinki Airport have been testing facial recognition assisted security and customs since 2017 (Duman, 2019). In addition, this technology is already in use at major airports around the United States, including “Baltimore, D.C., Atlanta, Boston, Dallas, Denver, Detroit, Las Vegas, Los Angeles, Miami, Orlando, Phoenix, Salt Lake City, San Jose, and Gulfport-Biloxi and Jackson” (Santana, 2023). These systems, while designed primarily to speed up the check-in process, can be easily modified to improve national security.

Again, the benefits of such a system hinge upon the ethical use of any data collected, following the principles of informed consent from anyone subject to a face scan. People have the right to know what data needs to be collected from them, and how it will be stored and used in the future. It is of utmost importance that the government’s data collection policy is transparent and readily available to all citizens subject to it. In the case of facial recognition to aid law enforcement, the only stored faces should be those of wanted criminals, and this dataset should always be publicly available for full transparency.

Conclusion

This paper has looked at the emerging technology of facial recognition. It asserts that facial recognition has many wide-scale use cases in the world, ranging from Face ID on iPhones, to 2FA on any login platform, to a streamlined process getting through security and customs at major airports. The main benefits facial recognition provides are increased convenience, personal security, and public security. While all of these positives poise facial recognition to become widely used, it is critically important that data collected is minimal and transparent to ensure ethical use of such technology.

References

Apple. (2024, January 10). *About face ID advanced technology*. Apple Support. https://support.apple.com/en-us/102381

Duman, T. (2019). Innovation in a zero-risk environment: Facial recognition experiment at Helsinki Airport. *Journal of Airport Management*, *13*(3), 215–224.

Mcclellan, E. (2020). Facial Recognition Technology: Balancing the Benefits and Concerns. *Journal of Business & Technology Law*, *15*(2), 363–380.

Santana, R. (2023, May 15). *TSA is testing facial recognition technology at more airports, raising privacy concerns*. PBS. <https://www.pbs.org/newshour/politics/tsa-is-testing-facial-recognition-technology-at-more-airports-raising-privacy-concerns>