Oftentimes, ethical issues in science are born when technology advances beyond the civil discourse that might restrain it. Arguably the most controversial issue in computer science is facial recognition. While facial recognition systems have been developed since the 1960s, there are few laws - at least in the United States - that seek to curtail the use of these systems by corporate entities, police, and government agencies. Privacy, racial bias, and use by law enforcement are the main, unresolved ethical issues surrounding facial recognition systems.

Facial recognition systems work by identifying facial features and matching those results to ones stored in a database. Newer systems can account for the three-dimensional shape and skin texture of a person's face. Advances in hi-resolution cameras (mobile and otherwise), machine learning, and large and (often overly) available databases of faces have proliferated the use of facial recognition systems in the past ten years.

Some uses of facial recognition have proved convenient and entertaining. With the iPhone X, Apple introduced facial recognition as a way for users to unlock their phones privately (facial recognition data is transmitted from the phone) while social media companies like SnapChat allow users to add fun filters to video and pictures by manipulating their appearance. Additionally, facial recognition is sometimes used with consent in addition to other biometric security checkpoints, although it has proved far less effective in correctly identifying a person than other means. The use of facial recognition to scan the faces of non-consenting individuals is where the deeper ethical issues lie.

Facial Recognition is used by government agencies around the world to track their citizenry in sometimes helpful but, more often, frightening ways. Facial recognition has been used to solve violent crimes and identify known terrorists, but those tools of surveillance could easily be used against regular citizens. The same systems that allow travelers to move through security checkpoints without showing traditional identification could be, and sometimes are, used to surveil citizens without their knowledge or consent. In countries like China and Russia, where rights to privacy are weaker than in the US and the EU, systems have been created to track the movements of citizens using facial recognition. In the US, where only some states prohibit the use of facial recognition, local police have maliciously used facial recognition services provided by companies like Clearview. Following the protests of Freddie Gray's murder, Baltimore PD used facial recognition software and social media profiles to identify, locate, and harass protesters. An undisclosed number of local and federal law enforcement agencies use facial recognition to pursue investigative leads. Clearview, a private and international company, mostly works in secret without the oversight of citizens.

Compounding this problem is the fact that facial recognition is less accurate when identifying people of color, especially women. In an MIT study, massive error rates were found when comparing the results of black women (36%) and white men (1.6%). With no federal guidelines pertaining to bias in facial recognition, companies are not accountable for eliminating these inherent prejudices. Coupled with the fact that facial recognition is more likely to be implemented for law enforcement purposes in cities because of population density, people of color would have to deal with an overused system that underperforms in its function, exasperating the issue of over-policing in their communities.

With promises of providing security and significantly reducing crime, facial recognition systems have proliferated in the last ten years with inadequate debate about how, or even if, it should be implemented by marketers, lawmen, or government agencies.