Ethics of Surveillance Technology in Immigration

Rank the stakeholders from least important to most important, with 1 being the most important and 5 being the least.

There are multiple stakeholders involved in this case. Marginalized communities are the most heavily affected and hurt by the use of surveillance technology, especially in immigration enforcement applications. With that being said, immigrants and non-US citizens, U.S. citizens, government agencies, politicians, tech companies, and human advocacy groups all play a role in this. Let's dive deeper into what each of these roles look like more specifically. Below are different stakeholders. While there may not be no "correct" answer, it is important to think about how others are impacted by this topic.

U.S. Citizens

While the general public are all affected, the impact looks different for immigrants and non-US citizens than for U.S. citizens. U.S. citizens often do not feel the same worries that immigrants and non-US citizens do because they don't face the same challenges. U.S. citizens, however, can still play a role in helping immigrants and non-U.S. citizens. Because of the privilege they have of stable citizenship, it is important that they stand up when an immigrant's rights are violated or being taken away.

Immigrants and non-US citizens

For immigrants and non-US citizens, their stake in this is larger than other stakeholders. Why? Because their lives depend so much on whether or not they are targeted by immigration agencies. When targeted by either immigration enforcement or by surveillance technology, immigrants and non-US citizens can have their whole lives uprooted and dismantled. Even if an immigrant has gone through the legal process of immigrating, are they truly safe? The answer should be yes, but Muniz touches on the idea that because surveillance technology does not have physical borders. Migrants must now face checkpoints in their daily lives, which is used to keep migrants reminded of the social construct set up to make them "outsiders".

Politicians

Politicians are involved in the decision making process and focus on the creation of immigration laws. An example of this can be seen in the effort made to pass the American Data Privacy and Protection Act. The Act was introduced in hopes of protecting consumer data privacy and furthering security, to ultimately limit data collection (Pallone). However, the Act was not passed (Pallone).

Government Agencies

Government agencies are large stakeholders, as well. Prominently because of the role they play in immigration enforcement and the implementation of surveillance technology. Agencies such as the Immigration and Customs Enforcement, the Federal Bureau of Investigation, and the Department of Homeland Security all work on immigration enforcement in some capacity. These agencies all use these surveillance systems, but also work with large tech companies to ensure these systems are set up. These agencies are used by the government because the government often justifies surveillance as a means to enhance national security. Whether that is true or not can be debated.

Large Tech Companies

Tech companies such as Palantir, which was mentioned earlier, and Northrop Grumman. Palantir may be the most well known for its controversial ImmigrationOS software (Hubbard, 2025). Further collaboration can be seen in the $51.6 million contract the government made with Palantir (Nalbandian, 2022). The goal of this contract was for Palantir to create a case management system. Similarly to Palantir, Northrop Grumman signed a $95 million contract with the Department of Homeland Security in 2018 (Nalbandian, 2022). With the ultimate goal of creating a new database that would hold data such as: fingerprints, palm prints, facial image and iris scans, and deported felons and immigration violators. The most notable feature of this system would be its ability to hold 500 million unique identities (Nalbandian 2022).

U.S. Citizens

Immigrants

Non-Citizens

Politicians

Government Agencies

Large Tech Companies

Which argument is commonly used to justify expanding surveillance at borders?

- ☐ It promotes cultural assimilation
- ☐ It reduces government spending on technology
- ☐ It enhances national security
- ☐ It eliminates all migration

What is ImmigrationOS

- ☐ A specific software company that has a contract with a government agency
- ☐ A tool created by Palantir, contracted by ICE in an effort to help with immigration
- ☐ A database used by the government

What company has a $95 million contract with the Department of Homeland Security?

- ☐ Palantir
- ☐ Cisco
- ☐ Northrop Grumman

What types of surveillance is used within immigration enforcement?

Surveillance technology may be artificial intelligence, machine learning, deep learning and neural networks. Artificial intelligence (AI), while not formally defined, can be understood as a machine-based operation that has the ability to mimic human intelligence (Nalbandian 2022). Artificial intelligence is also being integrated as a predictive tool, to collect data and identify patterns, and clearly identify possible people of interest. It can be used as a forecasting tool to identify the direction and intensity of such patterns. It can be used in facial recognition systems, as well (Rinaldo & Teo 2025, 61-89). Machine learning is a subset of artificial intelligence and can be more clearly defined as the system that automates analytical modeling; it enables systems to learn from data, identify patterns, and ultimately make decisions. Previously, machine learning has looked like a tool to predict whether visa recipients are overstaying their visas or not (Azizi & Yektansani 2020). A study found that the machine learning algorithm was correct 80% of the time when it came to their prediction of who would overstay their visas.

That leaves a 20% margin of error. For a use within immigration, which drastically impacts and uproots so many lives, having such a large margin of error is unacceptable, unjust, and inhumane. Social media can also be used as a surveillance tool within the immigration process. This tool is distinct because it can be used as a tool to surveil even across the world. In this day and age, most of the population has some sort of social media account, making this a very accessible form of surveillance for governments to rely on. With the implementation of surveillance technology, comes concerns of algorithmic bias. Algorithmic bias occurs when these tools cause more errors for already marginalized groups. A study performed by MIT Case Studies in Social and Ethical Responsibilities of Computing identifies racial disparities furthered by similar systems (Perkowitz 2022). Facial recognition software is bound to be inaccurate at times. Technology is not perfect, these errors are to be expected. Yet, what should not be expected is that these systems are typically less accurate when applied to people of color, with errors up to 35% of the time for faces of female women of color. That is unjust.

Name an example of biometric surveillance that's used in immigration control? _____

_____

_____

A study found that the machine learning algorithm was correct. How much of the time when it came to their prediction of who would overstay their visas?*

- ☐ 60%
- ☐ 80%

- ☐ 40%
- ☐ 20%
- ☐ 90%

Algorithmic bias in immigration surveillance refers to:

- ☐ Migrants hacking into surveillance systems
- ☐ Errors caused by poor internet access at borders
- ☐ Surveillance tools disproportionately misidentifying certain racial groups
- ☐ Governments relying too heavily on human judgment

Ethics of Surveillance in Immigration

One scholar that interested me in particular as I was doing research was Ana Muniz who argues that surveillance technology is an inherently racist practice that no longer stops at the border. Because technology is so ingrained into our society, borders are not an abstract idea that follows people around almost in a haunting way. Borders now serve more as a social barrier, constantly reminding immigrants and non-US citizens of their "outside"-ness. This comes with major ethical concerns. To name one major concern, particularly when it comes to migrants themselves, is whether or not they are able to fully consent to the government's use, collection, and analysis of their personal data.

What does Ana Muniz touch on?

- ☐ The idea of a non-physical border.
- ☐ Surveillance as an inherently racist practice.
- ☐ Surveillance systems and their furthering of systemic inequality
- ☐ All of the above

What is a major ethical concern with collecting migrants' biometric data?

- ☐ The cost of the technology
- ☐ Migrants may not fully consent to data collection
- ☐ Too many migrants prefer digital systems
- ☐ It slows down border processing
- ☐ Other:

Some things to think about

There's no correct answer for the questions below, but it gives you a chance to think about the topic in a more broad way.

What is one possible human rights concern associated with facial recognition technology at borders?

How might surveillance technologies push migrants toward more dangerous routes?

Name one type of data that border agencies commonly collect from migrants.

Why might private companies involved in immigration surveillance face calls for greater transparency?

How can heavy surveillance affect immigrant communities psychologically or socially?