PERSPECTIVES May 21, 2025

Trump’s Immigration Crackdown Is Built on AI Surveillance and Disregard for Due Process

Illustration by Mitch Blunt.

This piece was first published by Bulletin of the Atomic Scientists.

In March, officials at the US State Department revealed that they would use artificial intelligence to revoke the visas of "foreign nationals who appear to support Hamas or other designated terror groups." The new program, known as "Catch and Revoke," will scan social media accounts and is part of a broader uptick in the US government's use of AI-powered surveillance, with the goal of combating antisemitism, terrorism, and illegal immigration. And the word "uptick" may be a significant understatement. According to the Brennan Center of Justice, the Trump administration is planning to gather social media identifiers of more than 33 million people, "including those applying for permanent residence or adjustment of their immigration status."

Social media monitoring is not new, nor are US immigration policies necessarily an outlier when compared to other democracies. However, the US changes, which are in keeping with a global trend of increasing state surveillance of noncitizens, have implications for the free expression and due process rights of the population as a whole.

Social media surveillance differs legally and technically from other forms of surveillance. Because it is based on publicly available information, law enforcement agencies generally do not need to follow the robust legal safeguards that are associated with wiretaps and other covert types of monitoring. Autocratic leaders have used monitoring tools to silence political opponents and repress minority populations. In democracies, courts have found that security and law enforcement agencies have sometimes overstepped their authority and even abused antiterrorism policies to target protected speech. As monitoring has increasingly been outsourced to the private sector, a new industry of data brokers can collect, analyze, and share with law enforcement agencies people's personal data without their knowledge, undermining privacy and due process. Ubiquitous monitoring of speech, even public speech, has a chilling effect on free expression. Further, the automated tools officials use during investigations can produce costly errors, such as misinterpreting speech or context to arrest the wrong individual.

Laws and technologies first launched to combat the threat of terrorism and foreign invasion have now been repurposed to curtail migration. All governments have a responsibility to secure their borders from potential threats and enforce immigration policy in line with the rule of law. Without appropriate oversight, however, the growing use of AI surveillance technologies could exacerbate errors and injustices. Recent moves by the

Trump administration to sidestep due process for undocumented immigrants and even legal residents have generated legal scrutiny around the rights of noncitizens in a democracy. Across the Atlantic, European governments have taken this further by expanding powers to revoke the citizenship of naturalized citizens.

While democracies have granted national security and immigration agencies significant leeway to accomplish reasonable policy objectives, governments should provide some oversight and accountability to prevent malfeasance and error and to offer redress for those wrongly accused. In short, they must maintain democratic guardrails when employing powerful tools.

Surveillance states. Mass data collection and advances in AI have led to new tools for monitoring the everyday activities of billions of people at scale. When used responsibly and accountably, surveillance, whether physical or digital, can play an important role in protecting national security and fighting crime. Many governments, however, have resorted to extreme surveillance methods to maintain political control under the guise of ensuring public safety.

The Chinese Communist Party operates what is arguably today's most sophisticated surveillance state. Through a combination of digital technology and a decentralized but well-organized network of bureaucrats, spies, and informants, the Chinese Communist Party intrusively monitors its citizens for the purpose of repressing certain ethnic and religious identities, silencing political dissent, and preventing public demonstrations. Surveillance is most intense in Xinjiang and Tibet, two regions that are home to significant minority populations. If an algorithm flags certain behavior as "suspicious," an individual can end up in prison or interned in a state-run reeducation camp for years on end, without the right to a fair trial.

The Russian government uses AI to monitor social media platforms for content such as criticism of the invasion of Ukraine, calls for protests, support for opposition figures, involvement in persecuted religious movements, and material that is flagged as "extremist" or "LGBT propaganda." Similarly, Iran's Cyber Police (FATA) monitors social media for any speech that threatens regime stability, advocates for women's rights, or contravenes the regime's official religious doctrine.

The United States and other democratic powers are distinguished from authoritarian regimes by their better respect for civil liberties, due process, and oversight from judicial and legislative authorities. Nevertheless, their surveillance capacity is immense, making it all the more important for these

countries to adhere to their own democratic principles. Legal safeguards have not always been strong enough to prevent overreach by law enforcement and intelligence agencies in democracies. For example, a series of federal court rulings struck down elements of the US National Security Agency's surveillance operations that related to the collection of data on US persons. Additionally, Congress passed reforms to end the bulk collection of phone records in 2015. But in April 2024, US lawmakers reauthorized provisions that allow the government to sidestep judicial oversight when targeting non-US persons abroad, despite evidence that some law enforcement agencies have improperly used these capabilities to investigate Americans who communicate with foreign persons.

Similar developments have taken place in Europe. A wave of deadly Islamist terror attacks across the continent led to a spate of new laws with provisions that increased warrantless and indiscriminate surveillance of electronic communications, extended pretrial detention, curbed free expression, curtailed free movement, and even allowed revocations of citizenship. Some of these measures were later ruled unconstitutional or in contravention of European Union (EU) law. Nonetheless, European governments have continued to experiment with new and intrusive technologies, leading to significant abuses.

Outsourcing surveillance. A vast new private industry has emerged to service the surveillance needs of governments around the world. For example, mobile forensic tools allow law enforcement agents to bypass device passcodes and encryption when searching devices at national borders, police checkpoints, and detention centers. Researchers discovered that in 2024, Serbian authorities used a tool from Cellebrite, an Israeli mobile forensics firm, to bypass device encryption and load a spyware program onto the phone of a journalist held in detention. Commercial spyware, meanwhile, enables security agencies to remotely access a target's phone or computer and either download its contents, take a screen recording, or activate the camera and microphone. These powerful products have been abused to spy on politicians, journalists, opposition figures, lawyers, judges, businesspeople, and members of civil society around the world. In 2023, a European Parliament inquiry found illegalities around its use in Hungary and Poland over the past five to 10 years and noted insufficient safeguards in Greece and Spain.

Rather than focusing on access to individual devices, many commercial surveillance companies offer tools that exploit the trove of sensitive information that is publicly available and convert it into useful outputs for security and law enforcement agencies. Each time a person opens an app,

runs a search query, or makes an online purchase, an entire constellation of information is updated, analyzed, and shared across third-party services and advertising ecosystems. Without robust safeguards, personal data collected for one purpose may later be misused in ways that are dangerous, discriminatory, or unethical.

Clearview AI, a US company that offers facial-recognition technology, has been sued in the United States, France, and the Netherlands for privacy violations related to its alleged practice of scraping the internet and social media platforms to compile its extensive database of online facial images. The company's US clients have included the Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement (ICE), and local police departments. Separately, an investigation into hacked files from Gravy Analytics, a location data company, revealed that advertising firms had likely exploited thousands of applications—including popular apps used for gaming, dating, fitness, period and pregnancy tracking, email, and religious prayer—to monitor users without their knowledge. In January, the Federal Trade Commission took unanimous action to prohibit the company and its subsidiary from tracking and selling user data, except in "limited circumstances involving national security or law enforcement." Earlier reporting had shown that the subsidiary had commercial partnerships with the FBI, Customs and Border Protection, and ICE, indicating that such personal data covertly collected from ordinary users may indeed be accessible to powerful government agencies in practice.

Overall, mass surveillance has a chilling effect on free expression and other basic rights, as the fear of incessant monitoring deters people from interacting online, conducting academic research, practicing their chosen religion, or engaging in political activity. Moreover, tools such as facial-recognition technology and generative AI continue to produce errors and hallucinations, and when used for policing and criminal sentencing, automated systems can replicate and reinforce discriminatory practices. Unearned confidence in novel technologies may also cause police officers to neglect standard procedures and investigative methods that could yield different conclusions.

Beyond borders. All governments limit who can enter or reside in their country, and all have a duty to secure their borders from a wide range of threats. In the United States, border agents possess great authority to conduct monitoring and data collection, and legal protections for both noncitizens and citizens are generally weaker within 100 miles of any border—an area that encompasses roughly two-thirds of the population. As the United States expands its surveillance capacity for the purpose of enforcing its immigration policies, its officials must respect due process and

act within the bounds of the law. A series of recent Trump administration enforcement actions have sparked concerns about their haste, legality, and potential impact on free expression and other fundamental liberties.

On his first day in office this year, President Trump signed an executive order that called on federal law enforcement, immigration, and intelligence agencies to vet and screen “to the maximum degree possible” immigrants seeking admission to the United States, as well as those already in the country. The Department of Homeland Security (DHS) also stood up a task force to monitor the online activities of foreign students in the United States in order to find grounds for revoking their visas. In the three months since President Trump’s executive order, more than 1,500 students have had their immigration status abruptly altered or revoked, often with little explanation. Facing court challenges, the government later restored many students’ status but signaled that visa terminations would proceed under a different mechanism.

In addition to surveillance, the administration’s use of wartime powers not invoked since the 1940s has drawn objections related to due process and the rule of law. President Trump cited the 1798 Alien Enemies Act to justify the warrantless arrest and deportation of more than 100 alleged Venezuelan gang members to a prison in a third country, El Salvador. The US Supreme Court has since intervened to temporarily halt certain additional deportations and clarified that potential deportees must be granted some opportunity to challenge their designation; on May 1, a federal judge in Texas ruled that this use of the Alien Enemies Act to deport Venezuelans was illegal. But other deportees have received similar treatment on different legal grounds.

As part of a reported $15 million deal with the Salvadoran government, US authorities have sent a total of at least 252 Venezuelan and 36 Salvadoran migrants to El Salvador without due process, and all but one are currently being held incommunicado. Federal courts in Maryland have ruled that at least two people were unjustly deported to the country.

Due process refers to a spectrum of protections that vary according to circumstances. People who arrive at the US border without legal status do not enjoy the same rights as lawful permanent residents or naturalized citizens; the applicable level of process is specified by the courts, in keeping with the country’s constitution and laws. Practices that undermine due process for alleged criminals, undocumented immigrants, and visa holders can also have repercussions for permanent legal residents and even US citizens.

The detentions of Mahmoud Khalil and Mohsen Madawi, two US permanent residents and Columbia University students involved in pro-Palestinian activism, as well as Rümeysa Öztürk, a Tufts University student who coauthored an op-ed on the issue, have made national headlines due to their serious implications for freedom of speech and due process. And attorneys for three US citizens—the young children of undocumented immigrant mothers—have claimed in separate cases that the government acted too hastily when removing them to Honduras. A lack of due process could lead to significant mistakes or abuse, including the deportation of US citizens under laws designed for noncitizens. Alarmingly, President Trump has repeatedly stated that his administration is "looking into" methods for deliberately sending US citizens to prisons abroad, a move that legal scholars say would likely violate the constitution.

Fragile citizenship. While the US administration attempts to further reduce protections given to noncitizens, many other governments are taking this a step further by expanding the reasons for revoking the citizenship of naturalized citizens and dual nationals, purportedly as a means of addressing terrorism and serious crime. Governments generally have constitutional or legal provisions allowing for the revocation of citizenship or "denaturalization," particularly in cases of fraud during the application process. Revocations in the latter circumstance are allowed in the United States, though they remain relatively rare. However, several European governments have shown increasing openness to stripping citizenship for a wider variety of reasons, raising the potential for discrimination and even repression.

German authorities, who have notably ordered the deportation of three EU citizens and one US citizen for their alleged role in pro-Palestinian protests, are now negotiating legal reforms that would allow for the revocation of citizenship for "supporters for terrorism, antisemites, and extremists"—broad categories that could penalize forms of nonviolent political, social, or religious expression protected under international law. Swedish lawmakers are considering constitutional amendments that would allow the government to withdraw citizenship from those who commit certain crimes; Sweden's ruling parties have sought to emulate Denmark, where a 2021 law enables the loss of citizenship for gang-related crime, lowering the bar from grave offenses such as terrorism or treason.

All such laws risk creating a tier of "second-class citizens" whose rights and protections are more fragile and contingent than native-born citizens. Given the rise of nativist sentiment across the continent and the popularity of political parties that espouse exclusionary views on race and culture, there are also

fears such laws would be disproportionately used against certain ethnic and religious groups. Vague provisions can also be repurposed for political repression: A new law in Hungary allows for the temporary suspension of citizenship rights for dual nationals of non-European countries who have "undermined the sovereignty of Hungary" or acted "in the interest of foreign powers." Such charges have already been weaponized to investigate civil society organizations and curb political dissent in the country.

International law bars governments from revoking citizenship if it would render an individual stateless, meaning new laws and enforcement actions in democracies generally focus on dual nationals and naturalized citizens who could revert to their previous nationality. That's not necessarily the case in authoritarian regimes, which feature less respect for free expression and due process. For example, governments in the Middle East have stripped the citizenship of hundreds of journalists, dissidents, and human rights defenders over the past decade, leaving many of them stateless. Nicaragua's president revoked the nationality of 222 citizens—including political leaders, priests, activists, and students—who were deported to the United States in February 2023, as well as a further 135 political prisoners deported to Guatemala in September 2024.

The dangers of unchecked power. Modern societies have developed sprawling physical, institutional, and digital infrastructures to implement policies that secure the freedom and prosperity of their people. But in the course of addressing significant internal and external threats, all governments risk eroding the same rights they are tasked with protecting. What makes democracies unique is their ability to minimize, mitigate, and correct such mistakes using tools such as freedom of expression, due process, and independent courts of law. These protective and adaptive qualities distinguish the United States and other democracies from the corrupt and draconian regimes in Moscow, Beijing, and Tehran.

Without the software of democracy, the devastatingly powerful hardware of a modern state can easily be reprogrammed for authoritarian rule. Injustice in such a system soon becomes a feature rather than a bug.

https://freedomhouse.org/article/trumps-immigration-crackdown-built-ai-surveillance-and-disregard-due-process