ICE Facial Recognition Reveals Interplay Between Federal, State, Local and Private Surveillance

ICE Facial Recognition Reveals Interplay Between Federal, State, Local and Private Surveillance

by **Mike Maharrey**, *Tenth Amendment Center*
July 8, 2020

When it comes to the rapidly growing national surveillance state, federal agencies such as the NSA and FBI get most of the attention. But in fact, state and local law enforcement agencies, and increasingly private third-parties, make federal surveillance possible. A careful look at Immigration and Customs Enforcement (ICE) facial recognition surveillance reveals just how intertwined federal, state, local and third-party spying has become.

I've been arguing for years that the federal government encourages and funds surveillance technology at the state and local levels across the U.S., thereby gaining access to a massive data pool on Americans without having to expend the resources to collect the information itself.

The feds can share and tap into vast amounts of information gathered at the state and local level through fusion centers and a system known as the "information sharing environment" or ISE.

Fusion centers were sold as a tool to combat terrorism, but that is not how they are being used. The ACLU pointed to

a bipartisan congressional report to demonstrate the true nature of government fusion centers: “They haven’t contributed anything meaningful to counterterrorism efforts. Instead, they have largely served as police surveillance and information sharing nodes for law enforcement efforts targeting the frequent subjects of police attention: Black and brown people, immigrants, dissidents, and the poor.”

Fusion centers operate within the broader ISE. According to its website, the ISE “provides analysts, operators, and investigators with information needed to enhance national security. These analysts, operators, and investigators…have mission needs to collaborate and share information with each other and with private sector partners and our foreign allies.” In other words, ISE serves as a conduit for the sharing of information gathered without a warrant. Known ISE partners include the Office of Director of National Intelligence which oversees 17 federal agencies and organizations, including the NSA. ISE utilizes these partnerships to collect and share data on the millions of unwitting people they track.

The feds created the infrastructure supporting the national surveillance state, and they supply a lot of the funding, but state and local law enforcement agencies do the grunt-work. And increasingly, private companies are stepping in to fill the gaps.

ICE reveals how this system functions in the real world.

Like most law enforcement agencies, ICE has waded into the world of facial recognition. But as an article published by *Nextgov* explains “rather than build its own database and biometric apps, the agency opts to use third-party services from the private sector, state and local law enforcement and other federal agencies.”

An ICE division known as Homeland Security Investigations

(HSI) conducts all of the agency's facial recognition services. According to the *Nextgov* report, third parties including other government agencies and private vendors do all of the actual work.

> *According to a privacy impact assessment (PIA) issued May 13 and released publicly last week, HSI agents either send photos to the facial recognition service through encrypted email or upload through a third-party website. At no point does HSI manage any facial recognition software or image databases.*

The report lists a number of facial recognition "service providers" used by ICE.

- State and local law enforcement
- Regional and Subject Matter-Specific Intelligence Fusion Centers
- Federal Agencies – This includes a number of databases starting with DHS's Automated Biometric Identification System, or IDENT. This is currently on track to be replaced by the cloud-based Homeland Advanced Recognition Technology, or HART, system. ICE investigators also have access to the State Department's Consular Consolidated Database allowing it to check images against passport photos. It can tap into the FBI's Next Generation Identification System (NGI), a massive database that stores photos on more than 38 million convicted criminals. And finally, ICE can access the Defense Department's Automated Biometric Identity System (ABIS). This is primarily used in support of military operations and could soon be connected directly to the IDENT/HART system, according to the PIA.
- Commercial Vendors – primarily for open-source collections of publicly available images. Some vendors have also developed facial recognition software that HSI agents can use. In such cases, after an agent uploads an

> image to the application, the vendor is required to "delete the image immediately upon creation of a face template." The PIA notes that, "While HSI cannot directly control the means or methods of a vendor's data collection efforts, if HSI discovers that an FRS violates the privacy settings of an open-source system, HSI will discontinue using that vendor's FRS."

All of these existing databases allow ICE to run a facial recognition program without investing in facial recognition technology or expending the manpower to gather the data.

The *Nextgov* report focuses on ICE and facial recognition surveillance, but federal agencies almost certainly utilize the same strategy to facilitate other kinds of surveillance. It can tap into databases containing location data, cell phone information, license plate data, drone surveillance data and more without having to actually operate stingray devices, ALPRs, or drones. State and local cops gather the data and then dump it into these massive databases that every law enforcement agency in the country can access – including the feds.

The federal government continues to build out a national surveillance state, partnering with state, local and private entities to create a tangled web that becomes increasingly difficult to untangle. This is why it's critical to limit the use of surveillance technology and data sharing at the state and local levels. Every limit on surveillance in a county or city takes a small bite out of the system. Data that is never gathered can't be shared.