Photo ID is Obsolete and Unnecessary. Facial Recognition Technology Makes it Dangerous.

In mid-May, San Francisco, California became the first American city to ban use of facial recognition surveillance technology by its police department and other city agencies. That's a wise and ethical policy, as a July 7 piece at the *Washington Post* proves.

Citing documents gathered by Georgetown Law researchers, the *Post* reports that at least two federal agencies, the Federal Bureau of Investigation and Immigration and Customs Enforcement, have — for years — mined state photo ID databases to populate their own facial recognition databases.

To put a finer point on it, those agencies have been conducting warrantless searches, seizing private biometric data on the entire population of the United States, most of whom are neither charged with, nor suspected of committing, a crime.

They've conducted these fishing expeditions not just without warrants, but absent even the fig leaf of legislation from Congress or state legislatures to lend supposed legitimacy to the programs.

The *Post* story, intentionally or not, makes it clear that Congress must follow San Francisco's example and ban use of facial recognition technology, as well as repeal its national photo ID ("REAL ID") scheme, and require federal agencies to delete their facial recognition databases. The states should either lead the way or follow suit by doing away with government-issued photo identification altogether.

Photo ID has always been marginally useful at best. Anyone who's ever worked at a bar or liquor store knows that it's unreliable on a visual check — and that its uses have been stretched far beyond its supposed purposes.

The most common form of photo ID is the driver's license. States imposed their licensing schemes on a seemingly justifiable pretext: A driver's license proves that the driver whose photograph appears on it has taken and passed a test demonstrating safety and proficiency behind the wheel.

There are ways to do that without a photo. Three that come to mind are a fingerprint, a digitized summary of an iris scan, or a similar summary of a DNA scan.

Yes, those methods are more expensive and impose a slightly higher burden on law enforcement in identifying a driver who's been pulled over or arrested (and on anyone else who wants to confirm an individual's identity). But they're also far more reliable and less easily used in pulling police-state type abuses like those described in the *Post* story. They can’t be used for easy warrantless searches via distant cameras.

In recent decades, and especially since 9/11, the conversation over personal privacy has revolved around how much of that privacy “must” be sacrificed to make law enforcement’s job easier.

The answer to that question is “none.”

It’s not an American’s job to make law enforcement’s job easier. It’s law enforcement’s job to respect that American’s rights.

Since law enforcement has continuously proven itself both unwilling and untrustworthy on that count, we need to deprive it of tools that enable that unwillingness and untrustworthiness.

Photo ID is obsolete and unnecessary. Facial recognition technology makes it dangerous. Let’s take those tools away from their abusers.