# Should Law Enforcement Agencies’ Use of Facial Recognition Software Be Subject to Regulation?

As **The New York Times** and **The Washington Post** recently reported, facial recognition software is being heavily utilized by government agencies, who are using the software to search state driver’s license databases, despite the fact that most of the photos in the databases are of citizens who have never committed a crime and have never given any sort of consent to the searches.  The reports have raised concerns about the lack of regulation and oversight currently with respect to the use of facial recognition software by law enforcement.

According to a report by **The New York Times**, since 2011, the FBI has run nearly 400,000 facial recognition searches  of federal and local databases, including DMV records.  **The Washington Post** reports that the FBI is currently running about 4000 searches per month.

Moreover, **The New York Times** and **The Washington Post** are reporting that in states offering driver licenses to undocumented immigrants, Immigration and Customs Enforcement (“ICE”) is  using the software to conduct searches on undocumented immigrants.

**The Washington Post** reports that twenty-one (21) states and the District of Columbia allow federal investigators to scan driver’s license photos, and that those searches generally require no more than an email request to conduct the search.

A number of lawmakers in Washington are raising concerns about the recent revelations, and two cities, San Francisco and

Somerville, MA, have now imposed a ban preventing police and public agencies from using the software. **The Washington Post** reports that a privacy coalition has petitioned the Homeland Security Committee for the Department of Homeland Security ("DHS") to stop using the technology.

What are the arguments being raised in favor of greater regulation of law enforcement's use of the technology?

First and foremost, proponents for greater regulation argue that running facial recognition searches against photos of law-abiding citizens is a huge privacy violation. Secondly, they argue the scope of it use by law enforcement is too broad, since it has been used not only for the identification of criminal suspects but also to find witnesses, victims, and bystanders. Third, they argue its use often constitutes a breach of trust, since states encourage undocumented immigrants to submit their information to the databases and then proceed to to tun it over to ICE. Fourth, they argue that use of the software heightens the risk of misidentification and false arrest due to inaccuracies with how certain facial features are detected.

All in all, it is clear that law enforcement considers facial recognition software to be a valuable investigative tool. However, there are clearly some valid concerns with how the software is being used that warrant further consideration. Should law enforcement really be able to conduct these types of searches without a warrant? Should ICE be able to conduct searches of undocumented immigrants who have been encouraged to submit information for inclusion in a database? What kind of checks should be in place on law enforcement's use of software that that has inherent inaccuracies?