Automatic License Plate Readers: An Effective Law Enforcement Tool or the Latest Tool for Mass Surveillance? A Brief Look at the Legal and Policy Issues Involving LPR Technology

Professor Randy L. Dryer

Although license plate recognition technology has been around for years, concerns over privacy have only recently come to the forefront of the public's attention. This growing concern is due to several factors. First, LPR systems have proliferated throughout the country as law enforcement learns of its usefulness in crime interdiction. Currently, there are thousands of local police departments employing the technology on police cruisers and several cities record the comings and goings of every vehicle into or out of the city limits. Second, there is a movement to maximize the usefulness of the data collected by aggregating it in massive regional databases. The states of California, Virginia and Maryland already participate in such databases and others are considering doing so. The Department of Homeland Security recently scuttled plans by Immigration and Customs Enforcement to create a national database of license plate information. Third, there is a lack of uniform standards governing the retention, access and use of the data collected. Some government units destroy the data after a relatively short period of time, while others store the data indefinitely. Fourth, the federal government is funding the acquisition and expansion of the technology by local law enforcement agencies through grants from the Department of Justice and the Department of Homeland Security. Finally, there is a growing sensitivity to the privacy issues arising from geo-location tracking in light of the U.S. Supreme Court's recent decision in U.S. v. Jones, which held that the warrantless installation of a GPS tracking device on a suspect's vehicle implicated Fourth Amendment protections even when the surveillance was of movement on public streets. As a consequence, state legislatures have begun addressing this technology by either restricting its use or mandating certain standards regarding use, retention and access of the data collected. In Utah, a pending suit by a private company which deploys license plate reader technology and sells the collected data to police departments, debt collectors and repossession companies, has challenged Utah's law on First Amendment grounds.

This presentation will identify the privacy risks associated with unregulated use of this technology and the data it collects, survey the various legislative attempts to regulate the technology, offer a brief recap of the potential First and Fourth Amendment issues implicated and suggest some principles which should be considered in any regulatory regime.