Collin County Sheriff's Office

Memorandum

To: Keith Self, County Judge

From: Jim Skinner, Sheriff

Date: Wednesday, October 17, 2018

Re: Response to Keith Self's Oct. 16 Question about LPRs and Privacy

---

Judge Self,

I understand today that you have asked my staff about our efforts or policies that safeguard citizen's privacy rights as they relate to the use of License Plate Reader (LPR) technology. The short answer is that we are developing policies regarding how we use this technology to ensure we are compliant with the Constitution and laws of the Nation and state. Like you, we strive to be vigilant in meeting our obligations to protect all the rights of citizen's constitutional rights, including privacy rights. At the same time, the Texas Dept. of Public Safety states that law-enforcement officials have a duty to collect and disseminate certain information, including "active and historical [LPR] data." [1] To date, we typically use LPRs to give us warnings or notices of wanted individuals or missing children that have been entered into the National Crime Information Center (NCIC). Two recent examples of this would be the arrests by our highway interdiction deputies of two Capital Murder fugitives, one of whom had machine guns and drugs in his vehicle. Another example is the recovery of two missing children, one of which was in a vehicle with three adult men whom she did not know. In both of these instances, LPR technology identified the vehicle as it passed. Below is some additional information you may find useful.

LPR. A law-enforcement agency may use an LPR in a fixed location like a parking lot or under a bridge on a highway or an LPR in a police vehicle. The LPR records the license plates of nearby vehicles and saves the data (time, license plate, and location). This LPR data can be run through a subscription database (*e.g.*, ELSAG or Vigilant) to see if a license plate has been flagged or hot listed for a law-enforcement reason. In all, however, LPRs collect only license plate numbers, which are unconnected to any person's name.

Privacy Rights [2]. In general, a person has no reasonable expectation of privacy in driving a car through a public space like a state highway, public road, or public parking lot. [3] In contrast, a person has a reasonable expectation of privacy in certain movements on private property or within a private residence. [4] Also, the government's planting a GPS device on a vehicle and tracking it for an extended time may violate a person's privacy rights. [5] And, in a recent case, *Carpenter v. United States*, No. 16-402 (June 22, 2018), the U.S. Supreme Court held that the FBI needs a search warrant supported by probable cause to access seven days' or more worth of an individual's cell-site location information (CSLI). The Constitution protects the public, for example, by requiring law enforcement to act only upon reasonable suspicion or probable cause or to obtain a search warrant. [6]

LPRs and Privacy. Here, LPRs are much closer to police observation in a public place than to an officer's placement of a GPS tracker on a person's car without permission, using a thermal imager on a private home, or obtaining seven days' worth of a person's CSLI from a phone company. LPRs do not collect personal data. LPRs collect license plate numbers. An LPR readout does not give one the personal information that is unique to that license plate. The normal process of requesting license plate information through the Texas Law Enforcement Terminal System (TLETS) is required to obtain all personal information on a license plate, and we are restricted by rules and regulations promulgated by the Texas Department of Public Safety to do so.

To protect privacy while fulfilling our duty to keep the peace and investigate crime, we are in the process of updating policies that govern the deployment of our LPRs, use of hot lists, actions that deputies may take and on what predicates, data sharing, and data retention. For example, my policy would require a deputy to have a proper predicate—as part of a criminal investigation or effort to locate a missing person—to try to link a license plate number to a person's name. Also, our policies would limit the storage of any LPR data to 45 days or less. The *September 2014 Privacy Impact Assessment* for DPS discusses these privacy issues in greater detail. But I hope this helps place LPRs on the map of police technology and privacy rights.

Resources

[1] September 2014 Privacy Impact Assessment for the Texas Department of Public Safety (DPS), Collection, Storage, Management and Use of Automated License Plate Reader Data, at 3 ("Law enforcement (LE) officials have a duty to investigate crimes and criminal conduct. To fulfill this responsibility, officers collect, analyze, disseminate, and retain a variety of information, which should include active and historical License Plate Reader (LPR) data."), *available at* https://www.dps.texas.gov/administration/crime_records/pages/LPRPIA.pdf.

[2] U.S. Constitution, art. IV; Texas Constitution, art. I, § 9.

[3] A person has no reasonable expectation of privacy in driving a car through a public space. *See United States v. Knotts*, 460 U.S. 276 (1983); *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012); *Ford v. State*, 477 S.W.3d 321 (Tex. Crim. App. 2015).

[4] In contrast, a person may have a reasonable expectation of privacy in certain movements on private property or within a private residence. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27 (2001); *United States v. Karo*, 468 U.S. 705 (1984).

[5] *See United States v. Jones*, 132 S. Ct. 945 (2012).

[6] For example, an officer needs a reasonable suspicion that a person is, has been, or soon will be, engaged in crime to make an investigative detention. *See Rodriguez v. United States*, 135 S. Ct. 1609 2015); *United States v. Arvizu*, 534 U.S. 266 (2002). Without exigent circumstances, an officer needs probable cause and a warrant to conduct a search. *See Carpenter v. United States*, No. 16-402 (June 22, 2018); *Katz v. United States*, 389 U.S. 347 (1967).