

# METADATA AND PARKING

By Leonard T. Bier, JD, CAPP

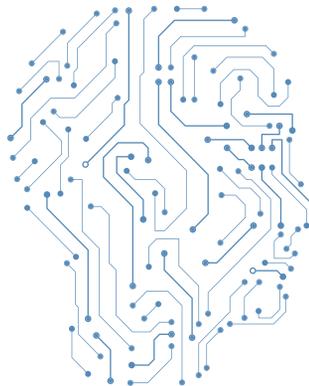
The defection by Edward Snowden from the U.S. to Russia spotlighted the metadata intelligence gathering of the U.S. National Security Agency's (NSA) Prism Program. The general practice of collecting and analyzing telephone metadata by the NSA and the federal government significantly intensified after Sept. 11, 2001, and the NSA has requested, received, and stored data from every domestic phone call since 2006.

The intelligence gathering of telephone metadata disclosed by Snowden has been the subject of acrimonious public debate. The Federal District Court for the Southern District of New York, in a well-reasoned and readable decision by Judge William H. Pauley III in the matter of *ACLU v. James Clapper et. al.*, ruled that the collection and analysis of telephone metadata by federal security agencies is constitutional.

Why is the gathering and analysis of metadata of concern to public and private parking operators? To begin with, the Foreign Intelligence Surveillance Act (FISA), amended in 1998, permitted the federal government, under certain conditions, to issue an order to produce records related to entities in the business of public transit, accommodation facilities, storage facilities, and car rental. The Patriot Act later allowed the federal government to secure an order from the Foreign Intelligence Surveillance Court (FISC) to review any business record. The government recognized that knowing where a person was flying, temporarily residing, renting or parking a car, or storing materials can have national security value.

After Snowden's well-publicized flight from the U.S., I received a number of emails from IPI members who use pay-by-license plate or cell phone and multi-space meters, as well as on-street license plate recognition (LPR) systems, asking what they should do with the license plate data they have accumulated and stored. These technologies allow operators to store data that include license plate number and the GPS location or meter zone where vehicles park, along with the duration of each stay.

Parking managers were concerned that by retaining license plate information, they accumulated metadata and could be infringing on their customers' constitutional



rights. Since 1979, the U.S. Supreme Court in *Smith v. Maryland* has stated that individuals have no expectation of privacy when they voluntarily give up telephone information to a third party (the phone company) by placing phone calls. The phone number from which the call was placed, the number called, and the duration of the call are business records of the phone company and available to law enforcement. License plate data collected by public

and private parking operators is similar to phone records and would fall in this category.

The U.S. Supreme Court in *U.S. v. Jones* reasoned that short-term monitoring of a person's vehicle movement on public streets does not violate a person's expectations of privacy, but the use of longer-term GPS tracking devices does. Later, in *U.S. v. Katzin*, the U.S. Federal Court of Appeals, Third Circuit, ruled explicitly that GPS tracking devices cannot be attached to a vehicle by law enforcement without a search warrant.

The accumulation of license plate metadata by public and private parking operators does not involve placing any tracking device on a vehicle and should not be construed as a trespass on the vehicle or a warrantless search of the operator. The parker voluntarily enters vehicle information into a cell phone app or pay station to park in the public right of way. Entering a facility with LPR is no different than going through an EZ Pass toll booth, which records the vehicle's transponder and license plate.

License plate data without analysis are benign. The fact that a public or private parking operator captures license plate data violates no constitutional rights unless and until the data is used to track a specific vehicle's location. At that point, a parking manager will need legal advice as to whether license plate information is available to law enforcement with or without a warrant. **P**



**LEONARD T. BIER,** JD, CAPP, is the principal of Bier Associates. He can be reached at [lenbier@optonline.net](mailto:lenbier@optonline.net) or 732.828.8864.