# STANDING FOR PRIVACY RIGHTS

Dear Valued Client,

Over the past few months, DigiStream has explored utilizing Automated License Plate Recognition (ALPR) data, so-called “vehicle location reports,” and after a period of testing and consultation has elected not to utilize this technology. ALPR data will not be part of our investigative infrastructure due to privacy and data breach concerns with resellers of such information.

These reports have been widely used in the investigative industry since they became available for private-sector use in early 2013. The temptation to use the reports is significant. They consist of a searchable ALPR database of over 2 billion motor vehicle sightings reports nationwide, with tens of millions of records added monthly. ALPR is a surveillance method that uses optical character recognition on images to read license plates from both fixed platforms such as light poles and mobile platforms such as patrol cars or tow trucks. These ALPR reports include photographs of the vehicle and its license plate, as well as the exact location and time the photograph was captured. If you drive a vehicle in the United States, your activity is aggregated in this database.

DigiStream prides itself on the prudent application of advanced investigative methods as long as they prove legal, ethical and practical. However, we found usage of ALPR data was fundamentally different from other forms of investigation for reasons outlined in this paper.

## REASONABLE EXPECTATION OF PRIVACY

DigiStream believes the aggregation of billions of driver records captured via ALPRs violates the “reasonable expectation of privacy” of subjects under investigation. Few insurance claimants expect that investigators are accessing a database of over 2 billion geolocated photographs of their vehicles in order to track their location. No claimant would reasonably expect their driving activities would be subject to randomized surveillance wherever they may drive their vehicle.

The “mosaic theory,” set forth in United States v. Maynard, applies the doctrine of reasonable expectations to location data which, compiled over time, may reveal intimate personal details and habits. When ALPR data on a person’s license plate is compiled and examined in a mosaic, it may violate the driver’s reasonable expectation of privacy and infringes Fourth Amendment protections even though there is no expectation of privacy in a person’s travels on public roads.[1] In short, the whole becomes more valuable than the sums of its parts. When looked at in totality, cumulative ALPR data is much more telling than one single data point.

The International Association of Chiefs of Police noted in a 2012 policy guidance paper that, “Although there may be no reasonable expectation of privacy in any particular sighting of a vehicle traveling on a public roadway, the systematic capture, storage, and retrieval of ALPR data may nevertheless raise important privacy concerns.”[2] Common law privacy torts build their foundation upon Fourth Amendment jurisprudence regarding what can be considered “reasonable” with regards to issues of privacy, so DigiStream considers these opinions notable.

This concept of a “Penumbra of Privacy” is not new. It gained popular attention after Justice William O. Douglas’s 1965 majority opinion in Griswold v. Connecticut, stating that rights can be interpolated from the “general ideas” explicitly expressed in constitutional provisions. The amendments, in their aggregate, provide a zone of privacy not explicitly mentioned in any single amendment.[3]

[1] Gutierrez-Alm, Jessica (2015) “The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law,” Hamline Law Review: Vol. 38: Iss. 1, Article 5, pages 129-130. Accessed via: http://digitalcommons.hamline.edu/cgi/viewcontent.cgi?article=1054&context=hlr

[2] David J. Roberts and Meghann Casanova, Automated License Plate Recognition (ALPR) Systems: Policy and Operational Guidance for Law Enforcement, Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2012, page 31. Accessed via: http://www.theiacp.org/Portals/0/pdfs/IACP_ALPR_Policy_Operational_Guidance.pdf

[3] Glenn H. Reynolds, Penumbral Reasoning on the Right, 140 U. Pa. L. Rev. 1333, 1334–36 (1992); see also J. Christopher Rideout, Penumbral Thinking Revisited: Metaphor in Legal Argumentation, 7 J. ALWD 155, 155–56 (2010).

## DATA SECURITY

DigiStream began to have serious concerns over the integrity and security of the databases containing ALPR metadata and photographs after an October 2015 report by the Electronic Frontier Foundation[4] highlighted data breaches of law enforcement agencies. In September 2015 it was revealed by an investigative reporter that City of Boston ALPR data was freely accessible to the public, containing hundreds of thousands of records dating back to 2012.[5] With over 2 billion cumulative vehicle sightings, there is no rigid control over this disparate data, which represents a major privacy risk if the databases were to be hacked. The driving patterns of hundreds of millions of Americans would be open to stalkers and criminals of all sorts.

We feel that if the public sector is proving to be a poor guardian of ALPR data then the private sector data brokers who resell it are also at risk.

## LACK OF IDENTITY RESOLUTION

Determining whether the vehicle observed in the ALPR data is in fact being driven by the subject, a process we call “identity resolution,” is not possible due to the limited photographic views. Identity resolution is a key process in all types of investigation and insures that the correct individual is being surveilled. During manned surveillance, this is accomplished via ID shots, DMV records and other methods; during internet investigations, this is accomplished via reverse email searches, “friend” comparisons to known relatives and many other methods. Since ALPR data does not allow for this type of verification there is no way to know whether the vehicle, at the time of capture, was driven by the subject.

## SPORTSMANSHIP

This final point perhaps speaks less to matters of legality or ethics but more to a vague concept of fairness. Omnipotent metadata aggregation violates an unspoken rule of surveillance, which had existed since ancient times: the subject being surveilled had at least a sporting chance of countering the surveillance. Whether the subject “loses a tail” during manned surveillance, or decides to increase privacy settings on Instagram, the ability of those under surveillance to mitigate their exposure has always been a factor in the investigative equation. Those hired to engage in surveillance had to rely on the quality of their tradecraft to conduct a successful investigation. Poor tradecraft equated to poor results. ALPR data turns this dynamic on its head, and it is DigiStream’s belief that it is not to the benefit of the industry.

[4] Dave Maass and Cooper Quintin,, “License Plate Readers Exposed: How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech,” Electronic Frontier Foundation, October 25, 2015, accessed May 4, 2016. https://www.eff.org/deeplinks/2015/10/license-plate-readers-exposed-how-public-safety-agencies-responded-massive

[5] Kenneth Lipp, “License to Connive: Boston Still Tracks Vehicles, Lies About It, and Leaves Sensitive Resident Data Exposed Online,” digboston, September 8, 2015, accessed May 4, 2016. https://digboston.com/license-to-connive-boston-still-tracks-vehicles-lies-about-it-and-leaves-sensitive-resident-data-exposed-online/

## DIGISTREAM'S STANCE

In 2015, the National Conference of State Legislatures noted that there were 18 ALPR bills introduced or considered across the country. Four states, Arkansas, California, Minnesota and North Carolina, enacted legislation seeking to assuage concerns that "the [ALPR] information collected may be inaccurate, placed into databases and shared without restrictions on use, retained longer than necessary and used or abused in ways that could infringe on individuals' privacy."[6] Many of these laws simply outlined the fact that ALPR information should be treated as personal information and detailed steps to safeguard the data. Many said nothing about reselling data to the private sector. None of the laws addressed the private sector collection of ALPR data through tow truck or repossession agencies, a major source of information for data brokers who resell this information.

DigiStream believes ALPR data should only be used by law enforcement agencies, and only after court orders have been issued related to ongoing criminal investigations. Further, the length of time such data is stored on servers should be severely curtailed as there is no reason to maintain databases with billions of records on individuals who are not under active investigation. ALPR data should never be sold to data brokers, and certainly not resold to the private sector. This includes private investigative companies such as DigiStream, regardless of how ethical we otherwise behave.

[6] National Conference of State Legislatures. "Automated License Plate Readers: State Legislation," last modified November 13, 2015. http://www.ncsl.org/research/telecommunications-and-information-technology/2014-state-legislation-related-to-automated-license-plate-recognition-information.aspx