Self-driving cars and geospatial data: Who holds the keys?

February 5 2019

As self-driving cars continue to develop, there will be plenty of data amassed through cars' navigational technologies. Questions regarding privacy, ownership, cybersecurity and public safety arise, as heavily guarded mapping data is collected and leveraged by companies. The geospatial data can be used to draw new maps identifying the spaces where we live and travel. That information is currently housed in technological and corporate black boxes. Given the social relevance and impacts of such information, these black boxes require greater transparency, according to a Dartmouth study posted in *Cartographic Perspectives*.

As autonomous cars strive to make sense of the world around them, they collect massive amounts of data, including traffic and congestion patterns, where pedestrians cross the street, which houses and businesses have Wi-Fi, and other details, which could be monetized. While companies may have intellectual property and other economic interests in protecting geospatial data, local governments, private citizens and other actors also have a vested interest in using that data to inform decisions on managing traffic, urban planning, allocating public funds and other projects, all of which may be of public interest.

"Self-driving cars have the potential to transform our transportation network and society at large. This carries enormous consequences given that the data and technology are likely to fundamentally reshape the way our cities and communities operate," explains study author, Luis F. Alvarez León, an assistant professor of geography at Dartmouth.

"Right now, the geospatial data obtained by a self-driving car exists in technological and corporate black boxes. We don't know who can see the data, appropriate it or profit from it. With insufficient government regulation of data from self-driving cars, this raises significant concerns regarding privacy, security and public safety," Alvarez León adds.

The author discusses how legislation, open source design and hacking are avenues that can be leveraged to help open the black box, enabling consumers and the government to gain access to this corporate collected information. While each of these three approaches has potential risks and rewards, they can help frame the public debate on the ownership and use of geospatial data from self-driving cars.

- Autonomous cars rely on computerized systems to run. User access to this data proves difficult when they are locked in closed networks controlled by automobile manufacturers. The study looks at how legislation could help make this data more accessible. Car manufacturers typically consider themselves the sole arbiters of the information pertaining to their vehicles, claiming that they "own the data" but legislation has provided pushback and the author cites examples, such as debates around the right to repair.
- When autonomous cars, including their components, assembly, operation and data, are designed through an open source framework, data might be more easily available to the public and inform greater understanding about its potential uses and implications, the author suggests.

  Companies such as Udacity, an online education company, offers a Self-driving Car Engineer Nanodegree program in which students learn, develop and refine code for autonomous systems. Although there may be economic and intellectual property tradeoffs for the manufacturers, open source design plays an

important role in allowing for greater transparency, according to the study.

- In addition to legislation and open source design, hacking is both a systemic risk for autonomous vehicles and an approach that has been deployed to make car data and automated systems more transparent while holding self-driving car companies more accountable. In 2013 and 2015, two security experts remotely hacked into a 2014 Jeep Cherokee, and a Toyota Prius and Ford Escape, respectively, demonstrating the security flaws in vehicles that were not autonomous. Security vulnerabilities are likely to run much deeper with fully autonomous vehicles.

Precisely because hacking is a generalized risk for autonomous vehicles, certain instances of hacking in the context of research and advocacy have shown the importance of building secure systems. Recent security breaches with Equifax and Facebook illustrate the many security risks relating to consumers' digital information. "If we're going to adopt self-driving cars, then we should really make absolutely sure that they are as secure as they can be. This requires input from parties outside of the corporations who are building those very systems, such as government, advocacy groups and civil society at large." says Alvarez León.

In the U.S., Arizona, California and Michigan are currently some of the most hospitable states for self-driving vehicles, serving as testing areas for companies such as Waymo, which started as Google's Self-Driving Car Project. While there are local regulatory battles, and often pushback from citizens and advocacy groups, other states may open their doors to this new mode of transportation in the future. Two weeks ago, Waymo announced that it will be building a manufacturing facility in southeast Michigan, as it looks to grow its fleet. As the study points out, oversight of the self-driving car industry cannot be left to the manufacturers themselves. It is up to the public and government to help define how this

new technology and subsequent mapping of our communities will affect our society.

Provided by Dartmouth College