Driving While Monitored: Who Owns Your Data?

THE UNIVERSITY OF ALABAMA | Alabama Transportation Institute
Transportation Policy Research Center

Trayce Hockstad J.D., & Justin Fisher J.D., Legal Research Associates
Transportation Policy Research Center, Alabama Transportation Institute

Overview

Raw data, like that generated from vehicles, cannot be "owned" in the same legal sense as other types of intellectual property can be owned. Consequently, "ownership" of data generated from vehicles refers to the "rights or ability to access, assign, transfer, use, destroy, or exclude others from that data."[i] Because raw data cannot be owned in a traditional sense, a great deal of uncertainty surrounds the ownership of data generated from vehicles. In fact, a review of 13 selected automakers conducted by the U.S. Government Accountability Office (GAO) found that even automakers do not agree on who owns the data collected from their connected vehicles.[ii]

The GAO review found that 7 of 13 automakers believed the data ownership was legally unclear and that they do not have a position on who owns the data. Three of the 13 automakers believe the vehicle owner owns the data. Two automakers said the manufacturer owns the data, and one automaker said the automaker owns anonymized data and the customer owns personal data like the data that is tied to a vehicle identification number.[iii]

However, U.S. law is not entirely settled when it comes to the ownership of data generated from vehicles. Raw data ownership does not fall within one of the existing intellectual property regimes like patent, trademark, or copyright. But one possibility is for ownership over vehicle data to exist by controlling access to the data through software barriers.[iv] Most vehicle data is collected or transmitted by proprietary software, which is protected by copyright law, and a federal anti-circumvention provision prohibits the circumvention of a "technological measure that effectively controls access to a work protected under this title."[v] The proprietary software in the vehicle is "a work protected," and accessing the data without permission of the software would be an example of "circumvention."[vi] Therefore, even though copyright law does not protect the raw data itself, the data is covered by proprietary software, access to which is protected under copyright anti-circumvention rules.

With the void left by the lack of statutory law, vehicle data will likely be governed through contractual law principles like privacy policies and terms of use.[vii] Vehicle owners do not have ownership rights in the proprietary software in their vehicles, and they likely have to agree to the

---

[i] *See* Zhang, S. *Note: Who Owns the Data Generated by Your Smart Car?* 32 HARVARD JOURNAL OF LAW AND TECHNOLOGY 303,(Fall 2018).
[ii] GAO, *Vehicle Data Privacy: Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role*, GAO-17-656 (July 2017).
[iii] *Ibid*.
[iv] Zhang *supra* n. 1 at 306.
[v] 17 U.S.C. § 1201(a)(1)(A) (2018).
[vi] Zhang *supra* n. 1 at 306.
[vii] *Ibid* at 316.

manufacturer's terms of use, which typically prohibit users from circumventing or tampering with the vehicle's software.[viii]

Such terms of use might be enforceable as proven in the Eighth Circuit case, *Davidson & Associates v. Jung*.[ix] In that case, defendants reverse engineered a computer game software to create their own version of the game, but the court found that even if the reverse engineering would have been protected by fair use, the parties agreed to the game's terms of use which contracted away their right to fair use.[x] Since most vehicle software includes terms of use agreements that prohibit the circumvention of the vehicle's software, consumers within the jurisdiction of the Eight Circuit likely give up any right to access or use of the data they might otherwise have had by agreeing to the terms of use.[xi] However, other circuits have not settled the issue and could come to a different conclusion than the result in *Jung*.

Since the current intellectual property law regimes are not well suited to regulate the ownership of raw data, industry-specific legislation could prove to be a better option. However, data ownership is rarely addressed in statutes addressing connected and autonomous vehicles.[xii] Most legislative action surrounding autonomous vehicles has focused on safety rather than data ownership and privacy issues.[xiii] And while no federal law currently regulates vehicle data, the SELF DRIVE Act, a federal bill that passed the House of Representatives in 2017, included a provision that would have addressed data privacy and autonomous vehicle manufacturers.[xiv] The bill would have required autonomous vehicle manufactures to develop a privacy and notification policy that would allow consumers to know the type of data being collected and for what purpose.[xv] The bill would not have assigned any property interests in the data to the consumer and would have created an exception to the notification requirement for data that was anonymized.[xvi] There is also some concern that anonymized data can be de-anonymized, especially highly unique information like location.[xvii]

A similar bill, the AV START Act, was also introduced in the Senate in 2017. The bill would have created a committee that would make policy recommendations with respect to the data that autonomous vehicles collect, generate, record, or store.[xviii] That bill did not address the ownership of autonomous vehicle data either. The lack of restrictions on how vehicle data could be used in either bill could suggest that car manufacturers do have "ownership" of the data.[xix] However, neither bill became law. Furthermore, even if one of the bills was enacted, it would only apply to autonomous vehicles. Because vehicles can still generate and collect data without autonomous functions, a large portion of data generated by vehicles would still be unregulated.

[viii] *Ibid* at 307.
[ix] 422 F.3d 630 (8th Cir. 2005).
[x] Zhang, *supra* note 1 at 13.
[xi] *Ibid* at 308.
[xii] See *Autonomous Vehicles State Bill Tracking Database*, National Conference of State Legislatures (August 3, 2021), https://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx.
[xiii] Zhang *supra* n. 1 at 309.
[xiv] Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act, H.R. 3388, 115th Cong. (2017) (as introduced, July 25, 2017).
[xv] *Ibid.*
[xvi] *Ibid*.
[xvii] Editorial: *Privacy Risk in Self Driving Cars? Senate Has to Fix That Loophole in Federal Bill*, Mercury News (September 14, 2017), https://www.mercurynews.com/2017/09/14/editorial-privacy-risk-in-self-driving-cars-senate-has-to-fix-that-loophole-in-federal-bill/.
[xviii] American Vision for Safer Transportation through Advancement of Revolutionary Technologies Act, S. 1885, 115th Cong. (2017) (as introduced November 28, 2017).
[xix] Zhang *supra* n. 1 at 310.