AUTONOMOUS VEHICLE INFORMATION ACT (AVIA)

MATTHEW KALINOWSKI, KELLY QI, DANIEL ROSENZWEIG, GABRIELLE WHITEHALL

What are autonomous vehicles (AVs)?

AVs are systems that can perform various driving functions with or without human control.

AVs have the potential to reduce driving related accidents and increase safety on the road.

Companies such as Google and Tesla each have their different AV implementations, but all collect sensitive user data.

The AVIA aims to protect one's **Personally Identifiable Information (PII),** any data that is linkable to a specific individual, from unauthorized collection, sharing or use by the manufacturer. Additional data pertaining to the AV that does not fall under PII is defined as **Vehicle Performance Information (VPI).** The AVIA also describes security practices for PII and VPI.

What is at risk?

Hackers were able to remotely take control of a Jeep Cherokee's steering, speed, and other system functions. The vehicle's security could be compromised.

Tesla was able to completely reconstruct a reporter's journey without his knowledge through his vehicle data. Private information about people's whereabouts could be exposed.

Where Current Law Fails

There are no existing federal laws that apply to AV data privacy. The National Highway Traffic Safety Administration and various states have passed guidelines attempting to regulate AVs, but neither provides adequate protection for operator privacy from misuse of personal information.

Our Solution

PRIVACY

Manufacturers must obtain affirmative, express consent from the operator and disclose any intention of collecting, sharing, and using the operator's PII.

Manufacturers must provide operators with remote and on-board access to their own PII.

Manufacturers must only keep PII for the minimum time necessary, and delete any PII that is no longer needed.

The FTC shall have authority to enforce this act.

SECURITY

Manufacturers must use reasonable security safeguards to prevent unauthorized access to PII and VPI including:

- Maintaining up-to-date software
- Encryption of all data at rest and in-transit
- Adhering to standard authentication mechanisms

Manufacturers must promptly alert operators in the event of security breaches.

Manufactures may receive tax credit for implementing these practices.