Professional Perspective

Privacy Implications of Autonomous Vehicles

David Kessler and Alexis Wilpon, Norton Rose Fulbright

Bloomberg Law

Privacy Implications of Autonomous Vehicles

Contributed by David Kessler and Alexis Wilpon, Norton Rose Fulbright

Autonomous vehicles are a common way for third parties to collect personal information about users. In an increasingly connected world, the concept of mobility as a service where rental or ridesharing services enable users to book, use, and pay for transportation has taken off and varying levels of AVs are increasing in popularity.

AVs range from cars that have some level of automated assistance with steering, parking, or breaking, to fully self-driving vehicles. While AVs offer many benefits to consumers, the vehicles collect an enormous amount of personal information about passengers. Some of the information collected may be shared with third parties that use the data for secondary purposes. While no federal law directly addresses these concerns, several state laws apply to the types of personal information AVs collect.

This article examines personal data collection of ridesharing or rented AVs. It reviews personal data collection of different types of AVs, what passengers should be aware of, and legal considerations for AV operators.

Overview of AVs & Privacy

AV Overview

The U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) defines AVs as vehicles where "operation of the vehicle occurs without direct driver input to control the steering, acceleration, and braking and are designed so that the driver is not expected to constantly monitor the roadway while operating in self-driving mode." The phrase autonomous vehicle is not synonymous with a vehicle that is completely self-operational.

Most car manufacturers and operators have adopted the SAE International levels of driving automation. These are varying levels of automation that range from cars in which the human driver does all driving (Level 0), advanced driver systems that assist a human driver with steering and breaking (Level 1), to automated driving systems in which the vehicle does all driving and the human occupants are merely passengers who do not need to be involved in the vehicle's operation (Level 5).

Passengers may make use of AVs in several ways:

Individually Owned AVs. Although many vehicles on the market today already achieve some level of automation, it may be unlikely to see individually owned level 5 AVs for some time because self-driving technology could add an additional $20,000 to a vehicle's price. For example, the 2020 Hyundai Sonata, 2021 Audi A4, 2020 Volkswagen GTI, and 2020 Ford F-150 all include upgrade packages to allow for autonomous parking and breaking.

AV Ridesharing. AVs may be the fleet of the future for private companies. Uber or Lyft may enable users to order a ride through an app and a self-driving car could pick them up and drop them off at their preselected pick up and drop off points. Ridesharing AVs would operate at level 5, where the user is not responsible for any of the actual driving. According to Lyft, they have already operated over 100,000 self-driving rides.

Rent AVs. AVs may be rented from traditional rental services. Alternatively, users may request a ride from a traditional car rental service but the car would drive itself to the user's location to pick them up and they could rent the AV for a set period of time. Zipcar—a rental service that allows users to rent cars by the hour or day—envisions the onset of self-driving cars to usher in an era of mobility-as-a-service. Users would be picked up by a self-driving vehicle and dropped off in another location without the need to drop off the vehicle at a specific location.

Collecting Passenger Data

AVs collect an enormous amount of data for a variety of purposes. The purpose of the AV may determine the type of personal information collected and the parties with whom the personal information is shared.

Individually Owned AVs. Individually owned vehicles have the capacity to collect geolocation data, behavioral data, and information from a synced smart-device. However, this article focuses on information collected by vehicles in a rental and ridesharing capacity.

AV Ridesharing. AV fleets of the future will likely operate similarly to current ridesharing companies such as Uber or Lyft. The ridesharing service will need to collect the individual's pick up and drop off point and the specific route taken to the user's destination. If a user does sync their smart phone to the vehicle, their music preferences, contacts list, and information from other applications may be collected.

Rented AVs. AVs may include largely human-driven vehicles with some autonomous functions, such as steering assistance. AVs can be rented by traditional rental services wherein the user picks up the car from the rental company for a set number of hours or days. The rental service may collect personal information including: the number of miles driven, demographic details about passengers, location data if the car includes a GPS system, and behavior information.

All vehicle manufacturers after 1996 must have an On-Board Diagnostic port (OMB-II) to collect information for safety and diagnostic purposes. For example, ports may track if a user exceeds a speeding limit, slams on breaks, or drives in a prohibited area. Rental operators may use a dongle device to connect to the OMB-II to collect this information.

If users link a smart device to the entertainment system, their contacts list, music preferences, and other personal preferences may be collected. If a user orders a AV rental that picks them up, specific geolocation information will also be collected. To authenticate the user, self-driving rentals may require biometric data, such as a fingerprint or retinal scan to allow a user to unlock and access the vehicle.

Secondary Use

A large concern in the AV space is the secondary use of passenger data. Rental and ridesharing services may share information with third parties that use riders' personal information to target their products to users. For example, consider a user that rents an AV to drop them off at the airport once a month.

If the rental service shares that user's data with a third-party advertiser, the user may receive advertisements for airlines, hotels, or other travel-related services when they next enter the AV. Third parties may deliver advertisements through forced radio and pop-ups on the dashboard or rental application. Similarly, infotainment manufacturers may sell or share passenger data to third parties who use the information to target their products to consumers based on their interests and habits. The legal implications of selling or sharing passenger data are discussed in greater detail below.

Rental services may also share behavioral information with third parties. For example, according to a joint Workshop hosted by the FTC and the NHTSA, rental companies may share safety information and details about excess speed and other similar details with auto insurance companies, which may use the information to determine consumer rates.

Cybersecurity Concerns

AVs have more in common with sophisticated computers than they do with early cars. AVs are not immune from cyberattacks that could have drastic implications on operations and safety. A 2019 FBI-issued warning cautioned the auto industry that the data collected by AVs could become a cyberattack target. According to an AV chip manufacturer, AVs may have the equivalent of 200 laptops in its trunk. Potential implications range from a ridesharing app going offline causing significant downtime costs to an attacker gaining remote access and control of a vehicle, causing serious safety concerns.

U.S. Privacy Law & AVs

Existing U.S. federal privacy legislation is mostly inapplicable to AVs. However, several existing and proposed state laws directly apply to AVs.

CCPA

The California Consumer Privacy Act is the most extensive law protecting consumer privacy in the U.S. The CCPA governs the collection and handling California residents' personal information. Pursuant to CCPA, businesses—which may include AV rental or ride sharing services—must provide consumers certain rights regarding their personal information. These rights include the right to notice about:

- What data they collect
- The purpose of that collection

- With whom the data is shared or sold
- Right to access one's personal information
- Right to delete one's personal information
- Right to opt out of a sale of one's personal information
- Right to nondiscrimination

CCPA defines a sale of personal information as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." Cal. Civ. Code § 1798.140(t)(1).

Other valuable consideration is interpreted broadly but where a business has received any benefit in exchange for the transfer of personal information, a sale has likely occurred. In that instance, a business must update its privacy notice to notify consumers of the sale and include a link on its homepage titled "Do Not Sell My Personal Information" so consumers may opt out of the sale. Cal. Civ. Code § 1798.135(a)(1).

CCPA violations may result in a civil penalty up to $2,500 per violation (or $7,500 for every intentional violation). Cal. Civ. Code § 1798.155(b) To date, the California Attorney General has brought approximately 13 separate enforcement actions specifically related to violations of CCPA's sale provisions.

Finally, CCPA provides a private right of action to consumers whose personal information was subject to a data breach. Cal. Civ. Code § 1798.150(a)(1). Given the amount of personal information AVs collect, rental and ridesharing services must ensure they implement adequate safeguards to protect against cyberattacks that could result in significant costs related to downtime, breach response, and litigation.

CCPA & Rental or Ridesharing AVs

A rental or ridesharing service may provide information about users to a travel company, including users' drop off histories. In exchange, the travel company agrees to place advertisements for the rental or ridesharing service on its website. Even though the rental or ridesharing service does not receive monetary payment for the personal information, the advertisements constitute valuable consideration and so the service has sold the personal information under CCPA.

To ensure CCPA compliance, AV rental and ridesharing services should identify all third parties to whom the service provides user personal information, what precise personal information is provided to those third parties, and whether the service receives any monetary or other valuable consideration for the personal information.

If the service does engage in the sale of personal information, it must take steps to ensure CCPA compliance, including ensuring users receive adequate notice of:

- The sale of data in its online privacy policy
- The sale of data in its rental agreements
- The mechanisms users can use to effectuate opt outs

The service should include an opt out option in its rental agreement and an online mechanism to opt out after executing the initial rental agreement.

CPRA

The California Privacy Rights Act expands upon CCPA in several ways. CPRA introduced the concept of data sharing as transferring "a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration." Cal. Civ. Code § 1798.140(ah)(1). When businesses share data, CPRA grants consumers the right to opt out of sharing information for cross-context behavioral advertising purposes. Cal. Civ. Code §1798.135(a). Businesses must inform consumers of the right by posting a clear and conspicuous link on its internet homepage titled "Do Not Sell or Share My Personal Information."

Additionally, CPRA created a new category of sensitive personal information, which is defined as personal information that:

- Reveals a consumer's government-issued identification number, financial account information and account login credentials, precise geolocation information, the contents of emails or text messages, genetic data, racial or ethnic origin, religious beliefs, biometrics, health data, and data concerning sex life or sexual orientation
- Is used for the purpose of inferring characteristics about a consumer

CPRA grants consumers the right to limit the use and disclosure of their sensitive information to certain "business purposes." Cal. Civ. Code § 1798.121(a). Where businesses use or disclose sensitive information for reasons other than enumerated business purposes, the business must include a clear and conspicuous link on its homepage and within its rental agreements titled "Limit the Use of My Sensitive Personal Information." Cal. Civ. Code § 1798.135(a)(2).

CPRA created the California Privacy Protection Agency to oversee enforcement, which may include civil penalties of up to $2,500 per violation or $7,500 per intentional violation. CPRA also includes a private right of action for consumers whose personal information was subject to a data breach.

CPRA & Rental or Ridesharing AVs

AVs collect sensitive information, including geolocation data and information based on user habits. For example, drop offs at a psychiatrist office, place of worship, or gay bars reveal information categorized as sensitive under CPRA. Therefore, rental and ride sharing services may need to create a mechanism for limiting the use of this information.

An AV rental services that provides passenger data to a third-party targeting ads to the passenger, is an example of sharing under CPRA. Whenever a rental or ride sharing service provides information to third parties that reaches conclusions about users, including those based on locations traveled to, music listened to, how fast they drive, etc., they must ensure they comply with the notice and opt out requirements.

To ensure CPRA compliance, AV rental and ridesharing services should identify:

- Whether they share any personal information
- The parties with whom it is shared

Services must ensure adequate notice in its online privacy policy and rental agreements that the service:

- Shares personal information
- Whether it shares sensitive personal information
- Create mechanisms to opt out of disclosure or use of sensitive personal information

Like with CCPA, these mechanisms should be included both in the initial rental agreement, and online so that the service can track any future opt outs. Rental and ridesharing services should ensure adequate safeguards are implemented to avoid data breaches and any subsequent litigation.

Biometrics Laws

Some states have enacted laws specifically governing biometric data. The Illinois Biometric Information Privacy Act (BIPA) was the first law to do so and requires companies collecting biometric information to inform consumers prior to collection and obtain written consent. 740 Ill. Comp. Stat. 14/15. BIPA expressly prohibits companies from selling biometric information and requires consent from the consumer to disclose a person's biometric information.

BIPA includes a private right of action for any consumer whose biometric information was processed in violation of the act and fines of up to $1,000 (or $5,000 for intentional or reckless violations) or actual damages, whichever is greater. Texas and Washington also enacted biometric privacy legislation that includes notice and consent requirements.

These laws may come into play in the AV context. For example, imagine a consumer orders a rental or rideshare through an AV that drives itself to the consumer's designated pick-up location. Ridesharing and rental services must ensure that the individual entering the car is the individual that ordered the ride. Rental and ride sharing services may prefer biometric

information—such as a fingerprint or retinal scan—to verify the identity of the individual over information that may be shared with a third party—such as a key card or passcode.

While relying on biometric information may be the best way for rental and ridesharing services to verify the identity of the individuals using their vehicles, they must ensure their rental agreements include adequate notice of the collection and that the user signs a clear and conspicuous consent form. If services sell biometric information without necessary notice and consent, they may face steep fines and costly litigation.

Other Applicable State Laws

Following the passage of CCPA, other states enacted or proposed comprehensive privacy laws governing the collection and handling of personal information. This would include the personal information collected from AV passengers.

For example, Nevada passed SB-220, which includes a similar opt out of sale right to CCPA. Nev. Rev. Stat. § 603A.340. Virginia's Consumer Data Protection Act enables consumers to opt out of sales of personal information but defines a "sale" as an "exchange of personal data for monetary consideration." Va. Code § 59.1-575(A)(5). Finally, Colorado passed the Colorado Privacy Act (CPA), which includes an opt out of sale right as well. Colo. Rev. Stat. § 6-1-1306 Like CPRA, CPA also includes a special category of sensitive personal information. New Hampshire and Washington have also proposed comprehensive privacy laws

California passed a law specific to AVs that requires manufacturers to either:

- Provide written disclosures to the passengers of a vehicle that describe the personal information collected by the AVs that is not necessary for the safe operation of the vehicle and describe how that information is used or
- Anonymize that information. Cal. Code Regs. tit. 13, § 228.24.

Other states have proposed or enacted legislation addressing privacy concerns related to AVs. For example, Massachusetts' proposed bill would require the Massachusetts Department of Transportation to protect the privacy of individuals including operators and passengers of AVs. H.B. 3031, 191st Sess. (Mass. 2020). Michigan law requires AV manufacturers to make publicly available a privacy statement disclosing its data handling practices in connection with the applicable participating fleet. Mich. Comp. Laws § 257.665b.

Thirty-six states and the District of Columbia passed legislation or issued an executive order directly relating to AVs. However, these laws focus on testing, development, and passenger and pedestrian safety over privacy.

State Breach Notification Laws

All 50 states, the District of Columbia, and Puerto Rico have enacted state personal information breach notification laws that govern when notice must be provided to individuals and regulators. Importantly, these laws apply to the residency of the individual, not where a specific car is driven. In the case of a cyberattack, AV services must be able to identify their obligations to provide notice under these laws.

Conclusion & Takeaways

AVs collect and share a large amount of personal information from users. Rental and ridesharing services must be aware of their obligations under privacy laws and how to safeguard the data from a potential cyberattack. Recommendations for safeguarding are as follows:

Analyze Applicable Laws. Currently, there are no federal laws on point, but stakeholders should evaluate which state privacy laws may apply to them and ensure compliance. Stakeholder evaluations will entail updating privacy notices, reviewing data transfers, and creating mechanisms for effectuating data subject rights.

Review of Data Sharing Practices & Policies. Services should review all transfers of personal information to determine whether a sale or share has occurred under CCPA and CPRA. If so, manufacturers must confirm they have adequate notice and opt out mechanisms for such sales or shares.

Privacy by Design. The AV industry should recognize the importance of privacy by design—incorporating privacy considerations from the first stage of development—to safeguard personal information and avoid potentially catastrophic

safety implications that could follow a cyberattack. Many of the industry's leading players have invested millions of dollars in cybersecurity firms to mitigate potential threats.

Information Sharing. Stakeholders should be encouraged to share intelligence across the industry to facilitate cooperation and implementation of lessons learned. Potential organizations that could share information include the Auto-ISAC, the International Organization for Standardization, and the Society of Automotive Engineers. The FTC has recognized and encouraged the need for such information sharing.