

DASHCAMS

Privacy Considerations & Best Practices

Some drivers use dashcams in an effort to increase their safety, security, and peace of mind; as a result, dashcams are becoming increasingly common in vehicles. Dashcams often record video and audio continuously while the driver is using the vehicle, and some dashcams wake up from hibernation while the car is parked and record the vehicle's environment in response to activity near the car. Dashcams raise privacy concerns for passengers and pedestrians, and the laws about their use are not straightforward.

This resource provides privacy guidance for drivers who use dashcams to record inside or outside of their vehicles while offering rides as part of an app-based rideshare or ride-hail service. This resource primarily focuses on dashcams, but drivers may use other technology for similar purposes, such as recording apps or functions on their smartphones.

1 • Overview of Dashcams



A **dashboard camera** or **dashcam** is a video camera mounted on the dashboard or windshield of a vehicle that records the road in front of the vehicle. There are also inward-facing dashcams, which record inside the vehicle's cabin, and dual-facing cameras that record both inside and outside.

Drivers often use dashcams to capture unexpected incidents like crashes. These recordings can be used as video evidence in insurance or criminal claims. For drivers who use their vehicles for ride-hailing or other commercial purposes, dashcams can also help promote accountability if incidents occur with passengers inside the vehicle.

However, dashcams often include a range of features and capabilities that can raise privacy and security concerns.

Drivers should be knowledgeable about how recordings will be stored, as well as be able to configure the settings to maximize privacy and security.

DASHCAM ADVANCED FEATURES

- › **360° Surround View**
Some dashcams provide a 360° view around the vehicle. These multi-camera systems may be placed on various parts of the vehicle and stitch feeds together to generate a complete view around the vehicle.
- › **Parking Mode**
Dashcams with this feature go into hibernation when the vehicle is parked. They 'wake up' upon detecting motion or sensing an impact and begin recording. Some models can notify the owner of the dashcam about an incident and share footage in real-time.
- › **GPS and Telematics**
Dashcams with GPS and telematics can record the vehicle's speed, location, and driving behavior (e.g., sudden acceleration or hard braking). Certain driving events can trigger videos to be shared with a third party (e.g., the admin for the dashcam or an insurance company).
- › **Infrared LED Lights**
Infrared lights provide dashcams with night vision, enabling recording in poorly lit conditions, as well as total darkness.
- › **Computer Vision (AI dashcams)**
Some dashcams use computer vision to help the vehicle detect potential risks on the road, road signs, and high-risk driver behavior, such as fatigue, distraction, or intoxication.

2 • Legal Protections & Considerations

Depending on whether the video or audio is being recorded without consent and where the recording takes place, wiretap laws, privacy laws, or civil rights laws may not permit audio recording, may provide individuals with rights, and may place obligations on those collecting, using, or sharing recordings.

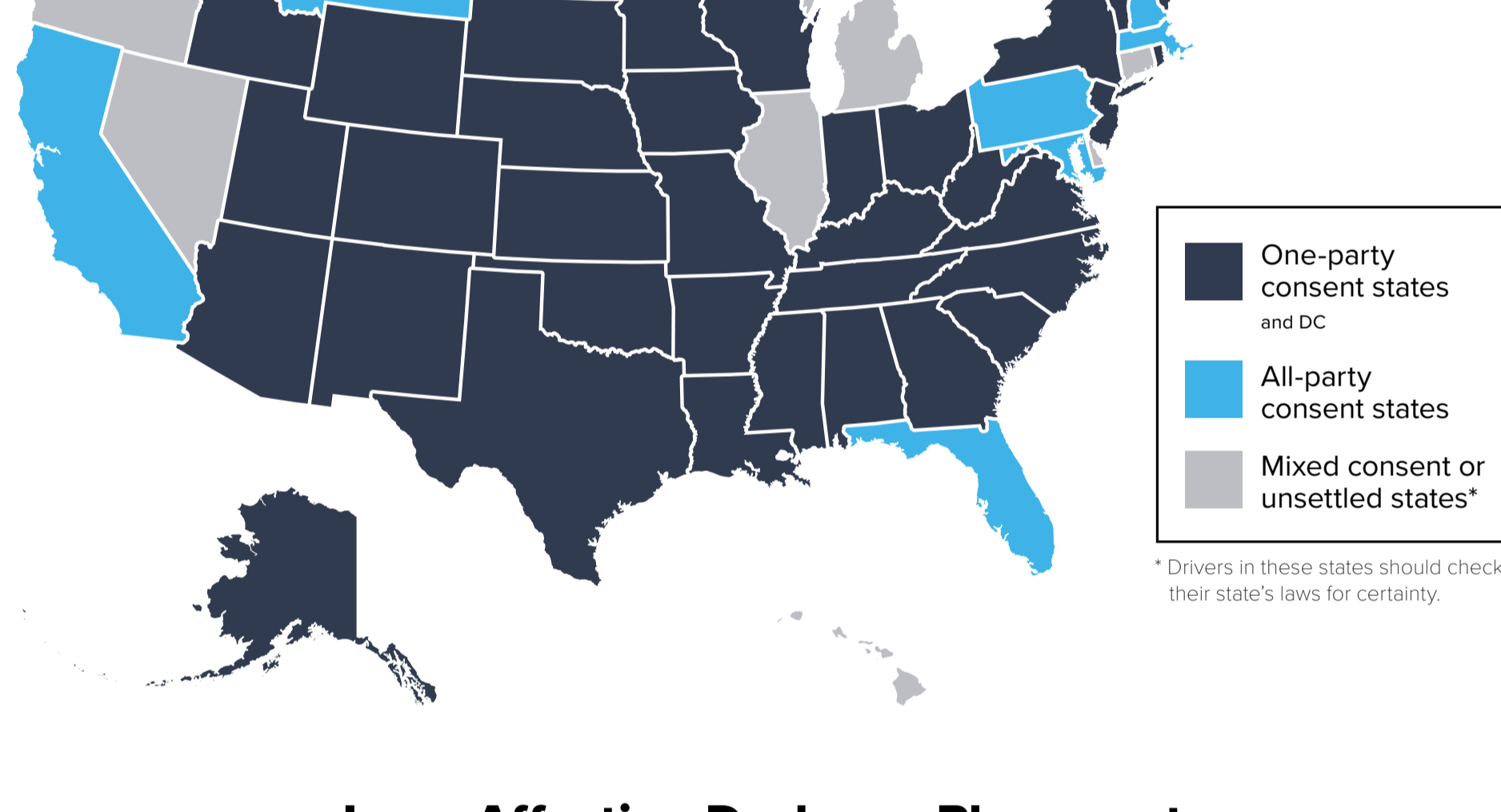
US Federal Audio Recording Laws

Federal laws generally protect the privacy of phone calls and conversations in the United States and require the consent of at least one of the parties involved to record (i.e., one-party consent). Federal laws establish the minimum privacy protections for all wire, oral or electronic communications. States may impose stricter requirements. These laws typically apply to audio recorded by dashcams.

US State Audio Recording Laws

The legality of recording audio and conversations differs from state to state and can also depend on the context. For example, some states may have both one-party and all-party consent laws depending on whether the law is criminal or civil and whether the conversation is in-person or on the telephone. Drivers should also check their state's laws regarding admissibility of recordings in civil cases.

- › **One-party consent states.** One-party consent laws permit the recording of conversations with the consent of at least one of the parties, which may come from the person recording if they are part of the conversation.
- › **All-party consent states.** All-party consent laws require that all parties to a conversation consent to the recording of the conversation.
- › **Mixed consent or unsettled states.** Some states are considered "mixed" or "unsettled" because the law's interpretation is in flux, when a wiretapping law conflicts with privacy law, or when the requirement for consent depends on the facts. Drivers in these states should check their state's laws for more detailed guidance and clarity.



Laws Affecting Dashcam Placement

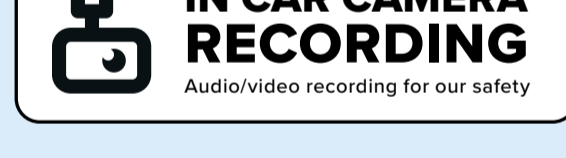
State and federal laws may restrict where drivers can mount dashcams. Under many of these laws, drivers can comply by placing their dashcams in places that do not obstruct their field of vision while staying in clear sight of passengers.

3 • Privacy & Security Best Practices

Because the legal requirements are not the same across the United States, drivers should follow these privacy and security best practices.

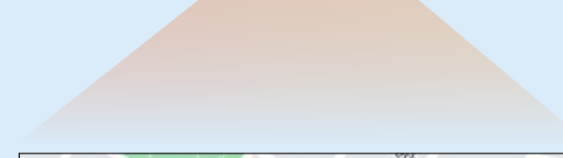
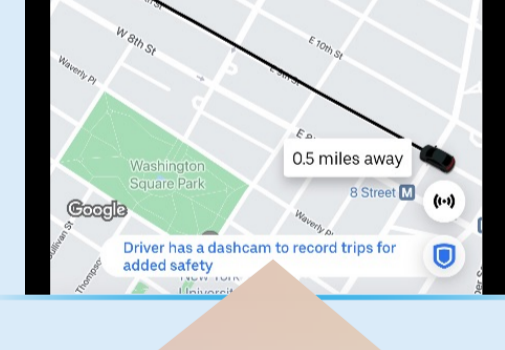
BEST PRACTICE #1: BE TRANSPARENT

Drivers should be transparent about their use of dashcams by providing prominent and effective notice. The notice should also include the reason(s) for recording.



In practice, drivers should

- › put recording notices both inside and outside the vehicle (e.g., a sign that indicates that there will be video and audio recording inside the vehicle).
- › mount the dashcam in a place that is clearly visible to passengers.
- › consider whether, in some situations, an oral notification may be appropriate (e.g., telling a passenger about the dashcam recording when they get in the car).
- › check into whether the ride-hailing app they are using has proactive notification features available. For example, Uber allows drivers to register a dashcam in the settings of the Uber app. When the dashcam is registered, this triggers a notification to each of their riders to let them know that their trip may be recorded.



BEST PRACTICE #2: LIMIT USE & SHARING

Drivers should only watch, listen to, and share recordings when there is an incident that necessitates review (e.g., to support an insurance claim).



In practice, drivers should

- › only share video and audio recordings with others, such as an insurance company or the ride-hail company's dedicated safety team, for reasons that align with the reason(s) for recording.
- › review the ride-hail company's community guidelines and data use policy if using an app-based rideshare service. For example, rideshare companies often prohibit streaming or sharing recordings on social media or using a passenger's personal data for any reason other than for the purposes of fulfilling safety and security purposes.
- › be familiar with the ride-hail company's dashcam registration process and how to submit recordings to the company's support teams.

BEST PRACTICE #3: KEEP AUDIO & VIDEO FOR SPECIFIC & REASONABLE PURPOSES

Drivers should only record video and audio for specific and reasonable purposes (e.g., driver and passenger safety or to support or dispute insurance or criminal claims). Recordings should be promptly deleted when no longer needed to fulfill the reason(s) for the recording.



In practice, drivers should

- › configure their dashcam to record on a loop or to automatically delete videos after a certain amount of time, for example, every 4–6 weeks.
- › not keep recordings indefinitely or for reasons not aligned with the safety and security reasons for using a dashcam. For example, it is reasonable to keep recordings for as long as is necessary to support or dispute insurance or criminal claims from a crash, an altercation with a passenger, or a clean-up fee dispute. It is not reasonable to keep recordings of passengers for personal reasons, such as reviewing recordings for enjoyment, reviewing recordings to identify a passenger for personal reasons, or for sharing on social media.
- › understand how long the ride-hail company will keep recordings once they are shared.

BEST PRACTICE #4: USE STRICT ACCESS CONTROLS & SECURITY

Drivers should protect video and audio recordings through appropriate safeguards. These safeguards include scheduling times to delete unused footage and ensuring dashcam footage is encrypted to prevent unauthorized access during the transmission and storage of the data.



In practice, drivers should

- › read dashcam consumer guides with an eye for privacy-protecting features. For example, some privacy-protective features include face blurring, automatic deletion of recordings on a set schedule, and default password reset prompts.
- › purchase and use dashcams with strong privacy and security settings for the device and a robust privacy policy that provides clear information on how video and audio recordings are protected. Some features, such as wi-fi connectivity that allows recordings to be uploaded to the cloud, may provide benefits such as conveniently storing and sharing recordings. These features often create responsibilities for the driver to ensure the recordings are kept secure.