The legality of recording audio and conversations differs from state to state and can also depend on the context. Some states are considered “one-party” consent states, where only one of the parties involved needs to consent to the recording (i.e., one-party consent). Other states require all parties to a conversation to consent to the recording of the audio or conversation (i.e., all-party consent). Some states are considered “mixed” or “unsettled” because the law’s interpretation is unclear or may depend on the facts. In practice, drivers should be familiar with their state’s laws regarding admissibility of recordings in civil cases, as well as any local or municipal laws that may apply.

Drivers should be transparent about their use of dashcams, and ensure that recordings are kept secure. Drivers should only watch, listen to, and share recordings for specific and reasonable purposes (e.g., driver and passenger safety, reviewing recordings to identify a high-risk driver behavior, or when the requirement for consent depends on the facts). Recordings should be promptly deleted when no longer needed to fulfill the specific and reasonable purpose for which the recording was made.

US State Audio Recording Laws

Drivers in these states should check their state’s laws for more detailed guidance and clarity. Some states may have both one-party and all-party consent laws depending on the context. In general, drivers should follow the local laws that apply to the recording of audio conversations in their state.

Drivers should be knowledgeable about how recordings may be used, shared, or stored. They should only record video and audio for the purposes of fulfilling safety and security purposes. Drivers should not keep recordings indefinitely or for reasons not aligned with the specific and reasonable purposes for which the recording was made. Drivers should review the ride-hail company’s community guidelines and data use policy if using an app-based rideshare service. For example, a driver should review the Uber Terms of Use or Privacy Policy, and any additional terms or policies in Ride-Hailing Apps’ Terms of Service or Privacy Policy, to ensure they understand any restrictions or requirements for recording and sharing of data.

Drivers who use dashcams in their vehicles for ride-hailing or other commercial purposes should follow these privacy and security best practices:

**BEST PRACTICE #1: BE TRANSPARENT**

Drivers should only record video and audio for specific and reasonable purposes, and ensure that recordings are kept secure. They should 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 driver app. They should put recording notices both inside and outside of their vehicles, and ensure that they are clearly visible to passengers. They should also check if they need to register their dashcam with the company or if they need to share the recordings with an insurance company.

**BEST PRACTICE #2: USE STRICT ACCESS CONTROLS & SECURITY**

Drivers should be transparent about their use of dashcams, and ensure that recordings are kept secure. They should use a dashcam that can record both video and audio, and ensure that recordings are encrypted to ensure they are kept secure. They should also put recording notices both inside and outside of their vehicles, and ensure that they are clearly visible to passengers. They should also check if they need to register their dashcam with the company or if they need to share the recordings with an insurance company.

**BEST PRACTICE #3: KEEP AUDIO & VIDEO RECORDINGS FOR OUR SAFETY**

Drivers should use dashcam footage to help protect themselves when driving, such as when reporting incidents with passengers inside the vehicle. They should use dashcam footage to support or dispute insurance claims. They should also use dashcam footage to help protect themselves when driving, such as when reporting incidents with passengers inside the vehicle. They should use dashcam footage to support or dispute insurance claims.

Dashcams with GPS and telematics can record the vehicle’s speed, acceleration, and other data that may help provide context for the recording.

**BEST PRACTICE #4: ATTEND TO THE WATERMARKING & BLURRING FEATURES**

Dashcams can be used to help address privacy concerns by using computer vision (AI dashcams) or infrared LED lights. Some dashcams use computer vision to record and stitch together various parts of the vehicle. Some dashcams also include features such as face blurring, automatic deletion of recordings after a certain amount of time, and default password reset prompts. Some dashcams enable recording during night or low-light conditions using infrared LED lights.

Drivers should be transparent about their use of dashcams, and ensure that recordings are kept secure. They should also 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 driver app. They should put recording notices both inside and outside of their vehicles, and ensure that they are clearly visible to passengers. They should also check if they need to register their dashcam with the company or if they need to share the recordings with an insurance company.