



Andrew T. Haling

PATHWAY LAW FIRM

Telematics, AI, and the new driver-data frontier

PRODUCING A MACHINE-GENERATED RECORD OF THE EMPLOYER'S KNOWLEDGE OF THE DRIVER AND THE DECISIONS THE COMPANY MADE

Many commercial vehicles – and even personal vehicles – on a California road today are rolling data recorders. Not in the way the EDR conversation has framed it for the last 20 or so years – a few seconds of pre-crash speed and brake application when “events” are triggered – but in a continuous, machine-interpreted way. Telematics is an integration between vehicles and a central system via a wireless network that reports information such as GPS coordinates, speed, and other vehicle data.

Telematics can capture vehicle position several times a minute, log every hard brake and hard acceleration, capture inward- and outward-facing video, and increasingly run computer-vision models that flag distracted driving, following too close, rolling stops, and seatbelt violations in something close to real time. Those alerts can go to a fleet-safety manager who decides whether to coach the driver, retrain him, discipline him, or do nothing. Additionally, some insurance companies are offering telematics through their cell phone application in exchange for reduced rates.

There is also the Video Event Data Recorder (VEDR), which employs dual-facing cameras that capture the road ahead as well as the driver. Do not be surprised if defense only turns over the dash-cam footage but excludes production of the driver-facing video.

This telematics data is a valuable evidence source not only for the subject crash, but can transform what a plaintiff can prove about the employer's knowledge of the driver. The pre-telematics negligent hiring claim was often pinned on what the employer should have known or did know by exploring personnel files or complaint history. That reasoning can now be strengthened with telematics

data showing the employer did know, or had the tools to know, about a driver's behavior.

The technology landscape

A handful of vendors are popular in commercial-fleet telematics. Geotab supports more than four million connected vehicles, and offers driver tracking and AI-powered dash cams. Samsara is a major competitor and is used by over 500,000 vehicles. Lytx – known for years by its DriveCam product – was a pioneer in the field with a stated goal of achieving a “flight recorder” for vehicles to identify root causes of crashes. Motive, formerly KeepTruckin, grew with the federal electronic logging device (ELD) mandate and now offers a safety tracking platform. Verizon Connect is strong in light-commercial and service fleets. PowerFleet has moved up rapidly after acquisitions and mergers.

There are dozens of smaller vendors and resellers, but these are the names that show up most often. Many of these companies offer both telematics and VEDR, and actively advertise their ability to track and identify unsafe driving and encouraging companies to develop and use key performance indicators (KPI) related to safe driving performance.

What these systems capture is broadly similar across vendors. The GPS layer reports position, speed, and heading at high frequency – often every few seconds while the vehicle is moving, configurable by the fleet customer. The accelerometer layer detects and timestamps hard-braking, hard-acceleration, hard-cornering, and impact events. Most modern installations include a forward-facing dashcam, and an increasing share include an inward-facing camera trained on the driver that can constitute part of the

VEDR system.

Be sure to always ask not just for dash cams, but for inward-facing camera footage. Cameras run continuously, but typically retain only video that is event-triggered or manually flagged. The platforms also pull data directly from the vehicle's J1939 or OBD-II bus (the digital systems vehicles use to monitor vehicle mechanics; essentially the computer in your car): engine RPM, throttle position, brake application, seatbelt status, and, on heavy trucks, the hours-of-service logs that satisfy the federal Electronic Logging Device (“ELD”) mandate. On top of the raw data, there can be a driver scorecard – a vendor-calculated safety rating.

Insurance usage-based products – Progressive Snapshot, State Farm Drive Safe & Save, Allstate Drivewise – collect a thinner version of the same telemetry on private vehicles enrolled in those programs. Original-equipment-manufacturer telematics – Tesla, Ford, GM's OnStar, and the Stellantis and Toyota equivalents – collect proprietary data streams of varying depth that are often discoverable through the manufacturer rather than the driver. Rideshare platforms maintain their own location and trip logs.

What data actually exists – and how long

The data falls into four buckets, and they have very different lifespans.

Real-time telemetry – the near-continuous stream of GPS, speed, accelerometer, and engine-bus data – may upload to the vendor's cloud and be retained according to the fleet customer's contract. Most major platforms allow customers to choose retention periods. The default a particular fleet has selected can be a discoverable fact, and counsel should ask

for it specifically. Additionally, counsel should use discovery to find policies on data retention when there is a notification of an accident, and the persons responsible (if any) in reviewing data and ensuring it is saved.

Event-triggered video is the most fragile and most consequential. Modern dashcams record continuously to local device storage but, by design, only upload short clips to the cloud when an event triggers them – a hard brake, a hard cornering, an AI-detected behavior, or a manual save. The locally stored video that wasn't triggered is overwritten on a first-in-first-out basis as new driving generates new footage. The overwrite window for a busy commercial vehicle can be a matter of days to a few weeks depending on storage capacity and operating hours. The clock is running from the moment of the crash, and unless someone manually preserves footage from the device, it is gone. Some systems automatically save video to the cloud when triggers occur.

AI safety alerts – the machine-generated flags for distracted driving, following too close, no-seatbelt, and so on – are typically stored as event records in the cloud regardless of whether the underlying video survives. The alerts and the human review of those alerts – who reviewed it, when, what they did about it – typically persist longer than the video itself. This metadata can be more valuable to a plaintiff than the video in relation to proving an employer should have known about unsafe driving behavior long before the subject crash. Find out who receives the AI safety alerts at the company and depose that person.

Driver scorecards and coaching records – the historical safety rating of the driver and the documented coaching sessions – typically persist for the duration of the employment relationship. So do dispatch records, electronic logs, and hours-of-service data, which under federal regulations must be retained

for six months for drivers subject to the regulations. (49 C.F.R. § 395.8(k).) Use wide-ranging vocabulary for the scorecards, such as KPIs, to avoid gamesmanship in the responses.

The practical takeaway: In the first week after a serious crash, video is the highest-priority preservation target. Telemetry, alerts, and coaching records typically have longer retention windows, but still need to be locked down before retention defaults expire or routine deletions kick in. Preservation letters should be updated to include the modern electronic data that can be collected by telematics and VEDR.

Getting it: California discovery practice

Preservation has to happen immediately upon signing up a case. Send a preservation letter to the motor carrier, employer, and insurance company on the day of intake. Work fast to identify potential telematics vendors. Send a separate preservation letter directly to the telematics vendor when the platform is identified. The preservation demand should specify: (1) raw telemetry data – GPS, speed, accelerometer, and engine-bus output – for the subject vehicle for a defined window before and after the incident; (2) all video and image data within a defined window that was captured by the vehicle's dashcam, including footage that has not been event-triggered or uploaded to the cloud; (3) all event records, including AI-generated safety alerts, regardless of severity score; (4) all coaching and review records associated with the driver; and (5) the driver's complete driving behavior and scorecard history. Reference the spoliation framework – Code of Civil Procedure section 2023.030 sanctions and the adverse inference under Evidence Code section 413 – and put the recipient on notice that destruction or routine overwrite of the listed categories will support sanctions. (See CACI Nos. 204, 205.)

The duty to preserve evidence can

arise when a party is objectively aware that the evidence would be relevant to anticipated future litigation, including litigation that is reasonably foreseeable. (*Victor Valley Union High Sch. Dist. v. Superior Court* (2023) 91 Cal.App.5th 1121, 1143–1149.) *Williams v. Russ* remains the touchstone authority for terminating sanctions when that duty is intentionally violated. (*Williams v. Russ* (2008) 167 Cal. App.4th 1215, 1223.)

When facts on the ground demand it, consider an injunction in aid of discovery requiring the carrier and vendor to preserve specified categories of data pending litigation. (*Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2003) 105 Cal.App.4th 1414, 1419.) This is rarely necessary if the preservation letters are timely and specific, but it is a powerful backstop where a defendant has signaled it intends to let data lapse.

Once suit is filed, party discovery should be tightly scoped to the platform. Document demands under Code of Civil Procedure section 2031.010 et seq. should request data in native format, not PDF screenshots of dashboards. Native production preserves the timestamps, metadata, and event flags that are the actual evidence; a PDF report of a Samsara dashboard is heavily summarized and often omits the AI-alert layer entirely. A PDF or screen shots could “scrub” key metadata. Special interrogatories under section 2030.010 et seq. should identify the telematics vendor, the account administrator, the configured data retention settings, and every person who reviewed any safety event for the subject driver in the 12 months before the loss. Requests for admission can lock down whether AI-generated alerts were issued for that driver, when, and what was done with them.

Person-most-knowledgeable depositions under section 2025.230 can do the heavy lifting as the written responses often will unsurprisingly be evasive. Notice two, or more, separate PMK depositions:

one on telematics systems, configuration, and retention; another on the carrier's safety, coaching, and disciplinary program. There are often different witnesses who are responsible for different aspects of safety and telematics, and if so, question the witnesses about the collaboration between the two (which is often lacking).

Third-party discovery on the vendor is the backstop when the carrier produces selectively, claims data was not saved, or claims data did not exist. Be on guard for when video turned over in written discovery is not all the camera angles (such as the inward camera angle is missing). Business records subpoenas under section 2020.410 reach Samsara, Lytx, Motive, Geotab, and the others directly. Vendors can have the raw data regardless of whether the carrier has chosen to retain it on the dashboard, and they are accustomed to responding to subpoenas in litigation.

When data is destroyed despite a preservation demand, Evidence Code section 413 permits the trier of fact to draw an adverse inference from the suppression of evidence. Code of Civil Procedure section 2023.030 authorizes monetary, issue, evidence, and terminating sanctions for misuse of the discovery process. California courts have recently described spoliation as a serious form of discovery abuse, confirming that the trial court has broad discretion to fashion an appropriate sanction. (*Victor Valley Union High Sch. Dist. v. Superior Court*, *supra*, 91 Cal.App.5th at p. 1139.) California courts evaluate prejudice from spoliation by examining whether the lost evidence would have been favorable to the moving party. (*Id.* at pp. 1140–1142.)

Defense counsel will likely respond to a spoliation claim over routine overwrite by pointing to the ESI safe harbor in Code of Civil Procedure section 2023.030, subdivision (f)(1), which bars sanctions for ESI lost through the routine, good-faith operation of an electronic information system. (See also Code

Civ. Proc., § 2031.300, subd. (d)(1).) That defense fails when the duty to preserve has already attached. (*Victor Valley Union High Sch. Dist. v. Superior Court*, *supra*, 91 Cal.App.5th at p. 1142.) Your preservation letter, sent as close to the day of the incident as possible, is what can flip the safe-harbor analysis. Use written discovery to prove receipt of the letter of preservation.

Using telematics to expand liability

Diaz v. Carcamo (2011) 51 Cal.4th 1148, has been the defense's favorite tool for shutting down direct-liability claims against the employer of a driver. *Diaz* holds that when a defendant employer admits vicarious liability for an employee-driver's negligence, claims for negligent entrustment, hiring, retention, and supervision become irrelevant and cannot be tried to a jury. (*Id.* at p. 1161.)

The practical effect has been defense attempting to keep the worst evidence about the employer – its safety culture, its discipline practices, its history of letting bad drivers stay on the road – away from the jury.

Six years later, the Court of Appeal in *CRST, Inc. v. Superior Court* (2017) 11 Cal.App.5th 1255, carved out the exception that defines plaintiff strategy in this area. *CRST* holds that an employer's admission of vicarious liability does not bar recovery of punitive damages, and that in punitive-damages cases neither the allegations of employer misconduct nor the evidence supporting those allegations are superfluous. (*Id.* at p. 1264.) When a viable punitive-damages claim is on the table, all of the *Diaz*-suppressed evidence about the employer's conduct comes back into play.

The gatekeeper for *CRST* is Civil Code section 3294, subdivision (b). That subdivision permits punitive damages against a corporate employer only when the malice or conscious disregard is on the part of an officer, director, or managing agent of the corporation. A managing agent is an employee who ex-

ercises substantial independent authority and judgment such that the employee's decisions ultimately determine corporate policy. (*White v. Ultramar, Inc.* (1999) 21 Cal.4th 563, 566–567.) A fleet-safety manager who reviewed alerts on a single driver may not be enough – *CRST* itself granted summary adjudication for the employer on exactly that point.

Telematics evidence is what can get a plaintiff past that hurdle in the cases where it can be cleared. A fleet's AI-driven safety platform is likely not the work of a single supervisor; it is corporate infrastructure, configured and operated according to corporate policy. Companies embracing AI to take over key public safety issues are likely administering decisions made upstream by top persons at a company. The retention settings, the alert thresholds, the coaching protocols, and – most importantly – the corporate policy on what to do with high-severity AI alerts are decisions that “ultimately determine corporate policy” within the meaning of *White v. Ultramar*. When a plaintiff can show that the carrier's system generated repeated severe alerts about a driver and that the carrier's policy was to clear them without coaching or discipline, the showing could reach the corporate-policy level by definition.

The pattern that supports a punitive-damages claim looks like this: The AI dashcam flagged the driver for distracted driving, following too close, or rolling stops on multiple occasions over a meaningful window before the crash; the safety scorecard showed the driver in the bottom; coaching records show the alerts were ignored or reviewed and dismissed without follow-up; and the same pattern is documented across other drivers in the fleet, suggesting an institutional approach rather than one supervisor's lapse. (See *Pfeifer v. John Crane, Inc.* (2013) 220 Cal.App.4th 1270, 1299; *West v. Johnson & Johnson Prods., Inc.* (1985) 174 Cal.App.3d 831, 867 [conscious disregard inferable from awareness of

probable dangerous consequences and deliberate failure to avoid them]; *cf. Butte Fire Cases* (2018) 24 Cal.App.5th 1150, 1176 [evidence of properly enforced corporate safety programs negates malice – implying that documented failure to enforce them supports it].) It is very likely that many cases will develop a common theme; a company purchases AI telematics for safety; the warning signs existed, but the follow-through of using the data to improve safety is missing.

This reframes why a plaintiff should pursue telematics evidence even when respondeat superior is admitted. The *Diaz* admission may resolve compensatory liability, but it does not resolve punitive exposure, and under *CRST* the negligent-entrustment claim can survive alongside a viable punitive-damages claim. The telematics record can be critical documentary evidence that turns “should have known” into “knew, in writing, with timestamps, and decided to do nothing.” A singular crash can unlock a dangerous pattern of putting the public in danger – very compelling evidence for the jury to consider.

The AI accelerator

The technology described in this article is not a future-state – it’s here. Geotab, Samsara, Lytx’s MV+AI, and other vendors all advertise on their websites the robust tracking systems and ability to monitor a wide variety of risk factors in driver behavior. The entire chain – from

machine inference to human decision – can be timestamped and stored.

Before AI dashcams, “the carrier should have known the driver was unsafe” was an inference a plaintiff lawyer had to build through depositions and document review, which often ran into a wall of “I don’t know” and a lack of records. After AI dashcams, the same fact is documented in the carrier’s own systems with date, time, severity score, and reviewer ID.

The expansion beyond commercial fleets is already underway. Insurance usage-based products are moving toward AI scoring of individual drivers, with telematics apps and devices feeding behavior data into pricing and underwriting models. OEM in-cabin cameras – Tesla, GM’s Super Cruise, and a growing list of competitors – now monitor driver attention as a condition of advanced driver-assistance features, and the data those cameras collect is retained on the manufacturer’s side of the connection.

The same evidentiary pattern that defines commercial-fleet litigation today will perhaps within a few years be available in consumer-vehicle cases too. Asking whether a driver was insured by State Farm, Progressive, or Allstate now needs follow-up questions on whether they enrolled in their telematics offerings.

A complete discovery request should specify: the configured detection thresholds and any changes to those thresholds during the relevant period; the human

review queue and disposition logs for every alert involving the subject driver; and the fleet-wide pattern data that shows whether the carrier’s response to AI-flagged risk was consistent with its written safety policy or a departure from it.

Conclusion

Telematics evidence is becoming a more consequential category of proof in commercial-vehicle litigation, and the AI frenzy will likely accelerate the widespread use of telematics. Soon telematics data may also become more common in personal-vehicle cases if insurance discounts tied to telematics use catch on.

The practical work is not glamorous: timely preservation letters, native-format document demands, multiple PMK depositions, and chasing down third-party vendors with subpoenas. Done well, these steps put a contemporaneous, machine-generated record of the employer’s knowledge and decisions in front of the jury – and turn admitted vicarious liability into a much more compelling story. 

Andrew T. Haling is a partner at Pathway Law Firm, where he represents plaintiffs in personal injury and wrongful-death matters throughout California. His practice focuses on motor vehicle collision and premises liability cases, with an emphasis on serious-injury, catastrophic injury and wrongful death litigation. He can be reached at ah@pathwaylawfirm.com