



Electronically stored information issues in personal-injury practice

ESI DISCOVERY FROM VEHICLE ELECTRONIC-DATA RECORDERS, CELL PHONES, COMPUTERS AND SOCIAL MEDIA

“You’ve come a long way baby,” was a cigarette slogan and may be apropos for data collection from smoking crashed cars. The first flight-data recorders were used in the 1940s and became required for measuring 88 different parameters starting in August 2002. More recently, upwards of 700 pieces of information and the plane’s position are accounted for. (<https://exchange.aaa.com/automotive/automotive-trends/event-data-recorder/#:~:text=Ninety%2Dfive%20percent%20of%20new,excessive%20rate%20of%20vehicle%20deceleration>)

Cockpit-voice recorders have been recommended since 1960. Since 1999, they have been required to be solid-state, powered independently and carry at least two hours of crew communications. (*Ibid.*)

Marine vessels – passenger ships – carry voice-data recorders capable of recording 12 hours of data for identified performance standards. Trains are equipped with “Locomotive Event Recorders,” which also record crew communications for purposes of investigating accidents.

Event-Data Recorders

Event-Data Recorders or EDRs are the successors to “On-Board Recorders,” that were once used in commercial vehicles to record duty, status, distance and hours driven. (See, 49 CFR § 395.15). In 1997, EDRs were introduced in passenger cars to gain information on “crash pulses,” and other crash parameters. After August 2012, all passenger cars, multipurpose passenger vehicles, trucks and buses weighing over 8,500 pounds (GVWR) were required to carry EDRs. (49 CFR § 563.3.)

EDRs are regulated by title 49, Part 563 of the Code of Federal Regulations, “to help ensure that EDRs record, in a readily usable manner, data available for effective crash investigations and for analysis of safety equipment performance (e.g., advanced restraint systems). These data will provide a better understanding of the circumstances in which crashes and

injuries occur and will lead to safer vehicle designs.” (49 C.F.R. § 563.2.)

“The recording logic of Part 563 means that if a vehicle has experienced an event that reached the trigger threshold, it will be stored on the EDR. Rather than being erased due to a number of ignition cycles, an event can be overwritten by another event.” (Watson, et al., Event Data Recorder Trigger Probability in the Crash Investigation Sampling System Database, SAE Technical Paper 2024-01-5027, 2024.) Thus, “capture,” refers to the process of buffering EDR data in a temporary, volatile storage where it is continuously updated at regular intervals. An “unlocked event” may be overwritten by subsequent events. Once an event is locked in, it cannot be erased except by a manual reset.

General Motors has used “Sensing and Diagnostic Modules” (SDM) since 1994, to record pre-crash data, such as vehicle speed, engine rpm, throttle position, and in some 1999 models, brake status. This evolved significantly over time to include acceleration, angular momentum, seatbelt use, and other variables. Federal regulations require that EDRs record at least 15 data points. (See, 49 CFR § 563.7 (a) (2019).)

Note that aftermarket or retrofitted systems may not be visible to the vehicle’s EDR. And EDRs do not record dates, per se, but record ignition cycles from which approximate dates can be ascertained for purposes of analyzing fixed events in the nonvolatile memory and events remaining in the volatile memory.

EDR triggers

The *trigger* for an *event* is a longitudinal, cumulative delta-V of over .8 km/h that is reached within a 20 ms interval. For vehicles that record a “delta-V lateral,” the first point in the interval is a cumulative value of 0.8 km/h within 5 ms; or deployment of a nonreversible deployable restraint or activation of a VRU (vulnerable road user)

secondary safety protection system. These extraordinarily brief intervals are given perspective in the cases that include EDR data, and a sample is provided below.

California Vehicle Code section 9951

Very little has been written about California Vehicle Code section 9951, and it bumps up against federal regulations (Part 563). Section 9951 requires that manufacturers disclose whether a car it leases or sells is equipped with one or more “event data recorders (EDR)” or “sensing and diagnostic modules (SDM).” (*Id.* at subdivision (a).) If a subscription service can record and transmit this information, it must be disclosed in the “subscription service agreement.” (*Id.* at subdivision (e).)

[A] ‘recording device’ means a device that is installed by the manufacturer of the vehicle and does one or more of the following, for the purpose of retrieving data after an accident:¶

(1) Records how fast and in which direction the motor vehicle is traveling; ¶ (2) Records a history of where the motor vehicle travels; ¶ (3) Records steering performance; ¶ (4) Records brake performance, including, but not limited to, whether brakes were applied before an accident; ¶ (5) Records the driver’s seatbelt status; [and] ¶ (6) Has the ability to transmit information concerning an accident in which the motor vehicle has been involved to a central communications system when an accident occurs.

Pursuant to this section, the only person authorized to retrieve EDR/SDM data is the “registered owner,” unless, (1) “the registered owner... consents to the retrieval of the information;” (2) There is a valid court order; (3) There is an *unattributed* retrieval using the VIN (only) for “the purpose of improving motor vehicle safety, including for medical research of the human body’s reaction to motor vehicle accidents;” or (4) it is downloaded by the dealer or technician for diagnosing, servicing or

repairing the... vehicle. (Veh. Code, § 9951, subd. (c).)

Anyone retrieving the data may not share it except with “the motor vehicle safety and medical research communities to advance motor vehicle safety, and only if the identity of the registered owner or driver is not disclosed.” (Veh. Code, § 9951, subd. (d).)

It is unclear how much difficulty this section would pose for parties attempting to gain access to EDR data in *lawsuits* because a party will be coerced to consent or face the prospect of a court order. *Privacy* is not a factor of any consequence beyond ownership of the vehicle. EDRs do not identify the operator or even the date of an event, just the ignition cycle from which it must be deduced. The data reflects what the public perceives in plain view when the vehicle is in operation. It would be a stretch to claim discovery of EDR data violates the owner’s right of privacy in some legally tenable fashion if they are involved in a collision of any consequence. (*People v. Diaz* (2013) 213 Cal.App.4th 743, 757-758.)

Accident reconstruction in the cases

The value of EDR data in the hands of a qualified expert is obvious. *People v. Diaz, supra*, 213 Cal.App.4th 743, serves as an example of the process and its conclusion.

MAIT investigators downloaded the SDM on a Chevrolet Tahoe by going underneath the driver’s seat and cutting through the carpet. (*People v. Diaz, supra*, 213 Cal.App.4th at 751.) “MAIT inspection protocols include download of SDM data because it corroborates data the investigators look at when they check brakes, acceleration, and the steering column....” (*Ibid.*)

Data downloaded from the SDM showed that *five seconds before the impact*, the driver was not pushing on the gas pedal, and the Tahoe’s speed was 84 miles per hour. *Four seconds before the impact*, the vehicle was traveling at 80 miles per hour with 7 percent pressure on the gas pedal. *Three seconds before the impact*, the vehicle was traveling at 77

miles per hour, with 31 percent pressure on the gas pedal. *Two seconds before the impact*, the vehicle was traveling at 77 miles per hour, with 84 percent pressure on the gas pedal. *One second before the impact*, the vehicle was traveling at 76 miles per hour, with 94 percent pressure on the gas pedal. *The brake was not on from six to eight seconds before the impact*. It was *on at five seconds before the impact*, and *not on from four to one seconds before the impact*. Officer Wong testified, based on his “training and experience with collision reconstruction,” that “the photographs that [he] saw of the damage to both vehicles” was consistent with “the Tahoe traveling at 76 miles per hour.” (Emp. supp.) (*People v. Diaz, supra*, 213 Cal.App.4th at 748.)

The manipulability of the data and value of testing protocols, even when expert (police) testimony is involved, comes through Court of Appeal decisions with appropriate incredulity. (See, e.g., *People v. Hughes* (2020) 50 Cal.App.5th 257.) In *Hughes*, an initial review of the information from the EDR suggested that the driver’s intoxication did not play a role in the crash. But late in the case, a controversy arose when a Sgt. Berns testified that the 63-mph speed that was determined by the MAIT Team’s “sophisticated calculations” were only for a minimum speed, but in his opinion, that speed had been underreported. (*Hughes, supra*, 50 Cal.App.5th at 270.)

He testified that the older EDR recorded only 78 ms, whereas newer recorders capture data for a longer interval. He claimed this caused an underreporting of the decrease in speed caused by the collision by approximately 3-4 mph, so that the defendant’s speed before applying the brakes was actually 67 mph (comparing that to someone driving at 55 miles per). By extrapolating statistics about how alcohol can impair reaction time, and applying that to *Hughes*, Sgt. Berns was able to offer testimony that had he been sober, *Hughes* would have avoided the collision. (*Hughes, supra*, 50 Cal.App.5th at 270-272.)

The trial court’s method of dealing with the new and puzzling expert testimony was essentially to do nothing. It was reversed on appeal for not allowing defense counsel the opportunity to discover how Sgt. Berns arrived at his calculations where none were present in the file. (*Hughes, supra*, 50 Cal.App.5th at 276, 284-285.)

Privacy rights in property and opposing rights of discovery

There are many cases that focus on the limits of a party’s right of privacy in the context of discovery for civil litigation. The California Constitution has an express right of privacy (California Constitution, article I, §1) and cases have respected the power of the people to say, “none of your business.” But there are limits.

The framework for examining privacy in the modern era was established by cases like *Valley Bank of Nevada v. Superior Court* (1975) 15 Cal.3d 652, 656, and built on by cases like *Britt v. Superior Court* (1978) 20 Cal.3d 844, culminating with *Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 35. *Hill* was followed and clarified in *Williams v. Superior Court* (2017) 3 Cal.5th 531, 533 (*Williams*), and can be summarized:

The party asserting a privacy right must establish a legally protected privacy interest, an objectively reasonable expectation of privacy in the given circumstances, and a threatened intrusion that is serious. [Citation omitted.] The party seeking information may raise in response whatever legitimate and important countervailing interests disclosure serves, while the party seeking protection may identify feasible alternatives that serve the same interests or protective measures that would diminish the loss of privacy. A court must then balance these competing considerations. [citation omitted]. (*Williams, supra*, 3 Cal.5th at 535.)

Williams specifically holds that not every request for discovery of private information is an “egregious invasion”

of privacy. Necessarily, this depends on what is requested and context, and it is the burden on the objecting party to establish the extent and seriousness of the prospective invasion and against that showing, the trial court must weigh the countervailing interests the opposing party identifies. (*Williams, supra*, 3 Cal.5th at 537.) Accordingly, a *compelling need* is only necessary when the violation of privacy is “fundamental to personal autonomy.” (*Ibid.*)

Cell phone and computer-discovery trends

It is established that California courts have the authority to grant inspections of digital devices. (*Ellis v. Toshiba America Information Systems, Inc.* (2013) 218 Cal.App.4th 853, 881 (as modified, Aug. 14, 2013, and as modified on denial of reh’g, Sept. 10, 2013).)

Discovery of cell phones and computers should include, “[a]ppropriate protective orders... defin[ing] the scope of, inspection and copying of information on the computer to that which is directly relevant to this litigation, and can prohibit the unnecessary copying and dissemination of... other information that has no rational bearing on this case.” (*TBG Ins. Services Corp. v. Superior Court* (2002) 96 Cal.App.4th 443, 454.)

Cell-phone discovery is important in cases where there is a controversy about whether an employee was within the course and scope of her employment at the time of a tort (*Miller v. American Greetings Corp.* (2008) 161 Cal.App.4th 1055, 1059-1060, 1062, and n.4 (no call to create triable issue)) and whether the phone was engaged without a Bluetooth device or by using voice commands while *moving through space*. (See, e.g., *People v. Ram* 2023 Cal.App. Unpub. LEXIS 3379, at *12-13 [“The calls were not made through Bluetooth or Siri or any other hands-free method. The data revealed the calls were made by physically manipulating the device and typing in the numbers on the phone’s screen”].)

The Superior Court cases illustrate occasions and limits where cell phone discovery is attempted. The parameters

for duration (of discovery) are the most restricted elements. In *Leiva v. Vasquez*, 2023 Cal. Super. LEXIS 85393, a trial court case that serves as an example, plaintiff sought discovery of the defendant’s two cell phones, between 5:00 a.m. and 9:00 a.m., on the date of the incident (*Id.* at*8-9). It was claimed he was using one or the other, and was distracted. (*Ibid.*)

Plaintiff sought a “*mirror image*,” surrounding the 5:30 a.m. collision. According to the call records, the defendant had been using his work phone at 5:28 a.m. and 5:31 a.m. (*Id.* at*5-7.) The objection was made that the demand did not explain how the “active use” data was differentiated from the “background data,” but that issue was left to the experts and the inspection was permitted. (*Ibid.*) There was sufficient justification for the inspection because the defendant could have been using his phone while driving. (*Ibid.*)

Federal discovery rules facilitate ESI discovery. Cell phone discovery has been attempted as fact discovery for use of alcohol/drugs while driving and indicia of genuineness of the relationships between the decedent and heirs-at-law. (*Jones v. Sunbelt Rentals, Inc.* (N.D.Cal. Nov. 16, 2023, No. 22-cv-05954-AMO (PHK)) 2023 U.S. Dist. LEXIS 236920, at *27-28.) In *Jones*, Sunbelt proposed a 30-day window for the cell phone search that included daily use, texts, social media messaging, photographs, and telephone calls. (*Ibid.*)

Plaintiffs sought to narrow the discovery window to three hours and 16 minutes and to exclude photographs and social media files. They also offered to produce a log of the texts, but not the text messages between the decedent and plaintiffs. (*Jones, supra*, 2023 U.S. Dist. LEXIS 236920, at *28-29.)

The District Court ordered that once the cell phone was copied to create a mirror image, the plaintiffs were ordered to produce the following materials about the date of the incident. In addition to those materials, the Court ordered,

Plaintiffs to obtain, review, and produce from Decedent’s cell phone

copies of the following: non-privileged text messages, social media messages (to the extent downloaded and stored on the cell phone already), phone call logs, and video conference call logs from the Decedent to or from any Plaintiff, provided that such ESI is relevant to decedent’s relationship with any of the Plaintiffs. The time frame for this category is limited to the week immediately preceding the approximate time of the accident, to avoid unnecessarily cumulative, duplicative, and nonproportional discovery. Accordingly, ESI produced in this category is limited to those electronic files created from August 29, 2020, until September 5, 2020.

(*Jones, supra*, 2023 U.S. Dist. LEXIS 236920, at *37-38.)

The rationale for limiting the decedent’s cell phone discovery from 30 days to a week was the amount of discovery Sunbelt had pursued with family members. The District Court found the cell phone discovery as proposed was unduly “cumulative, duplicative and not proportional to the needs of the case.” (*Jones, supra*, 2023 U.S. Dist. LEXIS 236920, at *37-38.) However, since plaintiff offered to produce a log of text messages (not the messages themselves), the Court ordered one month to demonstrate the frequency of their texting. (*Ibid.*) An ESI privilege log was also required for any communications from the decedent’s phone “that implicate privacy or are otherwise confidential.”

Developments in social-media discovery: Oh, snap!

Several cases have examined the rights of parties to engage in social-media discovery. For the most part, these are criminal subpoena cases, but the basis in adjudication applies equally to civil subpoenas. The courts have explained that in 1986, Congress passed the Electronic Communications Privacy Act (ECPA), and within that legislation was the Stored Communications Act, 18 U.S.C. § 2701, et seq., which defined the types of entities that could assert a

near-complete block against discovery subpoenas. (See *Facebook, Inc. v. Superior Court* (2020) 10 Cal.5th 329 (*Touchstone*); *O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 1440, discussing 18 U.S.C. § 2702(a)(2).)

There were occasions where “consent,” through court orders facilitated this type of direct discovery (see *Negro v. Superior Court* (2014) 230 Cal.App.4th 879, 889), but for the most part, companies like Meta, Inc. (Facebook), Instagram, Snap, Inc. were prohibited from furnishing responsive materials that were private or non-public.

However, on July 23, 2024, *Snap, Inc. v. Superior Court* (2024) 103 Cal.App.5th 1031, was decided by the California Court of Appeal, and embraced a theory that was initially amplified by the Chief Justice in her concurrence in *Touchstone*, which she wrote in addition to the (unanimous) majority opinion. (See, *Touchstone, supra*, 10 Cal.5th at pp. 362–363. (conc. opn. of Cantil-Sakauye, C. J.).)

That theory, “the business model argument,” posits that if companies are able to share the subscriber’s or member’s data with their “partners” (to offset costs of its operations, so that customers are not charged), they fall outside of the SCA and must assert some other basis to avoid the subpoena process. (*Snap, Inc. v. Superior Court, supra*, 103 Cal.App.5th at 1064-1065.)

Until legislation is passed updating the SCA, as the Chief Justice implored, this is likely to be the legal basis for unfettered discovery of social-media accounts – against which constitutional and statutory privacy arguments still remain – but “the camel’s nose is in the tent.” Any entity that is monitoring and coordinating ads likely will not pass muster for its “Terms of Service,” or “Data Policy.” (See, *Snap, Inc. v. Superior Court, supra*, 103 Cal.App.5th at 1052-1054.) There will be more to say about this next year.

Destruction and disposal of ESI

A recent Court of Appeal decision is instructive on the disposal of ESI, *Victor*

Valley Union High School Dist. v. Superior Court (2023) 91 Cal.App.5th 1121, 1140.

“‘Electronically stored information’ means information that is stored in an electronic medium.” (Code Civ. Proc., § 2016.020, subd. (e).) “‘Electronic’ means relating to technology having electrical, digital, magnetic, wireless optical, electromagnetic, or similar capabilities.” (*Id.*, subd. (d).)

The safe-harbor provision of section 2023.030, subdivision (f) specifically addresses when a trial court is authorized to impose sanctions for the spoliation of ESI.

Notwithstanding subdivision (a), or any other section of this title, absent exceptional circumstances, the court shall not impose sanctions on a party or any attorney of a party for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as the result of the routine, good faith operation of an electronic information system.

(Code Civ. Proc., § 2023.030, subd. (f)(1).)

Section 2023.030(f)(2) provides: “This subdivision shall not be construed to alter any obligation to preserve discoverable information.” The *Victor Valley* Court noted the statute did not define when a party was supposed to preserve information and expressly avoided entry into declaring any duties. (*Id.* at p. 1140.) Borrowing from federal discovery law because of its similarities the Court ruled,

[T]he safe harbor provision of section 2023.030 (f) does not apply when ESI was altered or destroyed when the party in possession and/or control of the information was under a duty to preserve the evidence because the party was objectively aware the ESI would be relevant to anticipated future litigation, meaning the litigation was “reasonably foreseeable.” (*Silvestri v. General Motors Corp., supra*, 271 F.3d at p. 590.) Litigation is reasonably foreseeable when it is “probable” or “likely” to arise from a dispute or incident (e.g., *MacNeil Automotive Products, Ltd. v. Cannon Automotive, Ltd., supra*, 715 F.Supp.2d at p. 801), but not when

there is no more than the “mere existence of a potential claim or the distant possibility of litigation.” (*Micron, supra*, 645 F.3d at p. 1320.) However, the “reasonable foreseeability” standard does not require that the future litigation be “‘imminent [or] probable without significant contingencies,” or even “certain.” (*Hynix II, supra*, 645 F.3d at pp. 1345, 1347, italics added.) (*Victor Valley Union High School Dist. v. Superior Court, supra*, 91 Cal.App.5th at 1149.)

Perpetuating discovery to preserve “ephemeral evidence”

Out-of-the-box discovery is generally what civil lawyers do every day because it is discovery that is geared to unique issues in individual cases. Once counsel understands the implications of the client’s claim, available evidence and what is available in her legal toolbox, she can choose the best course.

For example, if the plaintiff in a particularly serious injury case will require years to reach *maximum medical improvement*, a lawyer could be torn between filing a lawsuit – and conducting appropriate [investigation] discovery before evidence becomes stale or lost – or waiting on the patient’s recovery so that impending discovery obligations and trial do not overwhelm the client or push the case to judgment before it is ready, not just ripe. These can be difficult decisions in the best cases. It calls for decisive action, not handwringing.

One method of avoiding formal litigation, but accomplishing necessary discovery of “ephemeral evidence,” like the *data* from event data recorders or cell phones and computers is by petition to perpetuate discovery. It is easy to see why downloading event data recorders shortly after the occurrence is prudent planning when it is uncertain or dubious the involved (opposing) vehicle(s) will be available for inspection down the road and that the data will be preserved on volatile memory of the EDR.

It is even easier to understand that with everyone trading in and upgrading cell phones, that inspections of these

devices and computers are also within the realm of a good-faith petition to perpetuate testimony.

Historically, petitions to perpetuate discovery of things (e.g., documents) have been discussed in insurance discovery disputes. (See, *Griffith v. State Farm Mut. Auto. Ins. Co.* (1991) 230 Cal.App.3d 59, 64-65 (and cases cited); see also, *Conn. Indem. Co. v. Superior Court* (2000) 23 Cal.4th 807, 822-823 [not available for reinsurance agreements].) However, nothing in the case law suggests that these petitions are limited to insurance discovery.

That said, it's important to note that *general discovery* is not within the purview of these petitions and requests for non-specific, fishing expeditions could appear as subterfuge to avoid normal service of process of the summons and complaint for regular discovery. Moreover, according to the text of the statute, these petitions are not permitted for the purpose of ascertaining the *identity* of a prospective defendant. (Code Civ. Proc., § 2035.010, subd. (b).)

Code of Civil Procedure section 2035.010 is titled, "Right to obtain discovery to perpetuate testimony or preserve evidence for use if action is filed; Certain purposes not permissible." It provides in pertinent part:

(a) One who expects to be a party or expects a successor in interest to be a party to an action that may be cognizable in a court of the state, whether as a plaintiff, or as a defendant, or in any other capacity, may obtain discovery ... for the purpose of perpetuating that person's own testimony or that of another natural person or organization, or of preserving evidence for use in the event an action is subsequently filed.

(b) One shall not employ the procedures of this chapter for purposes of either ascertaining the possible existence of a cause of action or a defense to it, or of identifying those who might be made parties to an action not yet filed.

A verified petition must be filed in the Superior Court in the county of residence of at least one *expected* adverse party, and if no one resides in California, the county where the action or proceeding may be filed. (Code Civ. Proc., § 2035.030, subd. (a).) The petition is in the name of the person seeking to perpetuate testimony or preserve evidence. It must contain the following information:

- (1) The expectation that the petitioner or the petitioner's successor in interest *will be a party to an action* cognizable in a court of the State of California.
- (2) The *present inability* of the petitioner and, if applicable, the petitioner's successor in interest either to bring that action or to cause it to be brought.
- (3) *The subject matter of the expected action and the petitioner's involvement.* A copy of any written instrument the validity or construction of which may be called into question, or which is connected with the subject matter of the proposed discovery, shall be attached to the petition.
- (4) The particular discovery methods described in section 2035.020 that the petitioner desires to employ.
- (5) *The facts that the petitioner desires to establish* by the proposed discovery.
- (6) *The reasons for desiring to perpetuate or preserve these facts* before an action has been filed.

Recent developments in the construction of the California Arbitration Act suggests that

- (7) The name or a description of those whom the petitioner expects to be adverse parties so far as known.

- (8) The name and address of those from whom the discovery is to be sought.
- (9) The substance of the information expected to be elicited from each of those from whom discovery is being sought.

A successful petition authorizes the court to order any discovery countenanced in the Discovery Act, including oral and written depositions, inspections of documents, things and places, as well as physical and mental examinations. (Code Civ. Proc., § 2035.020.) Discovery is applicable here for preserving ephemeral evidence by way of the EDR, cell phone, and computer.

Conclusion

The more we enter and live in a digital world, the more lawyers must become familiar with and adept at using ESI discovery. Event-data recorders are becoming integral to accident investigation just as cell-phone data can facilitate location and activity. Keeping up with these advances will allow clients to gain advantages in redressing their harms and injuries by cutting through contrived defenses with cold hard facts: King Data.

David Hoffman is in private practice in Woodland Hills emphasizing all aspects of major tort litigation, including medical malpractice, insurance bad faith and civil rights violations. Mr. Hoffman is a former firefighter and has tried over 100 cases to verdict. He has been a member of the CAALA Board of Governors since 1993. He is a co-founder of the L.A. Bench-Bar Coalition, served a term on the LACBA Judicial Appointments Committee, and has spoken at numerous MCLE programs. Mr. Hoffman graduated from UCLA in 1984 and received his J.D. from Southwestern University School of Law in 1988.