



Richard J. Weston

WESTON INTELLIGENCE

Sub rosa surveillance: The cheapest witness in the room

HOW DEFENSE SURVEILLANCE GETS BOUGHT, WHO ACTUALLY PRODUCES IT, AND WHY PLAINTIFFS MUST STOP TAKING THE PACKAGE AT FACE VALUE

A surveillance video does not have to tell the whole truth to move a case. It only has to be believed. Show a jury 30 seconds of an injured plaintiff lifting a bag of dog food or bending to pick up a piece of paper, and that image can outlast hours of careful medical testimony, because people hold on to what they see more readily than what they hear. Psychologists call it the picture-superiority effect, one of the most replicated findings in memory research. In a case where sub rosa surveillance is in play, that asymmetry is the contest, and the defense has understood the advantage for as long as there have been cameras meant to capture it.

I spent more than 30 years on the side of the defense team that used it. I came up in carrier-side Special Investigations Units (SIU) as a Fraud Claim Law specialist trained in fraud and bad-faith investigation, working suspect high-exposure losses that needed a closer look than the adjuster could give. Part of that work was assigning sub rosa surveillance to the small group of private investigative firms lucky enough to make my vendor panel. I had no say on whose logo was on the panel, only the PI vendor I chose. I reviewed what came back from the field and moved files through the internal review chain, one case at a time, for the better part of three decades.

In all that time, as the investigator who assigned the work and surfaced the vendor failures, and at times as the operator in the field who produced the reports and the video, I was deposed about my own work twice. Neither of those depositions led to my taking the stand. I testified at trial three times, and in none of the three had I been deposed first. Sit with that. Three times a jury weighed surveillance I produced, and three times

the plaintiff's lawyer questioned me cold, with no prior sworn account to test and no transcript to hold me to.

Predictable, prosaic cross-exams

And the questions, when they came, stayed on the surface. How many hours I billed against how many minutes of usable video. How much I had earned from the defense attorney in the past year. Whether I followed the plaintiff inside. Fair questions, every one, and most every one aimed at the invoice rather than the evidence. "Did you follow him inside" and "how much have you earned from the defense attorney" both sit one inch from the questions that may win the case, why the continuity broke at the door and what the claimant did in the minutes the camera went dark, and they stopped short every time. How much you and your firm have made from the TPA or the carrier would open a whole next level of questions that could win the case, and maybe even the case beneath the case.

That is the gap, shown from the witness chair. The person who decides where the camera points, what is recorded, which minutes survive into the reel, and how the report characterizes them can shape evidence that moves a claim by six or seven figures, and in my own experience almost never answers for any of it under oath. Those lawyers had the right instinct and no map. The answers that might have changed the weight of the footage were in the file, never asked for, so I never had to give them.

Most sub rosa surveillance work performed by licensed investigators is done honestly, and I want to be clear about that. Most investigators engaged full time in the art of sub rosa operations are professionals who document what happened and turn in clean re-

ports. The problem is not the majority. It is a system that has been in place for decades and makes it nearly impossible to tell, even for the trained eye, from the four corners of a report, whether a package came from a seasoned, well-vetted professional or from someone hired three months ago who may have been flipping hamburgers for not much less, sent out alone with a camera and a cell phone.

Not so "raw"

Start with what a package actually is, and be careful with the word "raw." By the time footage reaches a carrier it has usually been handled more than once, pulled off the camera or card onto a field investigator's unsecured computer that re-encodes it, then encoded again inside an editing program of that investigator's choosing.

That editing step is typically where the date-and-time overlay in the corner of the frame gets added. On a professional handheld camera that stamp does not ride on the video automatically. The time and date live in the metadata, invisible until a forensic tool brings them out, and the same kind of tool lets whoever touches the file set the visible stamp to read whatever they choose, the change traceable only in metadata almost no one examines.

Some covert or static units do burn the time onto the image at capture, but the primary handheld generally does not. None of this is necessarily sinister. It is routine. But the file handed over as the "raw" record has already passed through the software of multiple decision-makers, often without either knowing what the other changed, not by accident, but by design, and that can alter what it appears to show.

The hours deserve the same skep-

ticism. An investigator may run static or unattended trail-cam-style cameras for long stretches, and that material can simply never surface. When something useful turns up, the dead time around it is sometimes cut for size, along with footage shot by accident. Some of this happens at the investigator's hands, some at the firm curating the version the client will see, and some carries no intent to hide anything. The point is not motive. It is that what arrives labeled the complete record is frequently neither complete nor, in any forensic sense, raw.

To know how much trust that artifact deserves, you have to look at how it was made, and that begins with how it was bought.

Bought on price

A plaintiff's lawyer tends to imagine the package as a deliberate choice, the seasoned defense team going out to find the best eyes for a high-exposure loss. It rarely happens that way. The work is placed by carriers, self-insureds, and the third-party administrators who handle files for them, and it is placed through relationships. Most work from a panel of approved vendors, assembled less on demonstrated accuracy, experience, and independence than on rates, relationships, and the persistence of a firm's sales staff.

Vendor reps cultivate the adjusters who assign the work, sometimes in ways that, if exposed, would end any resemblance of independence to the claim. Administrators often run their own investigative units as profit centers, a reason to keep the work in-house. I once had a TPA adjuster try to influence where he sent a case that needed surveillance, offering me a personal nonprofit account to donate into and a magazine ad for a power washer he wanted. A bit more than the occasional bagels or a lunch out. I refused it, ignored it, and laughed it off, and the case went where the merits sent it.

The decision that produces the video on your screen is made on price, coverage, and relationships, and the

relationships run shadier than most will ever know. It is not made on which investigator is the most experienced or the least likely to shade a corner for the client.

Defense counsel is usually not even in that loop and I would think this is by design. A good attorney may sometimes suggest a vendor, and the best of them do, because they know from prior work that a particular investigator delivers, but counsel rarely commissions the work or pays the invoice. The client does. The defense lawyer who later defends the footage often had no hand in choosing who produced it, and little visibility into how it was made.

That is the distinction the defense side would rather not examine, because it is the one that matters most. A package's quality is not set by the firm's brand or the owner's reputation. It is set by the individual investigator who sat in the vehicle, decided what was worth recording, and decided what went into the report. The firm is a logo. The investigator is the evidence.

And the investigator is precisely the variable the buying process does not select for. The most capable defense lawyers I worked with wanted to choose an investigator by reputation and deal with him directly. More often than not, they were not allowed to. For everyone else, the buyer usually does not know who actually held the camera and does not seem to care, content with the firm's name and the salesperson who last took them to lunch. An intentional layer of account staff sits between the client who paid for the assignment and the person who shot it.

A surveillance order looks like a small line item, so it gets bought like one. But the evidence it produces is often asked to move six and seven figures of claim value. When you buy a lever that size at commodity rates you have not saved money. You have quietly discounted your own exposure, and the bill arrives when the package fails under questions no one expected. If the footage must carry that weight, the thing

to pay for is the investigator operating as your agent in the field, not the logo on the invoice.

If at first you don't succeed...

There is a second layer plaintiffs' lawyers almost never see. When the first vendor comes back with nothing, hours of a claimant doing nothing that contradicts the injury, the carrier does not always take that as the answer. It re-assigns, and a new vendor goes out with the same hope. If that one fails, there is another. I have watched a single claimant worked by vendor after vendor until one finally produced the image the file was looking for.

The footage that did not deliver is not edited. It is left out completely, and unless plaintiff counsel asks for it by name it may never be produced. That is the real cutting room floor. It is not clips trimmed from a reel; it is whole assignments, sometimes whole vendors, set aside because they did not return the wanted result. After the cheaper operators come up empty, the carrier often brings in the expensive one who can get inside where the others could not, and the package that reaches the plaintiff carries no trace of the failed attempts before it. The defense did not edit the video. It edited the vendor list and kept the firm that got the shot.

Who is actually behind the camera

Consider who that investigator holding the camera is likely to be. The Bureau of Labor Statistics counted roughly 43,600 private detectives and investigators in the United States in 2024, at a median wage near \$52,000. Most do not do insurance-related sub rosa surveillance as their primary work. The pool that does is a fraction of that number, and the truly experienced specialists are a fraction of that fraction. The industry is overwhelmingly small shops. By IBISWorld's count there are about 30,877 private investigation enterprises in the country, roughly 85% of them with fewer than 10 people. Thin firms, thin margins, and a strong desire to keep the

client happy.

You need not take my word for it. Read the industry's own recruiting. The largest surveillance firms openly advertise for field investigators with no experience required, promising fully paid training, and a license, at rates that often start in the high teens and low twenties. These are people who may have been flipping hamburgers or serving your last beer, sent, frequently alone, to produce covert video in cases worth millions.

Training new people is fine; every profession does it. But consider the numbers. The low twenties an hour is roughly what a casino pays the surveillance operator who watches its floor for cheating. No one would stake a verdict on that operator's untested word. The insurance-defense system pays about the same to the person whose footage decides whether an injured plaintiff is believed in a seven-figure or eight-figure case, and then asks a jury to take it at face value. That is the mismatch the buyers engineered by buying on price.

"We missed that..."

You can read the inexperience in the reports if you know the work, and the most common tell is broken continuity. The target walks into a gym, a store, or a workplace, and the surveillance stops at the door. The report says the investigator entered but could not locate the subject, in a space too small for anyone to be missed. On the claims side, that report has a name. It is a prevarication, the polite word for a lie. I call it the "tap dance," the footwork a weaker operator does to explain why the camera went dark the moment the claimant left public view. Holding a subject in those moments without being burned is one of the hardest parts of the job, and the part the low-rate hire is least equipped to do.

The gap matters because of what it hides. Out of view, a claimant may have sat down, rested, taken medication, iced a joint, or moved in plain pain, none of it recorded, none of it in a reel built from the minutes spent crossing a parking lot. The investigator who never goes inside

cannot show you the claimant in distress. He can show you the walk from the car. A jury sees the walk. The distress happened where the camera would not follow.

I learned how invisible that operator is by accident. Inside a carrier's SIU, I flagged an investigator whose work kept failing in the same telltale ways and raised it with his firm. They let him go. Weeks later the same signature, the same gaps and excuses, surfaced on a different vendor on my own panel. It was the same man, moved to another firm I was already paying, and nothing on either report would have told me, because the reports carried a company logo and no human name or license number.

So, I changed the requirement. Every report I accepted would now name each investigator who worked the file and list their license number. Once the names appeared, so did the answer. A surprising share began with CC rather than C. In Florida a C is a fully licensed investigator who can open his own agency; a CC is an intern working under a sponsor while learning the job. The case-deciding video, in matter after matter, had been shot by a CC trainee, and the only reason I could see it was that I had forced the license onto the page.

AI is the accelerant

Artificial intelligence will make this worse, and it is the part everyone wants to discuss. Tools that alter speed, swap backgrounds, and generate deepfake audio and footage of things that never happened are getting better and cheaper every year, and some of what they produce will not be catchable by eye. That is real, and it is coming. But do not let the dramatic future of AI hide the ordinary present. The deepfake is the rare case. The inexperienced intern working a seven-figure exposure for the high teens and low twenties an hour is the common one. The greater near-term risk is not an AI-fabricated video. It is an authentic one, lawfully obtained, that is incomplete, poorly framed, or wrongly characterized by someone who did not know better, and then trusted

by everyone downstream who assumed somebody had checked.

AI can process what is in the package. Experienced investigative judgment knows what should have been there and why it may be missing. AI is the accelerant. The structural imbalance is the fire, and it is already burning. AI can search the graveyard; real intelligence knows where the bodies are buried before anyone drew the map.

Reading the package as an artifact

So, what should plaintiff counsel do? Change the assumption. The package is not a fact. It is an artifact, produced by an identifiable person or persons, through a process with identifiable weaknesses, in service of a result. Once you treat it that way, it becomes something you can take apart.

Begin with what you were given, and notice what you were not. A highlight reel or storyboard of grabbed frames is not the record. Demand the complete, unedited footage for every day of surveillance, not only the clips counsel produced, along with the original files as they came off the camera or card, not the editing-suite export, so the metadata survives. Demand the assignment itself, the instructions, the dates and hours worked, the surveillance logs, and the field notes and emails between the adjuster and the investigator or his firm.

Have the metadata examined. The encoding history shows how many times a file was opened and re-saved and in what program, and an expert can test whether the burned-in date and time match the metadata underneath, because on most cameras that overlay is a setting, not proof of when the footage was shot. Ask which device recorded it, and whether static or unattended cameras were used, then demand that footage separately and in full, since it is the most likely to have been culled and the least likely to be produced.

Then ask what the package is built to keep you from asking. Was this the only surveillance? Demand the complete assignment history: how many

vendors were sent, how many investigators worked it, and what each returned. The days that produced nothing useful existed once, and their absence from the production is itself a fact. A carrier that surveilled your client six times and shows you the sixth has told you something about the first five.

Demand the full name and license number of every investigator who worked the file, not the firm's owner, including those inside the firm who produced the package, and ask how long they have done this work and how many files they ran that week. License records reveal experience. In Florida a number beginning with CC is an intern. And consider the bar to become that intern in the first place. Florida requires 40 hours of training before an applicant can even apply for the CC license. To be licensed to cut hair in the same state, a cosmetologist or barber must complete 1,200.

The footage that may decide a seven-figure claim can lawfully be shot by someone the state asked for one-thirtieth of the training it requires before it will let a person cut hair. Other states differ. California, for example, issues one investigator license to a qualified individual rather than an intern class, so ask for the licensee's qualifying experience and who did the field work. In some states there is not even a license requirement. Either way, if a trainee shot the footage that anchors the defense, the jury should know it, and you will not learn it from a report that hides behind a logo.

In addition to matching the video to the report, turn to the still images, because almost every firm's report is built around them. Investigators pull frames into a photo log or storyboard, and the frames chosen are almost always the most damaging to the plaintiff, the single instant that looks worst, lifted out of motion that was otherwise unremarkable. Treat each grabbed image as a choice. Why this frame? Out of hours of footage, were any frames selected that show the plaintiff resting, guarding, or in pain, and if not, why not? A frame is

the most curated thing in the package, one instant standing in for everything around it.

None of this requires you to prove the video is fake. It requires you to show how little has been established about how it was made.

And do not stop at the firm. The witness who matters is the person who held the camera and wrote the report, not the case manager who fields the calls.

Ask about money the right way, in three steps, because most cross-examinations ask it wrong. The natural question is how many times the investigator has worked for the defense attorney in the room, and the answer is often very few, because the lawyer rarely hires or pays him. That small number looks like independence and is mistaken for it.

The better question is how much income has come to this investigator and his firm from the carrier, the administrator, the self-insured, and the adjuster who controls the panel, over years rather than this file. But even that understates it, because the investigator does not see what his firm collects. The real measure is what the firm has earned from that claims operation across all its files, which will not come from the witness in the chair. It surfaces only if you know which entity to ask, which is what an insider's audit supplies.

Reaching them is often where a package starts to come apart.

The harder question

Then there is the question that should interest anyone who litigates extracontractual exposure. None of this is, by itself, bad faith. An insurer is entitled to investigate, and hiring a vendor on price is a business decision, not a tort. The exposure arrives later, when a carrier leans on a package produced this way to deny, delay, or discount a claim it would otherwise have to pay. The question is whether the carrier knew, or should have known, it was relying on evidence built to be cheap rather than reliable.

That is a question counsel can develop from the record. The claims file

will often show what the carrier was told about the vendor and the investigator, what it paid, and what it chose not to ask. Documented defects, the missing footage, the unsupported characterizations, the inexperience of the operator, can bear on the reliability of the evidence and its admissibility. In the right case, the same record can speak to the carrier's good faith and its exposure beyond the policy limits. The audit does not announce bad faith. It builds the record from which counsel argues it.

As these cases are worked carefully, the economics shift. A carrier that learns its cheap package can become a bad-faith liability has reason to stop buying cheap. An industry that learns its work will be read rather than rubber-stamped has reason to compete on whether the work holds up. Price and relationships built the imbalance. Performance and reliability are the way out.

For 30 years the surveillance package was treated, on both sides, as the closest thing to objective truth a claims file could hold. It never was. It is a witness. It is very often the cheapest witness in the room, and almost always the one no one cross-examined. The plaintiff bar that learns to read it does not only win individual cases. It raises the price of doing the work badly, and in doing so, it raises the floor for everyone.



Richard J. Weston is the founder and principal of Weston Intelligence, a plaintiff-exclusive forensic consulting practice in Fort Lauderdale, Florida, that audits defense surveillance packages as non-testifying consulting work product under Federal Rule of Civil Procedure 26(b)(4)(D). He holds Florida private investigator (Class C) and private investigative agency (Class A) licenses, and he is an industry-designated Fraud Claim Law Specialist (FCLS). He spent three decades in carrier-side claims fraud investigation specializing in sub rosa surveillance operations. He can be reached at westonintel.com.