2026 Hospitality & Retail Practice Group Seminar

January 28-30, 2026

Somebody's Watchin' Me – Surveillance in Litigation and the Workplace

Ransome "Ranse" Hare
Moderator
MCDOWELL KNIGHT ROEDDER & SLEDGE
Mobile, Alabama
rhare@mcdowellknight.com

Introduction

In the 1984 Rockwell hit, *Somebody's Watching Me*, the protagonist struggles with a growing sense of paranoia due to what he feels is the constant observation – or surveillance – of his daily activities by unknown figures. What were just catchy lyrics in the 1980s now ring as an undeniable truth. And in the context of personal injury litigation and modern workplace management, it is no longer paranoia – surveillance is policy, practice, and in many cases, protocol.

But what does *surveillance* entail? When, why, and how do we *effectively* and *ethically* obtain and utilize it? In litigation, effective surveillance can expose exaggeration or fraud and lend credibility to a defense narrative. Improperly handled, it can trigger ethical violations, discovery sanctions, or jury backlash. In the workplace, monitoring technology empowers employers to oversee productivity, safety, and compliance in real time. Yet, these tools also raise critical questions: How far can employers go before privacy rights are infringed? When does vigilance become intrusion?

This paper explores the strategic, ethical, and evidentiary questions surrounding surveillance in personal injury litigation, alongside the growing privacy and policy considerations of employee monitoring and workplace surveillance. By examining the evolution of surveillance technology and its expanding legal footprint, this paper aims to help practitioners and clients alike navigate this new era of constant visibility – one in which somebody's always watchin'.

Surveillance in Litigation

What does surveillance entail?

Derived from the French words *sur* (over) and *veiller* (to watch), the word quite literally means "to watch over."[i] In the litigation context, practitioners likely think of "surveillance" in the traditional sense, i.e., a private investigator tailing a plaintiff in hopes of capturing some evidence that would undermine the plaintiff's claims. And with advances in technology, this type of physical surveillance can be performed via a myriad of nontraditional methods such as unmanned cameras, smart glasses, and drones – just to name a few.

Whether viewed as a component of or a complement to surveillance, other measures such as social media canvassing, medical canvassing, background checks, and witness interviews are also critical to effective surveillance and general claim investigation. These measures and the manner in which they can be effected could each be the subject of a standalone article. For the purposes of this paper, however, I will generally focus on traditional video surveillance and social media canvassing.

Why should we utilize surveillance? Why shouldn't we?

When deployed thoughtfully and ethically, surveillance can be a powerful, multi-faceted tool in personal injury litigation. Performed haphazardly, however, it has the potential to weaken your case or worse, expose practitioners to ethical violations, discovery sanctions, and in extreme situations, civil liability.

The Benefits

At its core, effective surveillance helps defense counsel test the accuracy and credibility of claimed injuries and damages. Beyond impeachment, surveillance serves a broader strategic purpose. Identification of inconsistencies may help shape litigation strategy, allowing counsel and clients to make more informed decisions about risk and resolution. Even when surveillance does not produce a "smoking gun," it can confirm the legitimacy of a claim, helping defense teams avoid unnecessary escalation and focus resources appropriately.

A Video Surveillance "Success Story"

Most attorneys and clients have one or two go-to surveillance success stories that best illustrate the value effective surveillance can bring to a case. In terms of video surveillance, a recent workers' compensation case is my current go-to.

The plaintiff was a blue-collar, middle-aged male who suffered a crush injury to his foot. This evolved into multiple "related" conditions and nearly three years of treatment and therapy. Because the employer had no positions available that could accommodate the plaintiff's restrictions, the plaintiff did not work at all during the pendency of his claim.

One afternoon, while making small talk with the nurse case manager following a physical therapy appointment, the plaintiff mentioned that he raised "fighting chickens" and that he was heading to purchase feed for them at a local farm store. Given the plaintiff's claimed impairments and restrictions, this remark raised immediate concerns and warranted further investigation. We therefore retained a private investigator to follow the plaintiff after his next physical therapy visit.

On two separate occasions, the investigator captured video of the plaintiff effortlessly lifting and tossing multiple fifty-pound sacks of chicken feed into his lifted pickup truck. Yet later, during his deposition, the plaintiff testified that he was barely able to feed his chickens at all. He further claimed that he relied on others to bring him chicken feed and that he had been unable to lift a bag of feed at any point since his injury.

In light of the surveillance footage, the plaintiff's testimony, and multiple inconsistencies throughout his medical records, we believed the plaintiff's credibility could be effectively impeached at trial. Accordingly, we adopted an aggressive posture at pre-trial mediation. When the plaintiff reached his "bottom dollar," we generally advised the mediator that we possessed certain impeachment evidence that gave us great confidence. While I do not know precisely what was said in the other room, to our client's delight, the case ultimately settled that day – at a figure well below the plaintiff's purported bottom line.

A Social Media "Success Story"

Although I was only indirectly involved, my go-to social media story comes from a slip-and-fall case. The plaintiff was a middle-aged female with pre-existing spinal conditions. She alleged that the fall exacerbated these conditions, ultimately leading to a cervical spine fusion and chronic neck and back pain. As a result, she claimed she could no longer engage in many of the activities she once enjoyed and sought damages for loss of enjoyment of life and future pain and suffering.

The case was filed nearly two years after the incident, and the plaintiff was not deposed until approximately eighteen months later. Immediately after suit was filed, defense counsel captured screenshots from the plaintiff's and her husband's Facebook pages, both of which were publicly accessible. Despite the plaintiff's claims, her social media presence painted a very different picture. Rather than depicting a loss of enjoyment of life, the posts showed frequent casino trips, concert attendance, and multiple cruises and vacations – each documented in detail. Defense counsel continued to monitor the couple's social media throughout discovery and leading up to the plaintiff's deposition, during which time the plaintiff continued to portray an active and lavish lifestyle.

At the plaintiff's videotaped deposition, defense counsel introduced more than three years' worth of social media content – approximately 400 pages of posts across the two profiles. Counsel methodically questioned the plaintiff about many of the events depicted and how she was able to participate in those activities given her alleged physical limitations. One particularly memorable exchange involved the plaintiff's attendance at a Grand Funk Railroad concert. Visibly frustrated – as she had been throughout the social media questioning – the plaintiff testified that she did not know whether she had actually "seen them or not." In response, lead counsel asked: *"You know the song 'We're an American Band' – 'we're comin' to your town, we'll help you party down'?"* Despite identifying herself as a rock-and-roll fan, even those iconic lyrics failed to jog the plaintiff's memory.

The case ultimately settled before trial for an amount that the client was very pleased with. Lead counsel later described the social media evidence – and the plaintiff's testimony regarding the same – as a "huge deal" in bringing the case to a favorable resolution.

The Risks

Until recently, I did not fully appreciate the risks – beyond mere sunk costs – that surveillance can present. In my home jurisdiction, the Alabama Supreme Court has indicated that in most cases video surveillance would constitute protected work product and, arguably, such protection would only be removed if the party "decides to use the videotape as evidence."[ii] Therefore, in a worst-case scenario, unfavorable surveillance would never be used at trial and, in turn, would not materially affect the defense of the case.

However, in researching this topic, I have learned that is not always the case across the jurisdictions, and that the decision to conduct surveillance – even if it leads to favorable results – can carry real and tangible risks that extend well beyond expense alone. These possible risks include:

- Validation of a plaintiff's claimed injuries or limitations in jurisdictions requiring disclosure of surveillance materials;[iii]
- Juror backlash based on the performance and use of surveillance, even if arguably favorable to the defense;[iv]
- Exposure to ethical violations based on the use of improper and unethical methods in obtaining surveillance and social media information;[v]
- Exposure to discovery sanctions based on the improper disclosure and handling of surveillance evidence;[vi]

As such, practitioners and clients alike must understand the law in the jurisdiction where a claim is pending and weigh the potential risks presented when deciding whether to perform surveillance.

When and how do we perform effective surveillance?

These questions can be as important as deciding whether to conduct surveillance at all. Both inquiries are best approached through a disciplined cost-benefit analysis informed by the specific facts of the claim, the plaintiff's alleged limitations, and the procedural posture of the case. When deployed thoughtfully, early surveillance can assist in case valuation, discovery strategy, and settlement posture. When deployed prematurely, haphazardly, or without clear objectives, however, it can introduce unnecessary expense and expose the defense to avoidable risks.

Timing Considerations (When)

Video Surveillance

Although not an absolute policy, I typically prefer to delay any video surveillance until after receiving written discovery and pertinent medical records from the plaintiff (and, in certain cases, non-parties). I have found that without a robust social media capture at the outset of the claim or some "inside information" from a source with knowledge of plaintiff's day-to-day activities, such as the nurse case manager in the "chicken feed" case above, it can be difficult to obtain effective video surveillance. From a pure cost standpoint, engaging in speculative or "blind" surveillance – based largely on assumptions about where and when a plaintiff may be present – is, in my opinion, risky. With well-planned and carefully drafted discovery requests and non-party subpoenas, you may be able to obtain detailed information that can allow you to conduct more certain and targeted surveillance.

If after obtaining such information the defense team determines that personal surveillance is appropriate, I prefer to conduct said surveillance before the plaintiff's deposition, if possible. Even if I do not ultimately choose to directly confront the plaintiff with surveillance evidence during a deposition, I find it helpful to specifically tailor questions based on what the surveillance shows.

If you have not been able to obtain information to facilitate effective surveillance prior to a plaintiff's deposition, it can present an opportunity to obtain details regarding the plaintiff's daily activities and alleged limitations. At that point, surveillance should ideally be performed as soon as practicable. Assuming valuable surveillance is obtained, timely performance ensures that the activities captured are in close temporal proximity with plaintiff's testimony, strengthens your overall posture moving forward, and mitigates the risk of running afoul with disclosure deadlines further discussed below.

Social Media Canvassing

Unlike personal surveillance, the cost risks associated with early social media canvassing are minimal. The first thing I do when a new claim comes in is have a paralegal check the claimant's social media. Assuming any helpful social media information is publicly available,[vii] we immediately capture the same via screengrab. Moreover, we typically set internal reminders to periodically re-check any significant social media profiles throughout the duration of the case and update the evidence in our files as necessary.

There are at least two critical reasons for performing initial social media canvassing and capturing as quickly as possible. First and foremost, the social media world is an ever-changing environment. What is there today may be gone tomorrow – perhaps due to the targeted user removing certain posts or changing his or her privacy settings. While it may be possible to obtain information that is no longer available (or even information that was never available because of privacy settings) through discovery, it is certainly easier to capture that information without having to navigate discovery channels.[viii] Second, as alluded to above, an initial social media capture may provide information through which targeted and cost-effective personal surveillance can be performed.

While the cost risks may be minimal, as discussed in other sections, haphazard or rushed social media canvassing can present ethical risks – perhaps even more significant risks than personal surveillance presents. As such, regardless of whether such investigations are outsourced or performed in-house, practitioners and clients should ensure that all team members know not to sacrifice ethics in the name of haste.

Strategic and Execution Considerations (How)

Effective surveillance begins with clear objectives. Counsel should identify what specific claims, restrictions, or activities are at issue before surveillance is initiated. As discussed above, well-planned, targeted surveillance –

focused on dates, locations, and activities tied directly to alleged limitations – based on verifiable information is most likely to produce meaningful, defensible evidence.

The selection of qualified investigators and vendors is equally critical. Experienced professionals understand legal and ethical boundaries, maintain proper documentation, and know how to capture footage that is accurate, continuous, and minimally intrusive. Coordination between counsel, claims professionals, and investigators – at all stages – regarding costs, goals, expectations, and methods helps ensure surveillance aligns with the litigation strategy and budget, as well as evidentiary requirements.[ix]

How do we perform ethical surveillance?

While effective surveillance is the goal, as practitioners, *ethical* surveillance must be our overriding priority. Whether we allow firm staff to perform initial social media canvassing or outsource personal surveillance to a private investigative firm, we remain bound by the rules of professional conduct in our respective jurisdictions.

Instructive Authority

The Model Rules of Professional Conduct and interpreting authorities are a helpful polestar for attorneys navigating the ethical considerations underlying effective surveillance practices, with the most relevant Rules cited and summarized below:

- Model Rule 4.1 states that, "[i]n the course of representing a client, a lawyer shall not knowingly make a false statement of material fact or law to a third person."[x] According to the Rule 4.1 Comments, "[a] misrepresentation can occur if the lawyer incorporates or affirms a statement of another person that the lawyer knows is false," or if the lawyer makes "partially true but misleading statements or omissions that are the equivalent of affirmative false statements."[xi]
- Model Rule 4.2 prohibits lawyers from communicating "about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter" without consent of the other lawyer or authorization by law or court order.[xii]
- Model Rule 4.4 states that a lawyer "shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person."[xiii]
- Model Rule 5.3, in sum, provides that a lawyer having supervisory authority over nonlawyers employed, retained by, or associated with the lawyer, shall "make reasonable efforts to ensure" that said nonlawyers' conduct is compatible with the professional obligations of the lawyer."[xiv] Moreover, the Rule provides that a lawyer "shall be responsible for" the conduct of any nonlawyer under its supervision that "would be a violation of the Rules of Professional Conduct if engaged in by a lawyer."[xv] Given the broad nature of this language, it would appear to extend to firm employees as well as independent contractors, such as investigators, retained or "associated with" the lawyer.
- Model Rule 8.4 states that "[i]t is professional misconduct for a lawyer to . . . knowingly assist or induce another to [violate or attempt to violate the Rules of Professional Conduct], or do so through the acts of another."[xvi] In other words, "lawyers cannot do through third parties (such as investigators or paralegals) what they cannot themselves do under the rules."[xvii] The rule also states that it is professional misconduct for a lawyer to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation."[xviii]

Video Surveillance

Video surveillance of a personal injury claimant is likely one of the most common services requested of private investigators. With modern advancements, there seems to be an endless array of technology and devices available to investigators for the performance of such surveillance. Regardless of what technology an investigator chooses to employ, the mere surveillance of a plaintiff "in a public place such as outside the home or in a department store does not, in and of itself, appear to present lawyers with any difficulties under the Model Rules of Professional Conduct"[xix]

Problems may arise, however, if an investigator utilizes tactics or technology to observe a plaintiff in the privacy of their own home or other property not readily visible from a public space. First, such tactics could implicate an attorney under Model Rule 4.4, which prohibits a lawyer from obtaining evidence using means that have the purpose to embarrass, delay, burden, or violate the rights of a third person.[xx] Perhaps more concerning, such conduct could possibly give rise to civil liability to both the lawyer and the client (via *respondeat superior*) under a theory of tortious invasion or intrusion.[xxi]

Social Media Canvassing

Much like the surveillance technology available to investigators, it seems there are more social media platforms available today than the average person can keep up with. From Facebook, to Instagram, to X (formerly known as Twitter), these platforms, and the information plaintiffs post there, can often provide defense counsel with ready-made impeachment evidence. The manner in which we obtain this evidence, however, can potentially give rise to unintended consequences.

Similar to video surveillance, the consensus among interpreting authorities is that any information publicly available on a user's social media profile (i.e., not protected by privacy settings) is fair game.[xxii] Things become a bit more complicated, however, when the information we seek is not publicly available – meaning, in most cases, that you have to be a "friend" or "follower" of the targeted user. In these situations, a number of ethical rules come into play.

First, a "friend" or "follow" request made by a lawyer, or a nonlawyer acting under the lawyer's supervision (per Model Rule 5.3), to a target user who is represented by counsel is likely an ethical violation. Model Rule 4.2 expressly prohibits a lawyer from communicating "about the subject of the representation" with someone who the lawyer knows is also represented in the case.[xxiii]

Second, the use of a fake account or profile to "friend" or "follow" a target user, whether a party or a fact witness, can also give rise to ethical violations. The use of a fake name, picture, or other misrepresentation used to engage with a target user is directly at odds with Model Rule 4.1's prohibition against making false statements of material fact to a third party. Moreover, even if carried out by an investigator, this conduct likely runs afoul with Model Rule 8.4, which prohibits a lawyer (and, by extension, its investigator) from engaging in conduct involving "dishonesty, fraud, deceit or misrepresentation."[xxiv] Conversely, whether a nonlawyer, using his or her true identity, can "friend" or "follow" an unrepresented party or witness has traditionally been less clear.[xxv]

Due to what may be differing ethical rules and precedent across the jurisdictions, it is imperative that attorneys (and investigators) participating in social media canvassing consult the most current ethical rules, opinions, and case law in their jurisdiction.

How do we properly utilize surveillance evidence?

Once surveillance evidence has been obtained, the focus shifts to how it can be effectively leveraged in the case. The value of surveillance is not inherent in the footage or social media content itself, but in how it is evaluated, preserved, disclosed, and presented. Missteps at this stage can diminish, or even negate, the evidentiary benefit of otherwise helpful surveillance and expose the defense to avoidable procedural pitfalls. Accordingly, counsel must approach the post-collection use of surveillance evidence with the same degree of planning and discipline applied to its initial acquisition.

Strategic Considerations

From a strategic standpoint, counsel should promptly assess how any obtained surveillance fits within the broader litigation strategy. This includes determining whether the evidence is best characterized as substantive or impeachment evidence, whether it corroborates or undermines existing defenses, and how it may influence deposition strategy, expert opinions, or settlement posture. Counsel should also consider how the surveillance may be perceived by a jury, including whether the footage is susceptible to alternative interpretations or may appear incomplete or misleading when viewed in isolation. Thoughtful evaluation at this stage helps ensure that surveillance evidence is leveraged intentionally, rather than reactively, as the case progresses.

Discoverability and Disclosure Obligations

The discoverability and disclosure of surveillance materials is governed by a mix of procedural rules, evidentiary principles, and evolving case law. While federal courts have developed relatively consistent frameworks addressing when surveillance must be identified, produced, or supplemented, state courts have taken a more varied approach. As such, practitioners must understand *and comply* with the applicable governing law to avoid undermining the value of surveillance obtained during litigation.

Federal Law

Under the federal rules and case law, courts have generally held that the identity of a private investigator and the substance of any investigative report are subject to automatic disclosure, and that if surveillance is performed after initial disclosures, the party is required to promptly supplement its disclosures.[xxvi] Disclosure of the actual surveillance materials, and the timing of the same, largely hinges on whether the materials are in the nature of impeachment or substantive evidence.

For surveillance materials that a party intends to use strictly as impeachment evidence at trial, those may be withheld up until the deadline for pretrial disclosures (often thirty days before trial).[xxvii] However, federal courts have held that impeachment evidence is also subject to discovery.[xxviii] As such, if an opposing party has served discovery requests to which surveillance materials would be responsive, the standard production requirements (not the pretrial disclosure requirements) would apply.[xxix] The only caveat being that if the surveillance materials are protected by the work product doctrine, production is not required until after the plaintiff's deposition has been taken.[xxx]

Regarding work product claims, federal courts have distinguished the performance of surveillance and the actual surveillance materials.[xxxi] For example, the court in *Myers v. Aleutian Endeavors, LLC* held that "although surveillance material [i.e., photos and videos] is protected work product, whether a [d]efendant conducted surveillance and the dates on which any surveillance took place are not privileged."[xxxii] In other words, "the existence of surveillance is not protected work product."[xxxiii]

State Law

State law regarding the disclosure of surveillance materials varies across the country. Even states with similar procedural frameworks may have state-specific caveats and exceptions in their body of law. Therefore, it is important for practitioners to verify the current state of the law in the jurisdiction where a case is pending. Generally, most jurisdictions require the disclosure of video surveillance at "some point prior to trial."[xxxiv] In terms of discoverability and the timing of disclosure, most states likely fall into one of the following categories:

- Discoverable (not protected work product) and likely subject to initial or automatic disclosures requirements;[xxxv]
- Discoverable (not protected work product);[xxxvi]
- Work product but likely discoverable based on good cause, substantial need, undue hardship, etc.;[xxxvii]
- Work product but likely discoverable based on good cause, substantial need, undue hardship, etc., provided, however, the evidence need not be disclosed until after the plaintiff has been deposed;[xxxviii]
- Not discoverable (protected work product).[xxxix]

Whether or not expressly addressed, the distinction between impeachment and substantive evidence often underpins a court's analysis – especially in earlier reported opinions on the issue. However, "the pure impeachment argument generally has not been successful to avoid the discovery of surveillance."[xl]

Evidentiary Considerations

As surveillance evidence increasingly takes digital and online forms, courts have been required to reassess traditional evidentiary principles governing authenticity and admissibility. Video surveillance and social media content present distinct, but related, challenges – particularly as technological advances make recording, editing, and distribution easier and more accessible. In both contexts, courts focus on whether the proponent can establish that the evidence is what it purports to be, though the required showing varies by medium and jurisdiction. Accordingly, practitioners must be mindful of these authentication and admissibility concerns from the outset of any surveillance or canvassing efforts.

Video Surveillance

A number of objections may be raised when video surveillance is being offered into evidence. The most important issue for the presenting attorney to prepare for is authentication. With increasing accessibility to video surveillance, rising concerns about inauthentic videos through AI capabilities, and the ability to alter or modify video surveillance, it is no surprise that the law has changed significantly regarding authentication of video evidence.

Historically, video evidence was viewed only under the "pictorial communication" theory. Under this theory, the foundation for authentication could be laid by a witness with firsthand knowledge, usually the one who took the video, who would testify that the video "is what it is claimed to be."[xli] As courts began viewing video and photo evidence as substantive instead of just illustrative, the appropriate foundation could be laid by the "silent witness" theory.

The silent witness theory is most often used when authenticating automatic surveillance where there is no witness with personal knowledge who physically took the video themselves. Under this theory, courts may admit surveillance videos and photos when a witness testifies regarding the "type of equipment or camera used, its general reliability, the quality of the recorded product, the process by which it was focused, or the general reliability of the entire system."[xlii] In other words, the witness who may or may not have been present at the time of the recording, may authenticate the video by testifying about the "process or system and showing that it produces an accurate result."[xliii]

Social Media

Proper authentication of social media photos and videos is very unclear and a constant concern in litigation. The classic issue of social media authentication arises when a photo or video is posted from an account, but there is no evidence specifying exactly who used the account to make the post. In other words, courts may be concerned because although the account belongs to the plaintiff, technically anyone could use the plaintiff's log in information and create/post the photo or video.[xliv] An Ohio trial court and the Supreme Judicial Court of Massachusetts have ruled in opposite directions when presented with this scenario.[xlv]

Governing authority regarding the admissibility and authenticity of social media posts is constantly evolving and varies largely across jurisdictions.[xlvi] States like Maryland, Massachusetts, and Connecticut follow a strict approach that requires a heavier burden for authentication of social media posts than other photo and video mediums.[xlvii] Meanwhile states like Texas, California, and New York apply a moderate approach that only requires the proponent to provide what a "reasonable juror" would need in order to be persuaded that the evidence is authentic.[xlviii] Lastly, courts in Florida and Ohio have followed neither the strict or moderate approaches and require a relatively low burden similar to that presented in Rule 901 (i.e., it is authentic if evidence shows it is what it claims to be).[xlix]

Surveillance (Monitoring) in the Workplace

As technology advances and becomes more integrated into all workplaces, so does the ability of employers to monitor their employees.[l] An employee's personal information, and personal data in general, that was once considered off limits can now be "routinely collected, analyzed, packaged, and distributed instantaneously and at trivial cost."[li] From tracking keystrokes, to installing surveillance cameras in an office, there is a wide breadth of monitoring that is taking place in everyday workplaces. The ability of employers to monitor the activities of their employees in the workplace is governed by federal law, state law, and the Fourth Amendment privacy protections for government employees.

Why monitor the workplace?

Employers have a number of interests in monitoring their employees. Some employers may use monitoring as a mechanism for tracking the efficiency and safety of their employees, which may allow employers to provide their employees with objective feedback about their job performance or identify and address unsafe practices before they result in injury. Other employers may use monitoring as a risk management measure to protect themselves – either preemptively or remedially – from potentially harmful acts of their employees.

What does workplace monitoring entail?

Modern day employee monitoring can take a variety of forms and can take place before or after hiring. Some job applicants reported being asked to provide login information to personal accounts such as social media and Google/Yahoo.[lii] Some private companies report storing their employees' electronic data when there are potential violations of company policies, while others obtain and store such data as a routine matter.[liii] Such data could provide insight into what an employee is actually doing while using a company's property (computer, phone, etc.) and how much of their time "on the clock" is actually spent furthering the employer's interests. More specifically, company computers could be programmed to track and report the number of words typed per minute, how long it takes employees to complete tasks, and how long the computer is inactive (indicating how long of breaks employees are taking).[liv]

More intrusive forms of monitoring may occur when an employer hires an investigator to conduct surveillance on an employee who is claiming worker's compensation benefits or an employer using GPS capabilities on company phones, vehicles, or computers.[lv]

How far is too far?

Employee monitoring and workplace surveillance are shaped by a combination of constitutional principles and statutory privacy protections. Although many of the guiding principles originate in federal law and reported case decisions, those authorities often provide broader context for how privacy expectations are evaluated in the employment setting. State law may further refine or expand these limitations through constitutional provisions and statutory schemes that vary by jurisdiction. In light of these considerations, practitioners should be attentive to both federal and state-level constraints in implementing monitoring practices and in the subsequent use of information obtained through those practices.

Federal Limitations

Most reported case law regarding employee monitoring is in the context of government employees and the protections afforded by the Fourth Amendment. While private employers are not expressly restricted by the Fourth Amendment, the case law provides relevant background for considerations regarding employee monitoring. For example, the Supreme Court of the United States has held that a police officer's Fourth Amendment rights to privacy were not violated when his employer looked through his text messages that were sent and received on a pager issued by the employer.[lvi] Additionally, when evaluating the reasonableness of searches performed by employers, courts often find that a "work-related" search by an employer is reasonable even without a warrant.[lvii] A "work-related" search has been defined as a "search[] of 'those areas and items that are related to work and are generally within the employer's control.'" [lviii]

There are some federal statutes that outline privacy protections. For example, title III of the Omnibus Crime Control and Safe Streets Act of 1968 was amended by the Electronic Communications Privacy Act of 1986 (ECPA) and addresses how employers may monitor the communications of their employees.[lix] The ECPA prohibits intentional interception, and intentional attempts at interception, of "any wire, oral, or electronic communication."[lx] The Act further proscribes the use of such intercepted communications.[lxi] However, the Act does not prohibit reading or using communications that have already been transmitted (i.e., are not being intercepted), does not prohibit employers from monitoring communications on their own devices, and does not apply to surveillance videos without audio.[lxii]

State Limitations

Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington explicitly protect the right to privacy in their state constitutions.[lxiii] In Arizona it is as simple as "[n]o person shall be disturbed in his private affairs . . . without authority of law."[lxiv] The California constitution is more specific and more closely resembles the outlines of the Fourth Amendment.[lxv] Regardless of the range of protection, state constitutional protections have the same limitation as the Fourth Amendment in that they only apply to state action. A private employer will not be held to the privacy provisions in the state constitution unless for some reason they qualify as a state actor.

Most states have also enacted statutes similar to the federal Omnibus Crime Control and Safe Streets Act of 1968 discussed above. Some state statutes provide exemptions consistent with the federal statute and others may vary in their similarities to the federal law. For example, some state wiretapping statutes require the consent of both parties, while the federal Act only requires the consent of one party.[lxvi] Specifically, in the context of employee monitoring, some states such as Virginia and West Virginia require that an employer give the employee notice that their communications may be monitored.[lxvii]

How to best navigate these competing interests?

Navigating the tension between an employer's legitimate business interests and an employee's privacy expectations requires a deliberate and informed approach. As a threshold matter, employers should clearly define the purpose and scope of any monitoring program and ensure that the methods employed are reasonably tailored to those objectives. Advance notice and well-drafted written policies can significantly reduce risk by shaping employee expectations and strengthening the employer's position that any monitoring is work-related and reasonable. Where monitoring is more intrusive in nature, additional safeguards – such as limiting access to collected data and restricting its use to legitimate business purposes – can further mitigate potential exposure.

From a litigation and risk-management perspective, employers and their counsel should evaluate monitoring practices with an eye toward how the resulting information may later be used. Conduct that appears lawful in real time can create problems if monitoring exceeds stated policies, violates state-specific consent or notice requirements, or is deployed inconsistently. Regular review of monitoring policies, coordination with counsel familiar with jurisdiction-specific requirements, and thoughtful consideration of less intrusive alternatives can help employers strike an appropriate balance while preserving the utility of workplace monitoring when disputes arise.

Conclusion

Surveillance is no longer a niche litigation tactic or background workplace practice. Rather, it is a routine feature of modern claims handling and employment management. As surveillance tools and technology have expanded, so too have the legal, ethical, and strategic considerations that govern their use. In both litigation and the workplace, surveillance can be a powerful evidentiary and risk-management tool when employed thoughtfully, transparently, and in compliance with governing law. When misused or mishandled, however, it can undermine credibility, invite sanctions, and expose clients and counsel to unnecessary liability.

Ultimately, the effective use of surveillance is less about what technology allows and more about what judgment requires. Practitioners and employers alike must remain mindful that every surveillance decision – whether capturing a video clip, preserving a social media post, or monitoring employee activity – carries downstream consequences. By grounding surveillance practices in clear objectives, ethical constraints, and an informed understanding of disclosure and admissibility requirements, counsel can harness its benefits while mitigating its risks. In an era where somebody really is always watching, vigilance must be paired with restraint, and strategy must be guided by discipline as much as by opportunity.

---

[i] Online Etymology Dictionary, https://www.etymonline.com/word/surveillance (last visited Dec. 18, 2025).

[ii] *Ex parte Doster Constr. Co.*, 772 So. 2d 447, 451-52 (Ala. 2000).

[iii] *See infra* note xxxv and accompany text regarding states where mandatory disclosure rules potentially extend to surveillance materials. S*ee also McGee v. Burlington N. Inc.*, 571 P.2d 784, 791-92 (Mont. 1977) (holding that trial court properly allowed plaintiff to admit the contents of defendant's investigative report, which were helpful to plaintiff's case, at trial).

[iv] "The downside risk of using surveillance evidence has always been that a jury will become outraged over the intrusive tactic, and will return a verdict that punishes the defendant for being so rude as to spy on an injured plaintiff. In cases where plaintiffs are caught on film actually doing something they have claimed they cannot do, the drama can outweigh this risk, and these cases are the ones most likely lead to a decision to use surveillance evidence. Often, however, it is a close call. The point of the proof is to demonstrate that the plaintiff's claim is wholly fraudulent; and in instances where the plaintiff's claimed limitations were merely exaggerated, the subtle distinction between lying and mere hyperbole are often lost on a jury." William C. Altreutera, Use of Surveillance Evidence Poses Risk of Ethical Dilemmas and Possible Juror Backlash, 74-Aug NY St. B.J 40 (2002).

[v] *See infra* notes x-xxv and accompanying text regarding general ethics considerations.
[vi] *See infra* notes xxvi-xl and accompanying text regarding general discovery and disclosure considerations.
[vii] *See infra* notes xxi-xxv (social media ethics analysis) and accompanying text regarding ethics considerations in the social media context.
[viii] *See* Steven C. Bennett, *Ethical Limitations on Informal Discovery of Social Media Information*, 36 Am. J. Trial Advoc. 473, 479-81 (2013) (generally discussing the discovery of social media through formal discovery procedures).
[ix] *See infra* notes xli-xlix and accompanying text regarding general evidentiary considerations.
[x] MODEL RULES OF PRO. CONDUCT r. 4.1 (A.B.A. 2019).
[xi] *Id.*
[xii] MODEL RULES OF PRO. CONDUCT r. 4.2 (A.B.A.).
[xiii] MODEL RULES OF PRO. CONDUCT r. 4.4 (A.B.A.).
[xiv] MODEL RULES OF PRO. CONDUCT r. 5.3 (A.B.A.).
[xv] Provided the lawyer ordered or ratified the violating conduct, or, "knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action." *Id.*
[xvi] MODEL RULES OF PRO. CONDUCT r. 8.4 (A.B.A.).
[xvii] *See* Bennett, *supra* note viii, at 483.
[xviii] MODEL RULES OF PRO. CONDUCT r. 8.4 (A.B.A.).
[xix] Forrest Plesko, *On the Ethical Use of Private Investigators*, 92 DENV. U. L. REV. ONLINE 157, 159 (2015).
[xx] MODEL RULES OF PRO. CONDUCT r. 4.4 (A.B.A.).
[xxi] *See* Plesko, *supra* note ix, at 160 (citing Y*ork. v. Gen. Elec. Co.*, 759 N.E.2d 865, 868 (Ohio Ct. App. 2001), where the Court of Appeals of Ohio concluded that "surveillance activities outside the home would not rise to the level of invasion of privacy but that using a telephone lens or light enhancing equipment to look inside the home may."); *see also* Restatement Second, Torts § 652B, Intrusion upon Seclusion ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").
[xxii] Robert C. Nagle & Pamela Chandran, *Attorney Misconduct on Social Media: Recognizing the Danger and Avoiding Pitfalls*, 32 ABA J. LAB. & EMP. L. 427, 430 (2017).
[xxiii] MODEL RULES OF PRO. CONDUCT r. 4.2 (A.B.A.).
[xxiv] MODEL RULES OF PRO. CONDUCT r. 8.4 (A.B.A.).
[xxv] Forrest Plesko, *On the Ethical Use of Private Investigators*, 92 DENV. U. L. REV. ONLINE 157, 164-65 (2015).
[xxvi] *See* Fed. R. Civ. P. 26(a)(1)(A).
[xxvii] Fed. R. Civ. P. 26(a)(3)(B).
[xxviii] Brett D. Baber, *UNDER SURVEILLANCE*, TRIAL, Mar. 2021, at 46, 48.
[xxix] *Id.* at 49.
[xxx] *Id.*
[xxxi] *Id.*
[xxxii] *Myers v. Aleutian Endeavors, LLC*, No. 3:18-CV-0033-HRH, 2018 WL 2656162, at *1 (D. Alaska June 4, 2018).
[xxxiii] *Id.*
[xxxiv] Bradford J. Gower, *Discoverability of Private Investigator Surveillance in South Carolina: Navigating the Work Product Doctrine Under Samples v. Mitchell*, 61 S.C. L. REV. 691, 704 (2010).
[xxxv] It appears that only three states, Arizona, California, and Colorado fall into this category. Each of which have initial disclosure rules requiring the production of all items and materials *relevant* to the subject matter of the action – notably broader than the federal disclosure rules. *Compare* Ariz. R. Civ. P. 26.1, *and* Cal. Code Civ. Proc. §2016.090, *and* Colo. R. Civ. P. 26(a), *with* Fed. R. Civ. P. 26(a)(1)(A)(ii) (requiring disclosure of items a party "*may use to support* its claims or defenses.") (emphasis added). Moreover, courts in these states have held that both the existence and contents of surveillance are always discoverable. *See e.g., Zimmerman v. Superior Ct.*, 402 P.2d 212, 215 (Ariz. 1965); *Crist v. Goody*, 507 P.2d 478, 480 (Colo. App. 1972); *Suezaki v. Superior Court*, 373 P.2d 432 (Cal. 1962).
[xxxvi] *Williams v. Dixie Elec. Power Ass'n*, 514 So. 2d 332, 335-37 (Miss. 1987) (holding that defendant failed to comply with discovery rules when it did not provide surveillance videos prior to trial and that the trial court therefore erred in allowing the

videos to be admitted into evidence); *McGee*, 571 P.2d at 791-92 (holding that defendant's surveillance report was "properly discovered" by plaintiff and that trial court properly allowed plaintiff to admit the contents of said report, which were helpful to plaintiff's case, at trial); *Roundy v. Staley*, 984 P.2d 404, 408-09 (Utah Ct. App. 1999) (holding that video surveillance was relevant, discoverable, and not protected by the work product doctrine).

[xxxvii] *Olszewski v. Howell*, 253 A.2d 77 (Del. Super. 1969) (refusing to afford work product protection to surveillance due to a number of "substantial need" and "undue hardship" factors); *Hoey v. Hawkins*, 332 A.2d 403, 406 (Del. 1974) (existence of surveillance always discoverable and contents protected as work product which is inherently overcome by showing of good cause).

[xxxviii] *Dodson v. Persell*, 390 So. 2d 704, 708 (Fla. 1980) ("[F]airness requires that we allow the use of surveillance materials to establish any inconsistency in a claim by allowing the surveilling party to depose the party surveilled after the movies have been taken or evidence acquired but before their contents are presented for the adversary's pretrial examination.");.*Shenk v. Berger*, 587 A.2d 551, 556 (Md. Ct. Spec. App. 1991) (holding that where defendant intended to use surveillance videos as <u>substantive</u> evidence at trial it was required to disclose those opposing counsel but could refrain from doing so until after the plaintiff had been deposed) (emphasis added); *Fender v. Norfolk S. Ry. Co.*, No. L00-2840, 2001 WL 34037318, at *2 (Va. Cir. Ct. June 28, 2001) ("[B]efore Defendant is required to provide the surveillance videotapes .... the deposition of the Plaintiff and responses to all interrogatories and other discovery materials.., will have been provided by Plaintiff to Defendant.").

[xxxix] The most defense-friendly classification, it appears that only one state, Wisconsin, falls into this category – although this categorization is not ironclad. In the case of *Ranft v. Lyons*, 471 N.W.2d 254 (Wis. Ct. App. 1991), the Wisconsin Court of Appeals found that <u>both the existence and substance</u> of the defendant's post-accident surveillance of the plaintiff was protected from discovery under the work product doctrine. *Id.* at 261-62. Four years later, in *Martz v. Trecker*, 535 N.W.2d 57 (Wis. Ct. App. 1995), the Wisconsin Court of Appeals held that the trial court did not misuse its discretion in allowing the defendant to admit surveillance video evidence at trial that had not been previously disclosed to the plaintiff. *Id.* at 60. It should be noted, however, that both the *Ranft* and *Martz* opinions involved the appellate review of a trial court's <u>discretionary</u> decision to enforce the work-product privilege. In *Martz*, the court noted that the plaintiff never made a discovery demand for the surveillance and, therefore, "there was never any need for [the defendant] to respond to a discovery demand or to seasonably update a [response]." *Martz*, at 60. Moreover, both opinions also indicate that the plaintiffs were allowed to "seasonably challenge the surveillance material" prior to the defendant's use of it at trial. *Id.*; *Ranft*, at 262. As such, these opinions seem to at least imply that surveillance <u>may</u> be discoverable if the plaintiff serves a proper discovery demand and, if faced with a work product objection, demonstrates that there is "good cause" for the pretrial disclosure of surveillance. *Ranft*, at 60 ("The [plaintiffs] have not demonstrated that failure of pretrial disclosure would 'unnecessarily frustrate' the 'objectives of pretrial discovery' or, alternatively, that there is 'good cause' that requires disclosure before trial.").

[xl] Kenneth E. Siemens, *The Discoverability of Personal Injury Surveillance and Missouri's Work Product Doctrine*, 57 MO. L. REV. 871, 873 n.18 (1992).

[xli] Fed. R. Evid. 901(b)(1).

[xlii] *United States v. Stephens*, 202 F. Supp. 2d 1361, 1368 (N.D. Ga. 2002).

[xliii] Fed. R. Evid. 901(b)(9). For more discussion on the silent witness theory, see 2 Kenneth S. Broun et al., MCCORMICK, ON EVID. § 216, Westlaw (9th ed.) and 16 AM. JUR. PROOF OF FACTS 3d 493, § 5, Westlaw (1992).

[xliv] Breanne M. Democko, *Social Media and the Rules on Authentication*, 43 U. TOL. L. REV. 367, 389-90 (2012).

[xlv] *State v. Bell*, 882 N.E.2d 502 (Oh. Ct. Com. Pl. 2008); *Com. v. Williams*, 926 N.E.2d 1162 (Mass. 2010).

[xlvi] *See* Shawn Shepard & David C. Marshall, *FROM FOIA TO SOCIAL MEDIA Investigating Plaintiffs and Potential Jurors*, DRI FOR THE DEFENSE, Jan. 2019, at 66.

[xlvii] Kathryn S. Lehman & Lindsey Macon, *VIRTUALLY NO SECRETS Social Media in the Courtroom*, DRI FOR THE DEFENSE, May 2019, at 22.

[xlviii] *Id.*

[xlix] *Id.*

[l] *See* Ifeoma Ajunwa et. al., *Limitless Worker Surveillance*, 105 CAL. L. REV. 735, 738 (2017).

[li] *Shulman v. Group W Productions, Inc.*, 955 P.2d 469 (Cal. 1998), *as modified on denial of reh'g* (July 29, 1998) (Kennard, J., concurring).

[lii] METHODS AND EXTENT OF EMPLOYER USE OF ELECTRONIC MONITORING AND SURVEILLANCE, 2 EMPL. PRIVACY LAW § 8A:1 (West 2025).

[liii] *Id.*

[liv] *Id.* (citing Swoboda, *Pains of Electronic Monitoring: Study Finds More Stress for Workers Watched by Computers*, THE WASHINGTON POST, Oct. 21, 1990, at p F9).

[lv] EMPL. PRIVACY LAW § 8A:1, *supra* note 1 (citing *Roose & Griffin Landscape Contractors v. Weiss*, 558 So. 2d 102 (Fla. 1st DCA 1990)); *id.* (citing *National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace*, http://workrights.us/products=nwi-report-on-your-tracks-gps-tracking-in-the-workplace-pdf (last visited March 10, 2016)).

[lvi] *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 750 (2010).

[lvii] *See O'Connor v. Ortega*, 480 U.S. 709, 720-21 (1987); *U.S. v. Nasser*, 476 F.2d 1111 (7th Cir. 1973); *U.S. v. Blok*, 188 F.2d 1019 (D.C. Cir. 1951).

[lviii] *Port Auth. Police Benv. Assn., Inc. v. Port Auth. of New York and New Jersey*, No. 15CV3526KMWRLE, 2017 WL 4403310 (S.D.N.Y. Sept. 29, 2017) (quoting *Ortega*, 480 U.S. at 715).

[lix] OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968, 2 EMPL. PRIVACY LAW § 8A:12.

[lx] 18 U.S.C.A. § 2511.

[lxi] *Id.*

[lxii] Daiquiri J. Steele, *Surveillance As Retaliation*, 59 GA. L. REV. 517, 564-65 (2025); *Noel v. Hall*, 568 F.3d 743 (9th Cir. 2009); *Allen v. Brown*, 320 F. Supp. 3d 16, 38 (D.D.C. 2018); Ifeoma Ajunwa, Kate Crawford & Jason Schultz, Limitless Worker Surveillance, 105 CAL. L. REV. 735, 749 (2017).

[lxiii] *See* Steele, *supra* note 11 at 566-67.

[lxiv] Ariz. Const. art. II, § 8.

[lxv] Cal. Const. art. I, § 13.

[lxvi] For example, Maryland law requires consent of both parties for an interception of a communication to be lawful. *See* Md. Cts. & Jud. Proc. Code Ann. § 10-402.

[lxvii] Va. Code Ann. § 18.2-167.1; W. Va. Code Ann. § 61-3-24c.