



By John M. Julius III and Eric A. Savage

Julius and Savage are attorneys with the national employment and labor law firm of Littler Mendelson. Both have over twenty years experience representing businesses in litigation and arbitration matters. They also provide counseling to clients on a wide range of employment matters including preparation and review of employee manuals and policies. Based in San Diego, Julius may be reached at 619-232-0441 or [jjulius@littler.com](mailto:jjulius@littler.com). Savage may be reached at his Newark, New Jersey, office at 973-848-4700 or [esavage@littler.com](mailto:esavage@littler.com).

## Privacy Rights Pitted Against Security

### When It Comes to Surveillance Cameras, Nothing Is Sacred

Recent developments in surveillance techniques, coupled with rapidly increasing attacks on individual privacy in the post-September 11th world, now present the hospitality industry with added opportunities to protect customers, employees, and profits from harm. Conversely, these new technologies also provide owners the prospect of destroying loyalty and trust.

Without a doubt, violence against restaurant, bar, and nightclub employees and guests is a very real threat; one that repeats daily. Pilferage, theft, and shrinkage eat into profits faster than George Foreman at an all-you-can-eat night. Low-cost, effective solutions have been a Holy Grail for operators. Adding bouncers and security personnel are generally effective deterrents to violence, but the personnel costs often offset any benefits.

Many restaurants are now investing in surveillance technologies in an effort to reduce the likelihood of assaults and shrinkage, minimize lawsuits, and increase guest safety. But along with relatively low cost and convenience comes decidedly sinister connotations—the loss of anonymity and comfort for guests and the potential invasion of employees' privacy rights.

#### Current and Future Use of Cameras

The hospitality industry initially utilized cameras solely for loss prevention. Budgets could be squeezed to install a camera focused on the cash register so absentee owners could theoretically track, when needed, register usage. For convenience stores or other facilities where thefts were prevalent, cameras would sometimes be trained to show people arriving and exiting, or reaching across the counter. Only recently have camera and software price points fallen to allow operators the flexibility and control to record in a visual manner just about everything that takes place in or near eating and drinking establishments.

But often the mere mention of “surveillance cameras” will cause reasonable people to cry in outrage. Although their faces are viewed constantly in real time by anyone nearby, there is something darkly Orwellian about the concept that some unknown person may be viewing that same image in some dark room somewhere or, worse, keeping a record of that person's presence indefinitely. Despite the rage, surveillance cameras

have become commonplace, and advances in technology promise to make them ubiquitous.

For restaurant owners, the simplest surveillance technique involves installing cameras fixed to view certain areas—registers, doorways, emergency exits, storage rooms, or areas outside doors. Modern equipment digitally records images, often operating only where movement triggers the recording device. Images can be kept indefinitely, but more likely will be automatically overwritten in thirty to ninety days, unless something happens to warrant saving the recording. More user-friendly add-ons include the ability to monitor the images through the Internet on a real-time basis and allow cameras to be manipulated remotely.

---

**Although modern technologies provide the hospitality industry with a variety of surveillance options in order to reduce shrinkage and increase customer safety and satisfaction, they are rife with dangers.**

---

The wave of the future in surveillance is to add biometric capability, normally face-recognition software. This technology allows users to record facial images of every person passing the camera, and then uses advanced software systems to compare the images to images stored on a server. If that person has previously been identified as someone involved in a fight or who bounced a check or who was aggressive with the wait staff, management can quickly take action—escort them out, have security focus on them, or refuse to serve them. Theoretically, innocent images are purged.

In an added twist, retailers can share databases of unwelcome customers so that the guy who got into a drunken brawl at Cheers won't be welcome at Gary's Olde Town Tavern. Fears that such databases will be sold to insurance companies or employers to ferret out heavy drinkers, or by divorce attorneys to see who a spouse really spends his or her time with may lead to legal

*continued on page 76*

restrictions, but for now your public image is fair game when used in this context.

## Restrictions to Camera Use

Surveillance cameras do have their limits, and legislation eventually responds to techniques that were scientifically impossible or financially impracticable just last year. Currently there are certain guidelines with which the hospitality industry must comply, lest its attempts to minimize risk and loss results in devastating lawsuits. Some are well-defined and inviolable; others reflect the lack of certainty due to technology advancing faster than the law.

**Expectation of Privacy.** The primary restriction on the use of cameras is that the cameras must not peer into or record areas where someone has a reasonable expectation of privacy. By extension, and often by statute, cameras must not be placed in restrooms or changing rooms.

Situations may arise where there is a serious need to place cameras in restrooms. Perhaps there is a genuine suspicion that illicit drug use is prevalent. Sometimes sexual activities take place behind stall doors (just think Carolina Panthers cheerleaders). When is it appropriate to use cameras to monitor such illegal conduct? The reality is that it never is.

Despite the obvious deterrent effect, companies should avoid placing cameras anywhere that there is an expectation of privacy, and restrooms and changing rooms should be at the top of that list. Attempts to circumvent this rule, either by directing the cameras away from urinals and stalls, or directly above stalls so that visualization of private areas is minimized, inevitably lead to more harm than benefit.

Vic's Tavern in Hilton Head, South Carolina, is a case in point. They actually caught vandals in the act after placing cameras in its restrooms in an attempt to prevent vandalism. The hooligans, later arrested, were recorded ripping the cameras off the wall (at least until the power cord was severed). Although Vic's won the battle, it may have lost the war after it was hit with a lawsuit from the men who had been caught, seeking \$800,000 for invasion of privacy and infliction of emotional distress. Although the intent was honorable, the method appropriate, and the immediate result triumphant, the potential that private images would be recorded raised the specter that lawsuits and increased expenses would follow.

Leading to a different, but equally real threat, is the potential abuse of the control of the cameras and related equipment. As an entity, it is unlikely that policies would be in place to abuse cameras. But individual employees often buckle into temptation to "redirect" cameras to record private activities, either out of personal voyeuristic pleasures or financial gain. Hooter's is still facing significant liability over recordings that one of its managers made of applicants changing into the restaurant's uniforms. Several casinos have come under fire after their security personnel used cameras to ogle at women, usually training cameras on their cleavage. Even where cameras are designed properly so as not to invade privacy, control of those cameras must be delegated to responsible, trained personnel.

**Recording Sound.** The other primary restriction on camera usage is that it must not record sound. It is a violation of the Federal Wiretap Act and many state laws to record people speaking. Even if it were accidental or the installer messed up, the owner/operator faces significant civil and criminal liability if a camera picks up and records an audio component. Precautions commensurate to those risks must be undertaken to eliminate such a possibility.

## Policies and Procedures

As a general guideline, and except where cameras are targeted on a short-term basis to eliminate a specific threat or problem, it is prudent to provide warnings to employees that all of their activities may be monitored. Corporate policies in writing should be prepared addressing employee privacy expectations as well as company expectations regarding on-site conduct. It is imperative to perform all surveillance in an evenhanded and nondiscriminatory manner.

If surveillance is implemented, the procedures employed and the fruits of the surveillance should be periodically reviewed. If the information gathered reveals personal information unrelated to the reason for the monitoring, and that information suggests no criminal violations, misconduct, or threat to the organization, ignore the personal information and do not reference it in any communications with the employee(s) in question.

If the information uncovered by monitoring or searching suggests actual or potential misconduct, act upon that information as though it had been reported by an employee. Periodically check to be sure that the video recording device records only video and not audio, thus guarding against the interception of a "communication" and the potential applicability of the Federal Wiretap Act.

Although beyond the scope of this article, companies must be aware that video surveillance potentially implicates employees' rights under the National Labor Relations Act, even if utilized in a nonunion setting. All employees, regardless of union status, have a right to meet and discuss issues involving hours, wages, and working conditions. Visual monitoring of employees' union activities has generally been found to constitute an unfair labor practice, and the threatened use of surveillance as a way of curtailing organizing efforts has been treated similarly.

If an employer knows that workers use a break room to discuss working conditions, placing cameras in that area could be viewed as an unfair labor practice and therefore subject to federal injunctive relief. If the employer is involved in collective bargaining, an employer's use of a hidden surveillance camera is a mandatory subject of bargaining.

Although modern technologies provide the hospitality industry with a variety of surveillance options in order to reduce shrinkage and increase customer safety and satisfaction, they are rife with dangers. Implementing the above guidelines will minimize and hopefully eliminate awkward consequences.

*EDITOR'S NOTE: Additional legal, safety, and security articles and training related to the hospitality industry may be found by visiting [www.hospitalitylawyer.com](http://www.hospitalitylawyer.com). ■*