METAL DETECTORS, VIDEO CAMERAS AND BOMB-SNIFFING DOGS: BALANCING HOSPITALITY WITH PRIVACY AND SECURITY

Jeff Karlin
Dunkin’ Brands, Inc.
Canton, MA

and

Natalma (“Tami”) McKnew
Fox Rothschild, LLP
Greenville, SC

October 16-18, 2019
Denver, Colorado

©2019 American Bar Association
# TABLE OF CONTENTS

I. PRIVACY UNDER ASSAULT? .............................................................................................................. 1
   A. What is Privacy Today? .............................................................................................................. 1
   B. Can the Law Protect Privacy? .................................................................................................... 2
      1. Eavesdropping/Audio Recordings ....................................................................................... 3
      2. Photographic, Video, and Visual Surveillance ....................................................................... 5
      3. Biometric Screening ................................................................................................................ 12
   C. Is It Enough? ............................................................................................................................ 12

III. FRANCHISOR/FRANCHISEE LEGAL ISSUES REGARDING SECURITY .......................... 13
   A. Premises Liability for the Criminal Acts of Third Parties ...................................................... 13
   B. Vicarious Liability Issues in the Security Arena ................................................................. 17

IV. CREATING A PRACTICAL BALANCE ................................................................................. 20

V. THE FUTURE ............................................................................................................................. 20
METAL DETECTORS, VIDEO CAMERAS AND BOMB-SNIFFING DOGS

In the interest of security:

* Your iPhone reads your face;
* Touchpads read your fingertips;
* Geo-trackers know where you are;
* Smart speakers are listening;
* Metal detectors are everywhere;
* Google Earth films your backyard; and
* Cameras are everywhere.

Does all this security come at too steep a price – the loss of privacy? The law weighs in on both sides of this issue, supporting security measures and supporting privacy, but where is the balance? These issues weigh particularly heavily in the hospitality industry, where the public expects both a safe, secure environment and a modicum of privacy. Can a host satisfy both demands? The problem was concisely described by Judge Posner in Shadday v. Omni Hotels Management Corp.\(^1\) In the interest of security, a host “cannot keep [its guests] under continuous surveillance – they would be unwilling to surrender their privacy so completely.”\(^2\)

This paper will explore the intersection between the often dueling public expectations of security and privacy. We will tackle the security and privacy implications of methods such as eavesdropping, cameras, visual monitoring, and biometric screening; address potential franchisor vicarious liability for franchisee’s actions in this context; and explore the potential for achieving a practical balance between security and privacy in the franchise arena.\(^3\)

I. PRIVACY UNDER ASSAULT?

A. **What Is Privacy Today?**

“Protecting” privacy depends on one’s view of what privacy is in the first place. Each person’s expectation of privacy varies, depending on the situation, the setting, the people

---

1 477 F.3d 511 (7th Cir. 2007).

2 In the *Shadday* case, the Court considered whether existing cameras and a full crew of security staff could have prevented a rape of one guest by another. The Court concluded that it could not.

3 Just as important as what this paper will address is what it will not. This paper does not address cyber or electronic security, the California Consumer Privacy Act or the European Union’s General Data Protection Regulation (“GDPR”), Due Process in criminal situations, security and privacy in employment, franchisee background checks, or security and privacy in the context of discovery disputes. Several of these topics are addressed in other sessions. In addition, please note that the views and opinions expressed in this article are solely those of the authors and do not necessarily reflect those of their employers.
involved, and the topic. The ubiquity of social media such as Instagram, Facebook, dating sites, and too many other platforms to count throws into doubt even the basic legal assumption that people have a right, in the European parlance, “to be forgotten.” Can any right of privacy survive the intrusive reality of today’s world – let alone what future technologies may bring?! In litigation against Facebook stemming from the Cambridge Analytica scandal, Facebook’s lawyers seemed to suggest to Federal Judge Vince Chhabria that privacy as a concept is outdated, asserting that the expectation of privacy in the cyber age is “a brand-new right of privacy.”

Another commentator, Maciej Ceglowski, describes Facebook’s approach as attacking the very existence of personal privacy. The accepted definition of privacy, he writes, “is not adequate for the new reality of ubiquitous, mechanized surveillance”. He proposes consideration of another form of privacy, what he calls “ambient privacy,” based on “the understanding that there is value in having our everyday interactions with one another remain outside the reach of monitoring, and that the small details of our daily lives should pass by unremembered.” But is our system of laws in the United States sufficiently nimble to protect ambient privacy or the right to be forgotten?

The law’s interaction with traditional notions of privacy is inconsistent and unpredictable. In classic legal fashion, whether a right of privacy attaches at all is determined in an “all the facts and circumstances” test that almost never results in a reliable bright line rule. The legal wrestling matches reported below certainly don’t suggest the parameters of an achievable balance between security and privacy, but instead present well-intentioned ad hoc responses based on largely subjective views of individual situations.

B. Can the Law Protect Privacy?

Personal privacy is protected against intrusion by non-governmental actors in many state Constitutions, in common law, and by federal and state statutes. Constitutions and the common law typically apply to a broad range of situations, while statutes are usually more narrowly focused. These are the public’s first line of defense against privacy intrusions.

Unlike the federal Constitution, the privacy provisions of some state Constitutions apply to non-governmental, as well as governmental, actors. The California Constitution is one. The California Constitution, Art. I, Sec. 1 provides: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting privacy, and pursuing and obtaining safety, happiness and privacy.”

Common law invasion of privacy as a tort claim is widely recognized. “The law relating to a protectable ‘right to privacy’ is an American invention, developing over a period of approximately the last one hundred years. The law in its present form was authored almost entirely by Professor William Prosser, who, in a 1960 law review article in the California Law Review, opined that the right of privacy gave rise not to one, but to four different tort actions. These four torts, sometimes called ‘Prosser's Four Torts of Privacy,' found their way into the


5 Id.

6 See, also, the Constitutions of New Mexico (Art. 2, Sec. 10) and Indiana (Art. I, Sec. 11). The privacy provision in the Arizona Constitution, art. 2, Sec. 8, applies to state actors only. Onuigbo v. Early Warning Systems, LLC, No. 1 CA-CV 13-0563, 2015 WL 161110 (Ariz. App. Jan. 13, 2015).
The application of Constitutional principles and the tort of invasion of privacy in its various forms, as well as statutory protections, are discussed in the cases below.

1. **Eavesdropping/Audio Recordings**

Statutes prohibiting or limiting audio recordings are among the most common and most evolved approaches to privacy protection. The operative language of these statutes varies in whether recordings are absolutely prohibited and whether one or all participants are required to have knowledge of the recording. Otherwise, these statutes are fairly consistent.

The full range of available causes of action is evident in a franchise case more than four decades old. *Moore v. Telfon Communications Corp.*\(^8\) applies state, federal and common law approaches to eavesdropping in the context of a franchise dispute. The franchisor’s CEO Anderson, recorded conversations with the franchisee Moore to demonstrate extortion by Moore, which allowed the franchisor Telfon to terminate Moore’s franchise agreement. The recording was Anderson’s security against Moore’s extortion, but Moore viewed it as a private conversation.

The franchise at issue was the Columbia School of Broadcasting. Moore wanted to purchase the NYC franchise, but it was too expensive, so he instead opted for the Connecticut franchise. Moore then ignored the territorial limitations of his Franchise Agreement and extended operations to NYC. This was apparently only one of the problems the franchisor had with the way Moore was operating the franchise, prompting discussions between Moore and Anderson, Telfon’s CEO. During the course of these discussions, Moore threatened to file “a multi-million dollar antitrust suit” unless Anderson bought out his franchise for at least $1 million. Anderson recorded seven of these conversations to document the extortion and then terminated the Franchise Agreement. Moore sued, alleging violations of federal and California eavesdropping statutes and common law invasion of privacy. A jury found for the franchisor, and the Ninth Circuit affirmed on three grounds:

1. The Electronic Communication Privacy Act (“ECPA”)*\(^9\)* prohibits the willful interception of any wire or oral communication, but permits one party to record another when he is acting out of legitimate desire to protect himself, and not for the purposes of committing a crime, or a

---

\(^7\) *People for the Ethical Treatment of Animals v Bobby Berosini, Ltd.*, 111 Nev. 615, 628-629, 895 P.2d 1269 (1995).

\(^8\) 589 F.2d 959 (9th Cir. 1978).

tortious or injurious act.\textsuperscript{10} The franchisor’s actions, designed to preserve evidence of extortion for later use in terminating the franchise relationship, were permissible.\textsuperscript{11}

(2) California Penal Code Sec. 632 prohibits intentionally recording a confidential communication without the consent of all parties. However, Sec. 633.5 permits one party to a confidential communication to record a communication for the purpose of obtaining evidence reasonably believed to relate to the crime of extortion, an exception the evidence supported in this case.

(3) Under the California common law right to privacy, Anderson’s actions were not an unauthorized or unwarranted intrusion into Moore’s personal affairs, because (a) there was no right of privacy in the actions; and/or (b) Anderson was permitted to record and disclose the conversation.

A variety of state eavesdropping statutes function similarly to the ECPA. The first example, \textit{Mills v. PPE Casino Resorts Maryland, LLC},\textsuperscript{12} clearly demonstrates the security-privacy balance issue. A casino guest was annoyed when security officers ejected him from the premises and “surreptitiously record[ed]” his oral communications with the officers in an “enclosed, not-publicly accessible location of the Maryland Live! Casino.” The casino alleged a violation of Maryland’s Wiretapping and Electronic Surveillance Act, Jd. Code, Cts. & Jud. Proc. Sec. 10-401 \textit{et seq}. The recorded discussion took place in a secured back hallway of the casino, but was caught on casino video surveillance. Mills obtained a copy of the casino tape, merged it with his iPhone audio recording, and posted it on You Tube.

The Court explained that Section 10-410 of the Maryland Act prohibits willful interception, disclosure and use of impermissibly intercepted communications and provides a private civil remedy for violations. Under the Maryland Act, oral communications are defined as “any conversation or words spoken to or by any person in private conversations.” What constitutes a “private conversation” is not statutorily defined, but courts have defined it by “(1) whether the individual had an actual, subjective expectation of privacy with regard to the statements and (2) whether that expectation is one that society is prepared to recognize as reasonable.”\textsuperscript{13} In this case, the court concluded, security personnel had no reasonable expectation of privacy, even if they subjectively believed the conversation was private, due to the presence of “up to” nine people in the hallway. While they protected the casino’s security, the officers could not protect their own privacy.

The California and Illinois eavesdropping statutes likewise depend upon whether the conversants had a reasonable expectation of privacy at the time of the recording. \textit{People v. Newton}.\textsuperscript{14} Under the California law, “Whether a person’s expectation of privacy is reasonable may depend on the identity of the person who has been able to observe or hear the subject interaction. The presence of others does not necessarily make an expectation of privacy


\textsuperscript{13} 2017 WL 1862474 at *4 (internal quotes removed).

\textsuperscript{14} 42 Cal. App. 3d 292, 296, 116 Cal. Rptr. 690, 693 (Ct. App. 1974).
objectively unreasonable, but presents a question of fact for the jury to resolve." In Illinois, policemen found themselves in a situation similar to the Maryland Live! casino security personnel in *People v. Beardsley*, implicating the state’s eavesdropping law. Beardsley was arrested for speeding, but an eavesdropping charge was added when he recorded the conversation of two officers while they transported him to the law enforcement center. Because the officers’ conversation was in his presence, the court reasoned, there was no eavesdropping.

Other states have similar laws. Under the Pennsylvania statute, for instance, it is illegal to record private conversations, even in a public space. “To determine whether one’s activities fall within the right of privacy, we must examine: first, whether [the plaintiff] . . . exhibited an expectation of privacy; and second, whether that expectation is one that society is prepared to recognize as reasonable. To satisfy the first requirement, the individual must demonstrate that he sought to preserve something as private. To satisfy the second, the individual’s expectation must be justifiable under the circumstances.”

The Florida eavesdropping law, likewise turns on whether there was a reasonable expectation of privacy; where parties might be expected to be overhead, there is no reasonable expectation of privacy. “A reasonable expectation of privacy under a given set of circumstances depends upon one’s actual subjective expectation of privacy as well as whether society is prepared to recognize this expectation as reasonable.”

2. **Photographic, Video, and Visual Surveillance**

The laws governing the limits of visual security are more fragmented than those addressing eavesdropping and audio recordings. There is currently no federal corollary to the ECPA for video recordings. State statutes and common law often differentiate between direct surveillance and camera/video surveillance. The challenge of balancing security with privacy is especially acute in video or photographic surveillance.

*Direct Surveillance*

A long history of cases establish the permissible bounds of private investigative surveillance. As the cases below demonstrate, non-invasive surveillance typically does not

---


16 115 Ill.2d 47 (Ill. 1986).


21 Fla. Stat. Ch. 934.03.

offend an individual’s right to privacy, especially when a host has managed a guest’s expectation of privacy.

Again and again, courts have rejected claims of invasion of privacy where private investigators have engaged in routine surveillance. One example is Furman v. Sheppard, in which the plaintiff sued a private investigator who worked for defense counsel in a personal injury lawsuit who allegedly trespassed onto the property of a private club to videotape the plaintiff sailing his yacht. The intrusion, according to the plaintiff, invaded his privacy. The Court identified the particular variety of invasion – the intentional intrusion upon the solitude or seclusion of another or his private affairs and concerns that would be highly offensive to the reasonable person. Here, there was no violation. There was no liability for observing the plaintiff in public places, the Court held, since the plaintiff was not in seclusion. “If surveillance is conducted in a reasonable and non-obtrusive manner, it is not actionable,” the Court wrote, citing cases from Oregon, Pennsylvania and Georgia.

The same principal was decisive in Creel v. I.C.E. & Associates, Inc., in which an investigator secretly videotaped the plaintiff Creel playing the piano during a church service. The Court rejected the plaintiff’s claims for invasion of privacy under Indiana law. The Court also described the variety of invasion of privacy as invasion by intrusion, in terms similar to those in Curry v. Whitaker. But the claim failed for two reasons: first, Creel didn’t know of the taping and, more importantly, she was not alone or secluded during the taping.

Another example of the same principle is Hall v. InPhoto Surveillance Co., in which a hospital hired the defendant surveillance company in anticipation of Hall’s malpractice claim. The defendant used video surveillance, even going onto Hall’s rural property. Hall claimed that InPhoto trespassed to photograph her through the bedroom window. The defendant’s agent said he never could get the video camera to work, took no photographs, didn’t trespass, and didn’t look in any bedroom windows. Hall admitted she discovered the defendant’s actions not because she saw any photographs being taken, or anyone looking into windows, but because she saw the defendant’s agent across the road. The Court acknowledged that Illinois recognizes a right to privacy, but queried whether Illinois specifically recognizes a cause of action for intrusion upon seclusion of another. The Court didn’t have to decide the issue, however, as there was no factual support for the claim. Summary judgment for the defendant was affirmed.

While Furman and Creel do not involve security surveillance per se, the principle of reasonable direct surveillance should govern the actions of private security personnel, such as the officers involved in the Mills and MRE cases, who routinely patrol hospitality venues.

The department store involved in Lewis v. Dayton Hudson Corp. took a different approach to direct security. The store balanced its need to guard against theft against a patron’s

24 744 A.2d at 586.
right of privacy by reducing the patron’s expectation of privacy. The plaintiff, an off-duty policeman, carried a concealed firearm, which was seen over a store surveillance system as he was making use of the changing room. Lewis sued the store, alleging invasion of privacy by intrusion on seclusion or solitude under Michigan law. But whatever expectation of privacy Lewis might have had in a fitting room, the Court concluded, was extinguished by signs advising of surveillance. Had the notices not been present, the Court suggested, a violation may have been evident. Generally, “One who uses a dressing room is entitled to a modicum of privacy.”

It is easy to describe the cases above as tipping between security and privacy. Private investigators surveil as security against legal claims, and the department store balances security against theft and their patrons’ privacy expectations. Tort claims handily and reasonably managed the two interests. Extreme forms of direct surveillance also implicate an individual’s personal expectation of both privacy and security, and but may trigger harsh judicial responses that protect privacy more aggressively.

Highly public, highly intrusive surveillance may give rise to common law claims of stalking or “hounding” (in the parlance of the RESTATEMENT (SECOND) OF TORTS). The sale of a business gave rise to a hounding claim in Summers v. Bailey. Summers bought a grocery store from Bailey, operated it for a while, then in connection with a bankruptcy decided to sell it to another person. Bailey didn’t approve of the sale and harassed and threatened Summers and the potential buyer, causing the sale to fall through. Summers claimed invasion of privacy, a claim dismissed by trial court, but reversed by the Eleventh Circuit.

Bailey’s surveillance of Summers met the definition of hounding. He followed her, displayed a hand gun, parked for hours outside the store, told customers he wanted her out of the store, and parked near her home. Upholding Summers’ claims, the Court tracked the genesis of Georgia privacy laws to 1905, explaining that personal liberty means not only freedom from physical restraint, but the right to be left alone. Now, the Court explained, invasion of privacy embraced the Prosser four “loosely related but distinct torts,” including the tort of intrusion, evident in these facts. Bailey’s conduct, which suggested not only a physical intrusion onto Summers’ residential property, but an “offensive, frightening and unreasonable surveillance of her private affairs” stated a cognizable hounding claim.

Franchisors, franchisees and individuals could find themselves victims of political hounding, as in Huntingdon Life Sciences, Inc. v. Stop Huntingdon Animal Cruelty USA, Inc. The case arose from extreme picketing and related actions by PETA group members in front of the home of one of Huntingdon’s management level employees. PETA’s actions included dumping red paint on the employee’s driveway and on her husband’s car, puncturing tires,

---

29 339 N.W.2d at 859-860. To the same effect, Gillett v. State of Texas, 588 S.W.2d 361 (TX App. 1979), regarding the effects of posted notice.

30 Of course, many states have enacted criminal and civil statutes proscribing stalking, some of which provide for a civil recovery. Those are beyond the scope of this paper.

31 55 F.3d 1564 (11th Cir. 1995).

32 Id. at 1566.

33 Id. at 1567.

painting “HLS SCUM on the garage”, ringing her doorbell repeatedly, setting off an alarm, and standing at the end of the driveway shouting slogans through megaphones. Some of the incidents were filmed and posted on PETA’s website.

The employee and Huntingdon sued PETA for trespass and harassment under state statute, but for purposes of this paper the claim of invasion of privacy is more relevant. The trial court granted preliminary injunctive relief, finding cause to believe that PETA representatives had “engaged in, are engaging in, and are about to engage in acts, practices, and conduct that constitutes violations of” the employee’s right to privacy.35 That decision was affirmed by the Appellate Court, which explained that “Peace of mind is now recognized as a legally protected interest, the intentional invasion of which is an independent wrong, giving rise to liability without the necessity of showing the elements of any of the traditional torts.”36 The Court also affirmed preliminary relief on the basis of the California Constitution, Art. I, sec. 1 which condemns governmental and non-governmental actions in violation of privacy. The requirements of proof in the Constitutional setting are predictably similar to the common law privacy torts: intrusion into a private place, conversation or matter, in a manner highly offensive to a reasonable person. Specifically, the plaintiff must demonstrate that the defendant penetrated some zone of physical or sensory privacy, where the plaintiff had a reasonable expectation of seclusion or solitude in the place, conversation or data. The expectation need not be of complete or absolute privacy, but should be evaluated in the context of the identity of the intruder and the nature of the intrusion. Offensiveness is based on facts and circumstances, including degree, setting of intrusion, and the intruder’s motives and objectives. Based on these factors, it was not difficult for the Court to find that the employee demonstrated a likelihood of success on the merits of her privacy claims. Huntingdon, however, lacked standing to pursue tort claims committed against its employee.

As in the case of many hounding cases, the Summers and Huntingdon cases demonstrate a convergence of one person's rights of privacy and need for security, in the face of a competing right of the actor to express himself or herself. Huntingdon is noteworthy for what it says about the corporate entity that was the primary target of PETA's action: although its interests were evident, it had no cognizable, protectable privacy interest. A right of privacy is just that – private to an individual human person.

Video and photographic surveillance

Video and photographic surveillance is more often a specific target of state statutory limitation than direct surveillance. In Pla-Fit Franchise, LLC (d/b/a Planet Fitness) v. Pla-Fit Franchise, LLC,37 the surveillance was not performed by the franchise; rather, a gym member secretly videotaped other members in the franchised gym’s tanning rooms. Significantly for this paper, the case involved both the scope of premises liability and the host’s obligation to protect privacy. Victims of the surveillance sued the franchisee and franchisor, neither of which was ultimately found liable for negligence or premises liability.

To demonstrate negligence, the Court explained in Pla-Fit, a plaintiff must allege a defendant’s duty, breach of that duty, and injury proximately caused by the breach. But under

35 Id. at 1243.
36 Id. at 1259.
Illinois law, a possessor of land generally does not have a duty to protect invitees from criminal or tortious acts committed by a third party. The exception is where there is a special relationship between the parties, such as common carrier and passenger; innkeeper and guest; custodian and ward; and business invitor and invitee. The Court concluded, however, that the relationship between the franchisor and the franchisee’s invitees was not a special relationship within the meaning of the exception; the franchisor did not control activities on the land, but merely allowed franchisee to use its mark. In addition, the Court held that neither the franchisor nor the franchisee was liable to the guests because Illinois requires physical harm as an element of the claim. Here, the damages sought by the guests were limited to emotional distress.

Photos of a gambler, shared by a casino with related venues, gave rise to the gambler’s claims in M & R Investment Co. v. Mandarino. The basic facts of the case are not surprising for Nevada. It involved a gambler who won big and had his winnings confiscated by casino personnel, who arrested him, photographed him and distributed his photo to other casinos. Based on his attire, which included dark glasses, a false mustache, and slicked down hair, the Court concluded that the gambler had no expectation of privacy. This case is perhaps unique in its implication that in extreme situations, one’s manner of dress (especially if the intent of the clothing is to disguise one’s identity) may trump any expectation of privacy.

Video surveillance was the issue in Soliman v. The Kushner Companies, Inc. et al. The defendant owned a building in which surveillance monitors were installed by the landlord. The plaintiff was a tenant’s employee. Because a door was left open that was usually closed and locked, a tenant’s employee discovered that there were video monitors and recording equipment concealed inside smoke detectors in the employees’ bathrooms. There was disagreement about whether the stalls, or activities in the stalls, could be observed, but activities in the common areas near the sinks were recorded. The defendant claimed that the devices were designed to provide security and deter vandalism, but the Court observed that even a good faith motive couldn’t destroy the plaintiff’s breach of privacy claims under the New Jersey Constitution, statute, and common law. Even if cameras didn’t catch activity in stalls, the Court commented, the common area cameras could have observed users engaged in personal grooming, or even in undress. The plaintiffs had a reasonable expectation of privacy in restroom, including common areas targeted by the cameras. On these facts, the case survived the defendant’s motion for summary judgment.

As the Soliman Court explained, the New Jersey Constitution, Art. 1, par. 1 affords rights to privacy and redress for violations by actors, whether public or private, and the facts of the case supported a claim for invasion of privacy based on Constitutional rights of privacy. Those rights encompass “the right of an individual to be . . . protected from any wrongful intrusion into his [or her] private life which would outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibility.” The common law tort of “intrusion on seclusion,” based on the RESTATEMENT [SECOND] OF TORTS, Sec. 652B, was also implicated. It imposes civil liability on “one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a

40 77 A.3d at 1223 (citations omitted).
reasonable person.” The Court echoed the Prosser Four Torts of Privacy history, and pointed out that the privacy interest involved is freedom from intrusion or prying into inherently non-public areas where there is a reasonable expectation of privacy “str[iking] at the personhood of [the] plaintiff.” Compensatory damages for personal hardships caused by the invasion of privacy, similar to those described in N.J.S.A. 10:5-3, were recoverable.

An employer who installed a video camera to identify the employee accessing pornographic sites on the internet impermissibly invaded his employees’ privacy, according to the Court in Hernandez v. Hillsides, Inc, although the camera operated only at night and did not capture images of the plaintiff’s activities.

The Hernandez Court identified two sources of privacy protection: the common law tort of intrusion and the state Constitution. The intrusion must be highly offensive, an inquiry that involves a “policy determination” based on the circumstances of the intrusion. Even with photo and recording devices, the Court commented, “California law provides no bright line on [offensiveness]; each case must be taken on its facts.” The Court described California Constitutional standards in similar terms.

The parties took neighborhood spats to another level in Curry v. Whitaker. A homeowner installed video cameras focused on common areas and on his neighbor’s property as a security measure. The videotaper sued his neighbor for vandalism, and the subject of the taping responded with a complaint for invasion of privacy. The videotaped neighbor asserted (a) invasion of privacy by intrusion, (b) invasion of privacy by false light; and (c) intentional

---

41 Id. at 1225 (emphasis added). The Court distinguished Villanova v. Innovative Investigations, 420 N.J.Super. 353, 360, 21 A.3d 650 (App. Div. 2011), in which the defendant installed a GPS tracking device on the plaintiff’s car without his knowledge. In the absence of evidence that the vehicle was driven into a private or secluded place that was out of public view, there could be no claim for invasion of privacy.

42 See Section II B above.

43 77 A.3d at 1227 (citation omitted).

44 Id. at 1228. Soliman’s privacy claims under N.J.S.A. 2A:58D-1a also survived. The statute provides civil liability for one who, without license or privilege photographs, films, videotapes or otherwise reproduces in any manner, the image of another person whose intimate parts are exposed or who is engaged in sexual activity without consent and under circumstances in which a reasonable person would not expect to be observed.

45 47 Cal. 4th 272, 211 P.3d 1063 (2009).

46 Id. at 1073.

47 The California Constitution provides a limited right of action against both private and governmental entities upon proof of the defendant’s intentional intrusion on plaintiff’s legally protected privacy interest in conducting personal activities without observation, intrusion or interference. The scope of a legally protected privacy interest is determined by established social norms, common law or statute, against a plaintiff’s reasonable expectation of privacy. Whether there was an opportunity to be notified and consent to the intrusion in advance is also pertinent. Finally, the plaintiff must demonstrate that the intrusion is so serious in nature, scope and impact as to amount to an egregious breach of social norms. The defendant may show justification (which need not be compelling) for the intrusion as a defensive element in the balancing test by which an alleged invasion of privacy is determined. The defendant can also show that less intrusive alternate means were not reasonably available. Also considered is whether the intrusion was limited, so that nothing confidential was gathered or disclosed. However, the Court admonished, these defensive moves may not be available in the “rare case” where a “fundamental” right of personal autonomy is involved.

infliction of emotional distress. All the claims failed. Invasion of privacy by intrusion, the Curry Court explained, requires an intrusion that is offensive or objectionable to a reasonable person. The conduct here did not rise to that level.

Oddly, New York recognizes no general right of privacy, a situation that leads to rather bizarre results. Stuyvesant Town-Peter Cooper Village Tenants’ Ass’n v. Metropolitan Life Ins. and Annuity Co.49 arose from landlord Met Life’s announcement that it would replace an old security system with an electronic card system. The new system would require periodic renewal and would include each person’s photo, which would be placed on the entry card and in the system so that security guards could check as people come in. The tenants sued on a number of theories, including invasion of privacy. The Court makes short shrift of the claim, simply stating, “In New York, there is no common law right of privacy.”50

The absence of an acknowledged right of privacy figured prominently in Dana v. Oak Park Marina, Inc.51 In that case, a marina in New York found itself in litigation over video surveillance in the ladies’ rest room. The Court explained that while the marina owed no common law duty as an innkeeper to protect the plaintiff’s privacy, it did owe a statutory duty under General Business Law Sec. 395-b(2) to refrain from installing a videotape camera in the restroom. The purpose of the law, the Court explained, is to protect persons who are surreptitiously viewed while lawfully utilizing the facilities covered by the statute. The statute prohibits the installation of cameras in “any fitting room, restroom, toilet, bathroom, washroom, shower, or any room assigned to guests or patrons in a motel, hotel or inn” for the purpose of surreptitiously observing the interior of those facilities. The Court held in Dana, however, that the New York statute afforded no private right of action; but violations of the statute could constitute the reckless or negligent infliction of emotional distress. THE RESTATEMENT (SECOND) OF TORTS, Section 46 describes the elements of the tort as extreme and outrageous conduct, with the intent to cause or disregard of a substantial probability of causing severe emotional distress, and severe emotional distress resulting from the conduct. Finding the essential elements of the tort present here, the Court restored the plaintiff’s claims.52

Some of the litigants in these cases found a reasonable, workable balance between security and privacy; others did not. Among the key balancing factors were the degree of intrusion, the expectation of privacy, and the need for security. Where the security purpose appeared to be attenuated, a greater respect for privacy was evident. Conversely, where the need for security was greater, a more uncomfortable intrusion on privacy was permissible. But overall, these cases advise caution – a consistent, predictable approach to achieving security while respecting privacy is not apparent.

49 4 Misc.3d 1030(A), 2014 WL 2250918 (Sup. NY, June 29, 2004).
3. **Biometric Screening**

Illinois is a leader in emerging legislative attention to biometric screening, chiefly through its enactment of the Biometric Information Privacy Act (“BIPA”). As the Court explained in *Rosenbach v. Six Flags Entertainment Corp.*, BIPA codifies the principle that “individuals possess a right to privacy in and control over their biometric identifiers and biometric information.” As defined in the Act, a “biometric identifier” is “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” The Act imposes duties on private entities regarding collection, retention, disclosure and destruction of a person’s biometric identifiers or biometric information. Failure to comply with one of the statute’s requirements “constitutes an invasion, impairment, or denial of” a person’s statutory rights. The Court importantly adds, “[o]ther than the private right of action authorized in Section 20 of the Act, no other enforcement mechanism is available.”

*Rosenbach* involved a teenager whose fingerprint was taken in connection with a season pass to Six Flags. His parents sued Six Flags for non-compliance with BIPA. Prior BIPA case law, including *Norberg v. Shutterfly, Inc.*, *Aguilar v. Rexnord, LLC*; and *Rivera v. Google*, had held that proof of actual damage was required. In *Rosenbach*, however, the Illinois Supreme Court concluded otherwise. Actual damage is not a required to allege a violation of the Act; mere non-compliance with BIPA states an actionable claim.

Illinois may be a leader, but other states may not be far behind. The National Conference of State Legislatures reports that at least 26 state legislatures addressed biometric data bills this year, according to Rich Ehisen, managing editor of State Net Capitol Journal. Legislation was enacted in Arkansas, New York and Washington, and bills were pending in California, Minnesota, New Hampshire, Massachusetts, New Jersey and Rhode Island. Even some cities, including San Francisco, California, Somerville, Massachusetts, and Berkeley, California, have banned or regulated the use of facial recognition software. Obviously, not all the pending bills will be enacted, and others may be introduced in the future. But the flurry of activity reflects legislative concern about the effects of biometric screening on personal privacy.

**C. Is It Enough?**

As reflected in the cases cited above, US privacy laws have developed in a piecemeal fashion, usually reactively, and were generally enacted in a pre-cyber era. Do they provide an effective response to the rapid development and deployment of evermore sophisticated security

---

53 2019 IL 123186 at *4.

54 740 ILCS 14/1 et seq.

55 2019 IL 123186 at *6 (Jan. 25, 2019).

56 Id. at *7.

57 152 F. Supp. 3d 1103 (N.D. Ill. 2015).


60 In *Rottner v. Palm Beach Tan, Inc.*, 2019 II App. (1st) 180691-U (March 4, 2019), the appellate court cited *Rosenbach* and held that actual damage need not be alleged to recover statutory liquidated damage.
devices? In the franchise context, will franchisees and franchisors be expected to deploy new security measures despite the muddied minefield of privacy laws – and how will they do that?

III. FRANCHISOR/FRANCHISEE LEGAL ISSUES REGARDING SECURITY

A. Premises Liability for the Criminal Acts of Third Parties

Having outlined the major concepts at play to the limitations business owners have with respect to privacy boundaries, this paper will now explore the length and breadth of a franchisee’s duty to protect their customers and potential customers (along with their employees) from harm. There is an underlying tension and interplay here, i.e., whether business owners can go so far in their efforts to keep others safe that they end up violating someone’s privacy rights. In other words, where does the duty to protect end and the obligation to respect another person’s privacy interest begin? Adding to the complexity is the overarching issue of what sort (if any) of direct or vicarious obligations franchisors have to the franchisee and/or employees.

A **HUGE** caveat to note. Premises liability is a creature of state law, each state has its unique law, and we have not attempted here to provide anything more than an overview of the general principles. That said, there are some terrific resources on these issues on the Web and elsewhere, such as:


Unlike the uncertainties associated with privacy issues, the law regarding physical security is fairly well-developed, even in the franchise context. Most of the privacy issues discussed above relate to consumer interactions with physical properties that are owned or controlled by business owners. To establish negligence in a premises liability action, an individual must prove three elements: 1) a duty of care owed by the property owner to the individual; 2) the owner’s breach of that duty by a negligent act or omission; and 3) damage proximately resulting from the breach of duty. The scope of the duty of care owed by a property owner to an individual in a premises liability action, if any, is determined based upon the status or classification of the person injured at the time of his or her injury. Visitors to property are classified in several ways, including:

- **Business invitees**: who enter a business property to conduct business with the property’s occupier;

- **Public Invites**: who enter onto (or into) a property owned by someone else for a non-business purpose for which the property is held open to the public; and

- **Licensees**: individuals who are invited onto a property as social guests.

That “other relationship” which may end up imposing a duty can include those between a business owner and its customers. And in fact, although some courts pay lip service to the
notion that business owners are not the “insurers” of a business invitee’s safety, in reality, they impose a heightened duty on businesses to protect their customers from all manner of harms. As such, it is widely recognized that business owners and their invitees are in a “special relationship.” Thus, despite the fact that the common law does not usually impose a duty on anyone to protect a victim from the criminal acts of third parties, that is not the case with respect to businesses vis-à-vis their customers. Instead, it is well-settled that business owners have broad duties to protect their invitees not only from their own acts or omissions, but those of third parties—including criminal acts that they had no part in. The RESTATEMENT (SECOND) OF TORTS, Section 344 provides, for example, that

[a] possessor of land who holds it open to the public for entry for his business purposes is subject to liability to members of the public while they are upon the land for such a purpose, for physical harm caused by the accidental, negligent, or intentionally harmful acts of third persons or animals, and by the failure to the possessor to exercise reasonable care to:

(a) discover that such acts are being done or are likely to be done; or

(b) give a warning adequate to enable the visitors to avoid the harm, or otherwise to protect them against it.

Comment (f) to Section 344 is also instructive as to the scope of the business owner’s duty to invitees:

[A business owner] may, however, know or have reason to know, from past experience, that there is a likelihood of conduct on the part of third persons in general which is likely to endanger the safety of the visitor, even though [the owner] has no reason to expect it on the part of any particular individual. If the place or character of his/her business, or his/her past experience, is such that [the owner should reasonably anticipate careless or criminal conduct on the part of third persons, either generally or at some particular time, he/she] may be under a duty to take precautions against it, and to provide a reasonably sufficient number of servants to afford a reasonable protection.

Over the years, the courts have simplified these standards to impose a duty on businesses to protect invitees “from imminent criminal harm and reasonably foreseeable criminal conduct by third persons.” Whether a criminal act is considered “foreseeable” or not is judged on various fact-based tests that focus on the “totality of the circumstances” regarding prior criminal acts in and around the property in which the incident took place. In other words, the courts have traditionally focused on whether the criminal act in question is similar in “degree and form” to prior crimes and the physical distance between the prior crimes and the crime at


63 See RESTATEMENT (SECOND) OF TORTS § 314; RESTATEMENT (SECOND) OF TORTS § 315.

64 Nivens v. 7-11 Hoagy’s Corner, 133 Wash.2d 192, 943 P.2d 286, 292-93 (1997).

issue. However, the courts in some states have commented that a more modern trend is that the foreseeability determination is “not absolutely dependent upon notice of prior crimes of a similar nature occurring on or near the premises, but may also be determined from all of the circumstances present.” And since every case presents different circumstances, of one kind or another, things can get quite deep into the weeds, quite quickly.

It is important to note that, despite the factual nature of the foreseeability standard, it is considered a legal issue because the court must first determine whether the business owner had a legal duty to the injured party. That has significant implications in how these sorts of premises liability cases are litigated since legal issues are decided by the judge, while the factual issues are determined by the finder of fact (which in many cases is the jury). However, where the legal duty determination is fact-dependent, many courts take the position that the duty issue cannot be resolved by the judge until the jury makes all of its factual findings. That can make summary judgment a more difficult (but not impossible) proposition and has the potential to make litigation in this area a lot more expensive.

In Corinaldi v. Columbia Courtyard, Inc., the parents of an invitee of a hotel guest (i.e., a guest of a guest) sued the hotel’s owner (a franchisee) after their teenage son was shot and killed during a party held in two adjoining rooms on the premises. The decedent was killed by a bullet that was fired through the wall of one room and into the other room where he was standing. The trial court granted summary judgment for the hotel owner on two grounds. The first was that while the hotel guest himself may have been a business invitee, the guest’s guest did not have a “special relationship” with the hotel owner and thus the owner had no heightened duty to the decedent to whom he owned only reasonable care. In turn, the trial court found that the hotel owner was not liable under the standard of reasonable care because the exercise of such care “would not have prevented the unforeseeable act of a … shooting through a closed door at persons unknown on the other side.”

The appellate court reversed and remanded. As a preliminary matter, the Court explained that there were three possible factual scenarios in which a victim can seek to hold a property owner liable for injuries inflicted by the intentional criminal act of a third person. The first is when the assailant entered the premises without the owner’s invitation or prior knowledge. In those cases, the appellate court commented, the legal claim is “based on an

---


69 Walpert, Smullian & Blumenthal, P.A. v. Katz, 361 Md. 645, 762 A.2d 582, 608 (2000) (holding that whether contractual privity existed between the parties, giving rise to a legal duty on the part of one of them, was a necessary preliminary determination to be made by the jury).


71 Id. at 487.

72 Id. at 488.
asserted duty to eliminate conditions that contributed to the criminal activity, such as providing security personnel, lighting, locks, and the like. Therefore, the duty imposed on the property owner is based on the owner’s prior knowledge of conditions on and surrounding the property, including “prior similar incidents.” The second factual scenario is when the property owner has some prior knowledge of the assailant’s past actions and, presumably, that the assailant was or was likely to be on the premises at some point. And the third scenario identified by the court was when the claim is based on the allegation that the property owner had actual knowledge of events “occurring on the premises, prior to and leading up to the assault, which made imminent harm foreseeable” regardless of whether the property owner had any knowledge of prior criminal acts on the property or in the surrounding area.

The appellate court found that the case presented a situation that fell squarely into the third scenario. It then dove into an examination of the facts relating to what the hotel owner (and its employees) knew about what was going on at the party. If it could be shown that the franchisee “knew or should have known of the imminent harm with adequate time and available resources to have prevented or mitigated the harm to decedent,” then the court determined it was possible for the owner to be held liable. And, indeed, the court found that a reasonable jury could reach that conclusion based on the following facts: the party was noisy, the noise could be heard in the hallway areas, hotel employees had observed “groups of youths passing through the lobby,” these same employees knew that other party guests were entering the hotel through a side door, hotel guests had complained to hotel employees about the noise, and one guest had informed the front desk shortly before the shooting that someone at the party had a gun. That last fact was the key for the appellate court in reversing the trial court’s summary judgment decision, both with respect to foreseeability and what it termed “preventability”:

Certainly, a reasonable jury could find that imminent harm was foreseeable when appellees were advised that an attendee of the party had a gun. In light of the fact that an officer responded within three minutes of the 911 call, a reasonable jury could also find that the harm was preventable if appellees’ agents had made the call to police immediately upon discovering that someone had a gun. If a jury found facts, such as those just related, that supported the imposition of a duty, it could also find that this duty was breached, proximately causing decedent’s death.

Beyond the fact that the Corinaldi case does a good job of discussing the basic parameters of the liability of business owners to the victims of the criminal actions of third parties...

---

73 Id. at 492.

74 Id.

75 Id. citing Univ. of Maryland v. Rhaney, 159 Md. App. 44, 858 A.2d 497 (2004), in which the crime at issue involved an assault by one of the defendant landlord’s tenant on another of its tenants.

76 Id. at 492.

77 Id. at 493.

78 Id. at 493-94. There was evidence that two of the party guests had gotten into a loud argument before the shooting, which the appellate court goes out of its way to mention a few times in the course of the opinion, but no evidence that any of the hotel employees were aware of the argument.

79 Id. at 495.
parties, it also shows how far the courts have gone and will continue to go with respect to imposing those duties. Business owners can be held liable not just to their customers, but to those who are invited onto the premises by those customers. A duty of care can be imposed by a court using a foreseeability analysis based solely on the conditions on the property at the time of (or shortly before) the criminal act without the slightest evidence of previous criminal activity at the site or the surrounding area. And a determination can be made that a business owner is liable because its employees did not take preventative actions (in terms of calling the police) within minutes of learning of a potential danger. While there are plenty of other cases where the decision is not as unfriendly to business owners\textsuperscript{80}, cases such as \textit{Corinaldi} do give one pause.

Finally, what exactly is “adequate” physical security for businesses under the law? As with most everything else in this area of the law, the determination is highly fact-specific, one of the facts being what type of business is involved. For example, the security measures that are expected to be implemented for hotel rooms far exceed what a quick service restaurant would be required to implement, given the fact that hotels seek to provide their guests with a private and safe room. Thus, hotels in areas with the lowest crime rates provide secure locks on the doors of guest rooms, safes for personal effects, and frequently limit access to the premises, especially during late night hours. Failure to provide (or maintain in working order) any of these features can lead to finding of liability on the part of a hotel owner as was in the case in \textit{Santangelo v. Omni Hotels Management Corp.}, where the court commented that “common sense instructs that the malfunctioning of locks on hotel room doors, coupled with the failure of the hotel to warn guests of this issue, creates a foreseeable risk that uninvited persons would enter guests’ rooms and assault or rob them.”\textsuperscript{81} By contrast, quick service restaurants even in potentially higher level crime areas would probably not be liable for third party criminal activity if they chose not to install security measures—or at least would be at lower risk compared to a hotel property if they chose not to. Thus, in \textit{Casey v. Ward}, the Court granted summary judgment in favor of McDonald’s and one of its franchisees’ motions for summary judgment in a wrongful death action on the grounds that the plaintiffs had failed to provide evidence establishing that there was a national standard of care requiring restaurant franchisee to provide security guards to ensure patron safety.\textsuperscript{82} The court reached this conclusion despite the fact that the restaurant was open 24 hours a day and was located close to a number of night clubs and bars.

\textbf{B. Vicarious Liability Issues in the Security Arena}

It is fairly common for plaintiffs in a personal injury lawsuit arising out of criminal activity on the premises of a franchise to sue not only the franchisee, but the franchisor as well based on a claim of vicarious liability. Generally speaking, the basis for this claim is that a principal is liable for the acts or omissions of its agents if those agents are acting under the principal’s direction or control.\textsuperscript{83} Vicarious liability is an exception to the general rule that a person injured

\textsuperscript{80} See, e.g., \textit{Folmar v. Marriott, Inc.}, 918 P.2d 86, 90 (Okla. Ct. App. 1996) (affirming summary judgment in favor of hotel operator, finding that the crime was not foreseeable because there was no evidence that the assailants were previously in the hotel lounge, nor were they seen loitering suspiciously in the parking lot before the assault); \textit{McCoy v. Gay}, 165 Ga. App. 590, 302 S.E.2d 130. (Ga. Ct. App. 1983) (holding that an armed robbery during the early morning hours in a Holiday Inn parking lot with allegedly insufficient lighting was not substantially similar to a prior purse snatching on an outside hotel stairway which provided access to guest rooms).

\textsuperscript{81} \texttt{2018 WL 6448842} at *3, Case No. 18-11263 (E.D. La., December 10, 2018)

\textsuperscript{82} \texttt{211 F. Supp. 3d 107, 114} (D.D.C. 2016).

by someone’s negligence is limited in seeking his or her remedy from the party who actually caused the injury.\textsuperscript{84} Thus, even if the injury was caused solely by the acts or omissions of the agent, the principal can still be found vicariously liable for the harm if the tort was committed by the agent while acting within the scope of the agency.\textsuperscript{85} On the other hand, a principal is not generally deemed responsible for the acts of their independent contractors so long as the principal does not retain or exercise control over the means of the work to be accomplished.\textsuperscript{86} Nonetheless, as anyone practicing in the area of franchise law will be able to appreciate, the problem for franchisors with respect to vicarious liability is that they promulgate detailed standards on most, if not all, aspects of their operations and expect their franchisees to adhere to these standards in the operation of their franchises.\textsuperscript{87}

Fortunately, in the area of tort liability, the courts have generally decided that franchisors are not vicariously liable for the acts or omissions of franchisees and/or their employees, despite the promulgation and enforcement of detailed operational standards. For example, in \textit{Allen v. Choice Hotels Intern.}, the plaintiff brought suit against a hotel franchisee and the franchisor arising out of her husband’s death and her own injuries allegedly sustained during a robbery that took place in their hotel room.\textsuperscript{88} In particular, the plaintiff contended that the franchisor was vicariously liable because of an alleged deficiency in the hotel’s security, citing specifically to the franchisor’s standards on guest rooms peepholes and deadbolt locks, both of which she claimed to have been inadequate.\textsuperscript{89} However, the appellate court in \textit{Allen} affirmed the trial court’s grant of summary judgment in favor of the franchisor, holding that its “requirements regarding hotel doors do not show that [the franchisor] had the right to control both the means and the ends of security” at the hotel.\textsuperscript{90} The court went on to point out that the general rule with respect to the application of vicarious liability in the franchise context is whether the franchisor had “the right to control the specific instrumentality or aspect of the business that was alleged to cause the harm.”\textsuperscript{91}

This specific instrumentality test has been applied in a number of other cases in which the courts have rejected the imposition of vicarious liability on a franchisor. For example, in \textit{Hong Wu v. Dunkin’ Donuts, Inc.}, the franchisor was sued under a vicarious liability theory


\textsuperscript{85} \textit{Id.}

\textsuperscript{86} \textit{Id.}

\textsuperscript{87} \textit{Schlotzsky’s, Inc. v. Hyde}, 245 Ga. App. 888, 538 S.E. 2d 561, 562 (Ga. Ct. App. 2000) (noting that “although the Franchise contract and operations manual set forth very detailed standards pertaining to food preparation, hygiene, and sanitation, [the franchisor] did not reserve to itself the right to control the time, manner, or method in which [franchisee], through [the franchisee’s] employees, actually executed those standards.”).

\textsuperscript{88} 942 So.2d 817, 819-20 (Miss. Ct. App. 2006).

\textsuperscript{89} \textit{Id.} at 822.

\textsuperscript{90} \textit{Id.}; see also \textit{Kerl v. Dennis Rasmussen, Inc.}, 273 Wisc. 2d 106, 682 N.W.2d 328, 334 (2004) (noting that “clear trend in the case law and other jurisdictions is that quality and operational standards and inspection rights contained in a franchise agreement do not establish a franchisor’s control or right of control over the franchisee sufficient to ground a claim for vicarious liability as a general matter ...”).

\textsuperscript{91} \textit{Id.} at 823.

\textsuperscript{92} 105 F. Supp. 2d 83 (E.D.N.Y. 2000).
arising out of a fatal attack on plaintiff’s decedent, an employee of the franchisee, while she was working alone one evening at a twenty-four hour location in Queens, New York. Among the undisputed facts considered by the district court on summary judgment, were that (1) the franchisor had hired a security consultant who made several suggestions to the company with respect to security measures at the store level; (2) franchisor had included a series of articles on store security issues written by this same expert in a newsletter that was distributed to all franchisees; (3) franchisor made security equipment available to the franchisees and suggested to them that alarm systems and other burglary prevention techniques were “important”; and (4) the franchise agreement required the franchise to remain open twenty-four hours a day. The court however, rejected the plaintiff’s argument that these facts demonstrated that the franchisor had exercised sufficient control over security measures at the store and thus concluded that the franchisor had no legal duty to the decedent. The court found that even if some of the franchisor’s requirements (including the one requiring twenty-four hour operations) increased the risk to a franchisee’s employees, it could not be held vicariously liable, since the requirements did not mandate that the franchisee take specific security measures “or otherwise control or limit [the franchisee’s] response to this increased risk.” And the court rejected plaintiff’s argument that the security expert’s work for the franchisor and his newsletter articles on security that were distributed to franchisees gave rise to a duty on the part of the franchisor since those activities were “merely advisory.” Finally, the district court noted that imposing liability on the franchisor for its “laudable desire” to assist franchisees on security issues could have the effect of “discourage[ing] franchisors . . . from taking steps to promote an awareness of security issues among franchisees.”

Although this discussion is certainly not comprehensive (given the numerous published opinions on both vicarious liability and security issues), it does provide a rough approximation of the present state of the law in this area. Courts generally take the position that franchisors are

93 Id. at 85-87. Full disclosure: one of the authors of this article worked on the Wu appeal when he was in private practice and now works as an in-house counsel for the franchisor at issue in the case.

94 Id. at 91-94.

95 Id. at 94 (“The court therefore determines that since there is no evidence that [the franchisor] actually mandated specific security equipment or otherwise controlled the steps taken by its franchisees in general, and [the franchisee at issue in the case] in particular, to protect employees, [the franchisor] is not vicariously liable for the alleged lapse in security at issue in this case.”). Among the cases involving criminal assaults at franchises examined by the district court were Hoffnagle v. McDonald’s Corp., 522 N.W. 2d 808, 813 (Iowa 1994) (holding that the franchisor’s authority under the franchise agreement “to insure the uniformity and standardization of products and services offered by a franchisee’s restaurant” was insufficient to give rise to a legal duty); Helmchen v. White Hen Pantry, 685 N.E. 2d 180, 182 (Ind. Ct. App. 1997) (franchisor’s efforts to “heighten awareness” and “offer suggestions” regarding security issues to its franchisees, the company was not vicariously liable for the alleged negligence of its franchisee because the franchisor “did not specifically mandate any security measures.”); and Kelley v. Wurzbach, Case No. 14-97-0557, 1999 WL 33640 at 6-7 (Tex. App. Jan. 28, 1999) (holding that although the franchisor made suggestions and recommendations to its franchisees regarding security, it did not control the security decisions made by the franchisees.).

96 Id. at 91.

97 Id. at 93.

98 Id. at 94. The dismissal was affirmed on appeal, with the court holding that the franchisor did not retain or exercise the right of control over security measures at the franchise level sufficient to impose vicarious liability. Wu v. Dunkin’ Donuts, Inc., 4 Fed Appx. 82 at *1 (2nd Cir. 2001). The court also rejected the plaintiff’s argument that working a graveyard shift was an “inherently dangerous activity” that imposed and enhanced duty on the franchisor. Id. at *2.
not vicariously liable for security measures taken by their franchisees and are not usually liable for harm caused by the criminal acts of third parties against franchisee customers or employees. However, as with virtually every legal issue in this space, the facts are controlling. And a franchisor that mandates specific security measures exposes itself to an increased measure of liability for criminal acts that occur at the system’s locations.

IV. CREATING A PRACTICAL BALANCE

The law requires hospitality providers to pay attention to the safety and security of their guests, but it also obligates them to respect their privacy. At first blush, the dictates of the law pose a Hobbesian choice – should a host err on the side of privacy or on the side of security? The Court concisely defined the intersection of security and privacy in *Carter v. Innisfree Hotel, Inc.* The innkeeper had an obligation to provide security and privacy simultaneously, by providing a room “free from fear that they were being viewed through their mirror.” What the Court did not do, but what is expected of hospitality providers, is to find and implement an approach that balances the two often-disparate dictates of security and privacy. An *ad hoc* practical balance may be the only rational choice.

Certain core principles can inform the impossible chore. For instance, a hospitality provider may be able to manage a patron’s expectations of privacy or security, narrowing the chasm between extreme limits of the two interests. Something as simple as signage, as in the *Lewis* case, may be effective. On the security side, a host can minimize the intrusive nature of security measures, focusing on least intrusive methods given the security challenges specific to the venue.

V. THE FUTURE

The security/privacy landscape is changing, although not at the speed of technology – the lag in statutes addressing biometric screening is clear evidence of that. To make matters even more challenging, security of electronic media seems to overshadow physical security concerns. Will cyber privacy standards redefine the boundaries of personal privacy? Will that affect premises liability?

An early indication of incipient convergence of personal and cyber privacy may be evident in lawsuits filed against Amazon, Apple and Google based on the eavesdropping and recordation capabilities of each company’s voice recognition system. Each of the California cases allege violations of California wiretap statute, while the Washington case, a putative class action, alleges violations of wiretap statutes in Washington, Massachusetts, Florida, Illinois, Maryland, Michigan, New Hampshire, and Pennsylvania. The cases and others like them may test the scope and agility of privacy laws born in an analog world, but living in a cyber-environment.

---

99 661 So.2d 1175 (Alabama 1995).

JEFF L. KARLIN

Jeffrey L. Karlin is a Director & Legal Counsel for Dunkin’ Brands, Inc., the parent company of the Dunkin’ and Baskin-Robbins brands, with a focus on litigation issues. Prior to joining Dunkin’ in August 2015, he was a shareholder with Gray Plant Mooty in the firm’s Washington, DC office litigating franchise law cases. Jeff started his career as a Trial Attorney with the Civil Division of the United States Department of Justice, where he defended cases brought under the Federal Tort Claims Act.
TAMI MCKNEW

Tami McKnew is a partner in the law firm of Fox Rothschild LLP, and served as Managing Director of a predecessor firm, Leatherwood Walker Todd & Mann, P.C., from January 1995 through December 2000. She received her B.A. degree in 1971 from the University of California at Santa Barbara, her M.A. degree in 1973 from the University of California at Los Angeles, and her J.D. degree in 1978 from Northeastern University.

Tami joined Leatherwood in 1978 and concentrates her practice in the areas of franchising, intellectual property, antitrust and complex litigation. She has been a member of the ABA Section on Antitrust since 1979 and a member of the ABA Forum on Franchising since 1980. With Andrew Loewinger, she co-chaired the 38th Annual Forum on Franchising in New Orleans in 2015. She is the co-editor of Covenants Against Competition in Franchise Agreements (Third Edition) and co-author of Annual Franchise and Distribution Law Developments, 2008, in addition to numerous other presentations at the Forum. Previous articles by her on internet trademark use appeared in Landslide, The Journal of Internet Law and Business Law Today.

Her current Board memberships include the South Carolina Chapter of the Nature Conservancy; the United Way of Greenville County; The Priester Foundation; and the Institute for Child Success of which she is a founder. She has one daughter, Bronwyn Kelson, who prosecutes bad guys in Sumter, SC, a lawyer son-in-law who strives to do good as a South Carolina Senator, and two grands, Adelaide and Joe, who are the most wonderful, amazing children in existence (except for your grandchildren).