The Columbia
SCIENCE AND TECHNOLOGY LAW REVIEW
www.stlr.org

PRIVACY IMPLICATIONS OF COMMERCIAL OFFICE BUILDING SECURITY TECHNOLOGY IN THE POST-9/11 ERA

Trevor T. Adler[1]

This Note examines a full range of security issues involving privately-owned but publicly accessible office buildings in the post-9/11 era, from a landlord's basic security duties to privacy infringement. The analysis focuses on the recent proliferation of computer-enabled access control and surveillance technologies, which have emerged in the last ten years as a viable alternative to increased security personnel staffing. The Note makes several conclusions and recommendations. First, to overcome the possibility of negligent security lawsuits, property owners must reevaluate the security provided in their buildings on an ongoing basis. Second, access control and surveillance technologies offer cost-effective means of satisfying security minima for a majority of commercial properties. Third, to balance the benefits of these technologies with the potential for privacy infringement, property owners should consider contractual and/or unilateral notice of security monitoring and recording practices. Finally, the burgeoning partnership between private security and law enforcement creates the possibility of Fourth Amendment privacy infringements.

[1] Trevor Adler is a 2007 J.D. candidate at Columbia University School of Law and an Executive Editor of the Columbia Science & Technology Law Review, Vol. VIII. He received B.A. and M.A. degrees in history from Johns Hopkins University in 2004, where he was the chief of the campus emergency medical services unit and taught numerous courses in emergency response under the American Red Cross curriculum. He has served as the head of security for a private real estate management and development company in New York City for the past four years. He has worked in conjunction with various law enforcement agencies and security organizations, and is a member of the New York City Police Department Area Police/Private Security Liaison and the Counter Terrorism Division's NYPD Shield.

INTRODUCTION

Striking a balance between privacy and security has emerged as one of the twenty-first century's greatest challenges. The rules of engagement have changed; battles in the War on Terror are rarely fought on an identifiable battlefield but instead in and among cities and citizenry. Yet, aside from the notable exception of the Patriot Act, privacy law remains the same. As the legal community engages in debate and action to effectively resolve the most divisive of constitutional issues forged by the terrorist threat to national security and the Bush administration's chosen means of combat, the private sector's response to the emergent threat must not be overlooked.

The most devastating attacks of 9/11 were borne by twin commercial towers, a fact that resounded clearly through the commercial real estate industry. Since then, office building security in major U.S. cities has dramatically increased. In sizeable commercial properties, access control and video surveillance systems have become the norm, and the actions of millions of workers are monitored and recorded twenty-four hours per day, seven days per week, often without their knowledge. Building security is not, in itself, intended to defend directly against future terrorist attacks. Rather, it is the industry's cost-efficient means of deterring would-be attackers and affording some protection to tenants, including enhanced safeguards from theft and other non-terrorism crime. Computer-enabled access control and surveillance technologies, which have emerged in the last ten years as a viable alternative to increased manpower, vest commercial property managers with the ability to increase facility security without breaking the bank. But at what cost to privacy?

This Note examines a full range of security issues involving privately-owned but publicly accessible office buildings, from a landlord's basic security duties to privacy infringement. Section I begins with an analysis of negligent security actions and discusses possible changes in negligence standards since 9/11. Section II provides an overview of the two mainstay technologies of post-9/11 office building security, access control and video surveillance. Section III examines privacy in the commercial property context, focusing on the reasonableness of privacy expectations and presenting a possible solution by means of contractual and unilateral notice. Finally, Section IV examines potential Fourth Amendment privacy infringements resulting from commercial property access control and video surveillance records falling into the hands of government authorities, a possible corollary of the burgeoning partnership between private security and law enforcement since 9/11.

I. NEGLIGENT SECURITY ACTIONS: COMMERCIAL LANDLORD DUTIES TO PROVIDE SECURITY MINIMA

This section seeks to establish that even though a universal minimum of security for commercial properties has not been specified by statute or case law, cost effective security technologies are likely to be considered reasonable security precautions that owners of sizeable commercial properties must take to satisfy their common-law duties to tenants and the public. New York case law – the most comprehensive on the subject – suggests that the amount of security precautions an office building must take in order to

satisfy the negligent security threshold is proportional to the existing threat. As the cases that follow indicate, prior criminal incidents and the probability of future crime are typically the criteria courts rely upon when determining whether a building's security was negligently inadequate. When similar civil negligence cases arise with respect to terrorist rather than criminal acts, prior acts of terrorism directed against a building and the likelihood of future occurrences or recurrences should remain the primary factors of analysis in judicial determinations of negligent security actions.

At common law in most states, a commercial landlord is duty-bound to take minimal security precautions, for the protection of tenants and visitors from the foreseeable criminal acts of third parties.[2] This duty extends to the managing agents of commercial properties,[3] yet it does not require a landlord or managing agent to become an insurer of a tenant's safety.[4] What security precautions may reasonably be required of an owner is most often a question of fact presented to a jury.[5] In order to win a negligent security action against a commercial property owner, a plaintiff must establish that criminal activity on the premises was foreseeable and that the negligent security at issue was the proximate cause of the injury.[6] Because the foreseeability component of the negligent security action has caused considerable controversy in the courts and has likely been affected by the events of 9/11, it is the first issue to which I turn.

A commercial office building, like any other business premises open to the public to the degree permitted by the landlord and its tenants, is subject to liability in tort. The court in *Nallan v. Helmsley-Spear*, the seminal case in New York concerning negligence standards for commercial property, began its foreseeability analysis by quoting the Restatement of Torts:

> 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 of the possessor to exercise reasonable care to

---

[2] *Nallan v. Helmsley-Spear, Inc.*, 407 N.E.2d 451, 458 (N.Y. 1980); *Wayburn v. Madison Land Ltd. P'ship*, 724 N.Y.S.2d 34, 38 (App. Div. 2001); *Saelzler v. Advanced Group 400*, 23 P.3d 1143, 1152-53 (Cal. 2001); *Nola M. v. Univ. of S. Cal.*, 20 Cal. Rptr. 2d 97, 108 (Ct. App. 1993); *Leslie G. v. Perry & Assocs.*, 50 Cal. Rptr. 2d 785, 790 (Ct. App. 1996); *see also Kline v. 1500 Mass. Ave. Apartment Corp.*, 439 F.2d 477, 481 (D.C. Cir. 1970) (the seminal federal case extending liability to landlords for third party criminal acts).

[3] *Wayburn*, 724 N.Y.S.2d at 38; *King v. Res. Prop. Mgt. Corp.*, 665 N.Y.S.2d 637 (App. Div. 1997); *Rudel v. Nat'l Jewelry Exch. Co.*, 623 N.Y.S.2d 878 (App. Div. 1995).

[4] *Wayburn*, 724 N.Y.S.2d at 38; *Jacqueline S. v. City of New York*, 614 N.E.2d 723, 725 (N.Y. 1993); *Nola M.*, 20 Cal. Rptr. 2d at 108.

[5] *Nallan*, 407 N.E.2d at 459.

[6] *Id.* at 458-60.

> (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.* Duty to police premises. Since the possessor is not an insurer of the visitor's safety, he is ordinarily under no duty to exercise any care until he knows or has reason to know that the acts of the third person are occurring, or are about to occur. He 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 he has no reason to expect it on the part of any particular individual. If the place or character of his business, or his past experience, is such that he should reasonably anticipate careless or criminal conduct on the part of third persons, either generally or at some particular time, he may be under a duty to take precautions against it, and to provide a reasonably sufficient number of servants to afford a reasonable protection.[7]

Nallan involved a theater union officer who was shot in the lobby of a midtown Manhattan office building in which the union was a tenant. The shooting occurred as the victim proceeded to a sign-in desk where the management stationed an attendant who was at the time away from his post performing his janitorial responsibilities elsewhere in the building.[8] The union officer survived the incident and brought a negligent security action against the building owner and manager.

Prior to *Nallan*, New York courts had held that to establish foreseeability, a plaintiff must demonstrate that crimes similar to the one at issue had occurred previously in a comparable location in the same building. This onerous burden was rejected by the *Nallan* court, which held that a landlord has a duty to take reasonable security precautions if "it is shown that he either knows *or has reason to know* from past experience 'that there is a *likelihood* of conduct on the part of third persons . . . which is likely to endanger the safety of the visitor.'"[9] The Appellate Division continued to abide by its pre-*Nallan* interpretation of foreseeability, at least until the Court of Appeals clarified in *Jacqueline S. v. City of New York*: "We have never adopted the restrictive rule urged by defendant and apparently embraced by the Appellate Division: that to establish the foreseeable danger from criminal activity necessary for liability, the operative proof must be limited to crimes actually occurring in the specific building where the attack took

[7] Restatement (Second) of Torts § 344 (1977).

[8] *Nallan*, 407 N.E.2d at 454-55.

[9] *Id.* at 458 (quoting Restatement (Second) of Torts § 344, cmt. f) (emphasis added).

place."[10] The *Jacqueline S.* court and subsequent New York decisions have followed the less-rigorous *Nallan* interpretation of foreseeability.[11]

Recent New York decisions have refused to expand the *Nallan* foreseeability doctrine to permit evidence of dissimilar criminal activity to render subsequent crimes of a more serious nature foreseeable. Thus, evidence of shoplifting in a shopping mall does not render an assault foreseeable on the premises.[12] Likewise, neither evidence of automobile break-ins in a hotel's parking lot nor that of vagrants loitering in the hotel's lobby establishes that an assault occurring on the hotel's sixth floor was foreseeable.[13] Along similar lines, "ambient neighborhood crime alone is insufficient to establish foreseeability."[14] Yet foreseeability remains a complex and unpredictable issue since its determination is subjective and "must depend on the location, nature and extent of those previous criminal activities and their similarity, proximity or other relationship to the crime in question."[15] The Court of Appeals in *Jacqueline S.* applied this reasoning to conclude that evidence of prior drug-related criminal activity and of open-access to a building's stairwells, corridors, and roof was sufficient to establish the foreseeability of a tenant's abduction and rape.[16] The Appellate Division has followed *Jacqueline S.* and applied the *Nallan* foreseeability doctrine to conclude that prior non-violent incidents in a building can render a rape and robbery foreseeable.[17]

In the post-9/11 world, "what was once unthinkable must now be treated as foreseeable."[18] Even though aerial attack is beyond the scope of commercial security efforts,[19] triers of fact are more likely to find other forms of criminal and terrorist activity foreseeable, especially when the property in question is a sizable commercial office tower

---

[10] *Jacqueline S. v. City of New York*, 614 N.E.2d 723, 725 (N.Y. 1993).

[11] *Id.*; *Wayburn v. Madison Land Ltd. P'ship*, 724 N.Y.S.2d 34, 38 (App. Div. 2001).

[12] *Durham v. Beaufort*, 752 N.Y.S.2d 88, 89 (App. Div. 2002).

[13] *Pascarelli v. LaGuardia Elmhurst Hotel Corp*., 742 N.Y.S.2d 98, 99 (App. Div. 2002).

[14] *Novikova v. Greenbriar Owners Corp*., 694 N.Y.S.2d 445, 448 (App. Div. 1999); *see also Levine v. Fifth Hous. Co*., 662 N.Y.S.2d 95, 96 (App. Div. 1997); *Johnson v. City of New York*, 777 N.Y.S.2d 135 (App. Div. 2004).

[15] *Jacqueline S.*, 614 N.E.2d at 726.

[16] *Id*. at 723-24.

[17] *Wayburn v. Madison Land Ltd. P'ship*, 724 N.Y.S.2d 34, 38 (App. Div. 2001).

[18] Daniel P. Dain & Robert L. Brennan, Jr., *Negligent Security Law in the Commonwealth of Massachusetts in the Post-September 11 Era*, 38 New Eng. L. Rev. 73, 74 (2003).

[19] James Glanz, *No Tower Can Withstand Attack as Jets Get Bigger, Expert Says*, N.Y. Times, Mar. 14, 2002, at B5.

in a major city.[20] As capable as police forces are, commercial owners are in the best position to provide an initial level of security at least sufficient to deter most forms of criminal or terrorist activity.[21] Despite the fact that courts have recognized that commercial property owners are duty-bound to provide a minimum level of security for their tenants and guest-invitees, "the law is nebulous. No book containing a code of security measures exists for landlords. Liability is premised on a series of considerations or elements that a jury weighs, and juries may weigh those considerations or elements differently in each case."[22] This "absence of clear rules or standards governing what level of security is reasonable"[23] suggests that recent innovations in access control and surveillance technologies may fulfill the property owner's post-9/11 security duty, and generally do so without any increase in attendance staffing.

As far back as the *Nallan* decision in 1980, courts have recognized that the principal aim of commercial property security is to deter potentially harmful acts. Recall that in *Nallan*, a shooting occurred in the lobby of the Fisk Building in midtown Manhattan while the lobby attendant was absent from his post and attending to his other duties.[24] In concluding that a jury "might well have inferred from the available evidence that the absence of an attendant in the lobby at the moment plaintiff Nallan arrived was a 'proximate' cause of Nallan's injury," the court determined that the mere presence of the attendant was a deterrent, regardless of his actual training or abilities:

> The clear implication of the expert testimony was that a would-be assailant of any type would be hesitant to act if he knew he was being watched by a representative of the building's security staff. Contrary to the reasoning of the majority at the Appellate Division, it would seem to us that the deterrent effect described by plaintiffs' expert witness would exist whether the lobby guard was a "trained observer" or, as here, was an ordinary attendant with no special expertise in the area of building security,

---

[20] *See* Joe Wientge, *Foreseeable Change: The Need for Modification of the Foreseeability Standard in Cases Resulting from Terrorist Acts After September 11th*, 74 UMKC L. Rev. 165 (2005) ("This Comment argues that in the post-September 11th world, terrorist attacks should be deemed foreseeable, allowing a jury to hear all of the evidence before a final decision is made.").

[21] *See In re September 11 Litig*., 280 F. Supp. 2d 279, 300 (S.D.N.Y. 2003) (recognizing that landowners can be found to be in the best position to prevent harm); Dain & Brennan, Jr., *supra* note 18, at 74 ("Negligent security law is premised on the principle that crime is preventable, and that the law places a duty of care upon the party in the best position to take security measures to prevent foreseeable crimes - the property owner or possessor."); *see also Hamilton v. Beretta U.S.A. Corp*., 750 N.E.2d 1055, 1061 (N.Y. 2001) ("The key . . . is that the defendant's relationship with either the tortfeasor or the plaintiff places the defendant in the best position to protect against the risk of harm.").

[22] Wientge, *supra* note 20, at 174.

[23] *Id*.

[24] *Nallan v. Helmsley-Spear, Inc.*, 407 N.E.2d 451, 454 (N.Y. 1980).

> since that fact would make no difference from the potential assailant's point of view.[25]

In terms of negligent security law, a finding of sufficient security for the deterrence of foreseeable harm is thus typically unrelated to actual prevention capability. Neither a locked door nor a security camera nor even a lobby attendant need be capable of disarming an assailant to satisfy the *Nallan* court's concept of sufficient security to deter harm and satisfy a commercial property owner's duty to that end.

To put the *Nallan* case in perspective, the Fisk Building at 250 West 57th Street in New York City is twenty-six stories high and has roughly a half-million square feet of rentable space.[26] In relative terms, at least in Manhattan, the Fisk Building would be characterized as a medium-sized property. The discussion above illustrates that a property owner's duty to provide security – and the reasonable minimum thereof – is measured against the foreseeable harm. The amount of security precautions a commercial property owner is obliged to maintain in order to survive a negligence action is therefore proportional to the threat that exists against the particular building and its occupants. Thus, the *Nallan* court found that an around-the-clock lobby attendant could be necessary to fulfill the owner's reasonable duty in the medium-sized Fisk Building with a history of criminal incidents while a recent trial court opinion found mere locked doors and an intercom system to constitute adequate security in a "fairly safe" building on Canal Street:

> Given the lack of prior similar criminal acts in the building, plaintiffs' expert's claim that 267 [Canal St. Corp. (property owner)] had a duty to provide enhanced security in the form of a closed-circuit television system, the posting of a security guard and/or additional elevator operator to screen persons entering the passenger elevator, and to lock the front door of the building during business hours is without merit. An after-the-fact realization that one or more of these measures might have prevented the tragedy that ultimately occurred does not establish that 267 breached its duty to provide minimal security precautions. 267 merely owed [the tenant] Mr. Woo a duty to adopt adequate security measures given the foreseeable risks, it was not an insurer of his safety.[27]

Courts have always been, and will likely continue to be, sensitive to the cost outlays of real property owners when evaluating reasonable security minima because owners are not insurers of public safety.[28] New security technologies will likely become essential

---

[25] *Id*. at 459.

[26] Listing, Office Buildings Mag., Manhattan Review 2006, at 93.

[27] *Yuen v. 267 Canal St. Corp*., 802 N.Y.S.2d 306, 309-11 (Sup. Ct. 2005).

[28] *Id*.; *Wayburn v. Madison Land Ltd. P'ship*, 724 N.Y.S.2d 34, 38 (App. Div. 2001); *Nola M. v. Univ. of S. Cal.*, 20 Cal. Rptr. 2d 97, 108 (Ct. App. 1993).

components of this evaluation because they enable property owners to increase the security in their buildings to meet post-9/11 reasonableness standards at a fraction of the cost of increased human asset deployment (i.e., pulling building employees off other assignments to monitor lobbies or other checkpoints) or staffing (i.e., hiring additional employees or contracting a security company to perform security functions), as will be discussed in Section II.

Note that in addition to increasing building security to meet what I argue will be stricter reasonableness standards since 9/11 in negligent security actions, many sizeable commercial property owners have chosen to take greater security precautions voluntarily to meet or exceed the security deployment instituted by neighboring or competing buildings – to keep up with the Joneses – in order to provide current and prospective tenants reassurances of safety and security.[29] This is not to say that I espouse – in fact, I am assuredly against – courts evaluating a building's security *ex post* based on a relative comparison of the respective security situations of comparably sized and rented properties. Commercial real estate is market-based. Owners should not feel compelled to implement the same level of security as the building across the street because some tenants may not want to deal with the inconveniences typically associated with security upgrades.[30] Thus, if all tenants decided they would only rent from buildings maintaining a certain level of security, the market would require all buildings to meet that standard to remain competitive. Yet voluntary security upgrades may have the unintended effect of holding the owner to a higher standard with respect to negligent security liability. Thus in *Jacobs v. Helmsley-Spear*, the defendant landlord recognized a garage area as vulnerable to intruders and "voluntarily undertook to install an electronic device to lock the door and as a result, the tenant was 'lulled into a false sense of security."[31] The *Jacobs* court concluded: "When one voluntarily assumes the performance of a duty, he is required to perform it carefully, not omitting to do what an ordinary prudent person would do in accomplishing the task."[32] Thus, once a property owner has installed a security technology that tenants have reasonably come to rely upon, the malfunction or inoperability of the system can be grounds for a negligence action so long as the system's failure is the proximate cause of the injury.[33]

---

[29] Erik Engquist, *Weak Spots Abound in NY, Despite Risk of Attack*, Crain's N.Y. Bus., May 1, 2006, at 21; Rachelle Garbarine, *When in Doubt, Office Building Owners Renovate*, N.Y. Times, Apr. 15, 2001, § 11 (Real Estate), at 7.

[30] Charles V. Bagli, *Too Tall? Not at All, Tenants Say; Mass Exodus is Absent at Skyscrapers as Anxiety Drops*, N.Y. Times, Nov. 5, 2001, at F2; Christine Haughney, *Landlords Seek to Balance Security with Access – Tenants Shun Inconvenience as Building Owners Grapple with Possibility of Terrorism*, Wall St. J., July 27, 2005, at B6.

[31] *Jacobs v. Helmsley-Spear, Inc.*, 469 N.Y.S.2d 555, 557 (Civ. Ct. 1983) (quoting *Nallan v. Helmsley-Spear, Inc.*, 407 N.E.2d 451, 460 (N.Y. 1980)).

[32] *Id.*

[33] *Id.* ("Under the circumstances of this case, the inoperability of the device for eight days would constitute constructive notice."); *see also Alvarez v. Masaryk Towers Corp*., 15 A.D.3d

Similarly, rent increases explicitly for improved security can create new duties and raise negligence standards. In *Sherman v. Concourse Realty Corp.*, the court distinguished the case at hand from a prior case cited by the defendant landlord, *Hall v. Fraknoi*, in which the court held a landlord-tenant relationship did not create a duty to provide security from criminal intruders in an apartment building: "*Hall* is immediately distinguishable from the instant case where the landlord, for a consideration, assumed the duty of providing a bell and buzzer system to protect against the hazard of criminal intruders."[34] Thus, even though security technologies, be it an intercom, access control, or surveillance camera system, can constitute adequate minimal security measures in themselves,[35] a landlord who receives actual or constructive notice of their disrepair may be subject to a negligent security action and held to a higher standard had consideration been received in exchange for the security upgrades.[36]

Hindsight is 20/20. It is easy to review an incident *ex post* and blame a property owner for not providing enough security. But as I have endeavored to establish here, "enough" security is a difficult determination to quantify. The recent jury finding of negligence on the part of the Port Authority to adequately safeguard the World Trade Center in the 1993 bombing case illustrates the challenge of determining negligence as well as the pitfalls of hindsight.[37] Insofar as the six-member jury relied upon the warnings and advisements of the Port Authority's security experts and consultants, many of whom suggested increased precautions prior to the 1993 attack, the outcome is problematic. This is not to say that the verdict should be overturned; the decision would comport with the common law of New York so long as the high-profile nature of the Trade Center and demonstrable terrorist threat – the risk and vulnerability posed by the parking garage – were the jury's primary considerations.

The advice of security consultants is not a solid basis on which to render a negligence determination and goes against the grain of the case law discussed in this section for two reasons. First, one would suspect security consultants almost always suggest that security should be enhanced – such cautions are in the very nature of their employment. If their advisements to property owners could be relied upon *ex post* as evidence of negligent security, a veritable parade of horrors could result, driving property

---

428, 428-29 (N.Y. App. Div. 2005) ("If a tenant or guest is assaulted by an intruder, recovery against the landlord requires a showing that the landlord's conduct was a proximate cause of the injury.").

[34] *Sherman v. Concourse Realty Corp*., 365 N.Y.S.2d 239, 244 (App. Div. 1975) (citing *Hall v. Fraknoi*, 330 N.Y.S.2d 637 (Civ. Ct. 1972)).

[35] *Moskal v. Fleet Bank*, 694 N.Y.S.2d 555, 560 (Sup. Ct. 1999); *Williams v. Citibank*, 677 N.Y.S.2d 318, 319-20 (App. Div. 1998).

[36] With the benefits of computer-controlled security technologies also come the pitfalls; newly emergent systems are prone to hardware and software bugs and failures. However, a property owner or manager cannot be held negligent as long as reasonable attempts to repair the equipment were made in a timely manner.

[37] *See* Anemona Hartocollis, *Port Authority Found Negligent in 1993 Bombing*, N.Y. Times, Oct. 27, 2005, at A1.

owners to refrain from seeking security advice altogether. Second, case law establishes that a determination of foreseeability in negligence actions must be based on substantive evidence, not conjecture. New York's *Nallan* foreseeability doctrine was recently echoed by the California Supreme Court, which held that a determination of whether a landlord could have prevented a criminal incident had it taken greater security precautions "cannot be based on mere speculation, conjecture and inferences drawn from other inferences to reach a conclusion unsupported by any real evidence, or on an expert's opinion based on inferences, speculation and conjecture."[38] Perhaps California's highest court went beyond New York's standards for limitation of liability when it stated: "it would be grossly unfair to permit a lay jury, after the fact, to determine in any case that security measures were 'inadequate,' particularly in light of the fact that the decision would always be rendered in a case where the security had, in fact, proved inadequate."[39]

While most commercial properties are not high-profile targets of either crime or terrorism, it may be plausibly argued that in the post-9/11 era, all commercial properties in major cities are at greater risk, and the threshold of security minima has risen accordingly. But property owners are not the insurers of public safety, and owe a duty to their tenants only to provide security minima "given the foreseeable risks."[40] It would be unreasonable and economically infeasible to require every office building in high-risk cities to institute a round-the-clock security presence. However, it would be reasonable for a court to determine *ex post* that an owner of a medium or large office building in such a city was negligent because it made an inadequate attempt to elevate security given the affordability of technologies, such as access control and video surveillance. Courts must therefore balance the commercial landlord's cost burdens for security with the foreseeability of the criminal or terrorist threat. Whether this threat is specific or generalized but demonstrable will determine to a significant extent whether cost-effective security technologies or more significant, physical security deployment will suffice to overcome a negligence action. In anticipation of this analysis, property owners should perform their own *ex ante* analyses to determine the level of security they should provide.

II. OVERVIEW OF COMMERCIAL PROPERTY SECURITY TECHNOLOGY

Technology has emerged as a crucial component of commercial property security because it is a cost-effective means to significantly increase safety and deter criminal acts.[41] While commercial real estate owners are typically concerned with the safety of their premises, decisions as to how much can be budgeted for security measures are made

[38] *Saelzler v. Advanced Group 400*, 23 P.3d 1143, 1151 (Cal. 2001) (quoting *Leslie G. v. Perry & Assocs.*, 50 Cal. Rptr. 2d 785, 795 (Ct. App. 1996)).

[39] *Id*. at 1153 (quoting *Nola M. v. Univ. of S. Cal.*, 20 Cal. Rptr. 2d 97, 102 (Ct. App. 1993)).

[40] *Yuen v. 267 Canal St. Corp*., 802 N.Y.S.2d 306, 311 (Sup. Ct. 2005).

[41] Victoria Rivkin, *Offices Erect Façade of Safety; Measures 'A Waste'; Specific High-Tech Systems Needed*, Crain's N.Y. Bus., Mar. 28, 2005, at 22.

with an eye to the bottom line.[42] In the post-9/11 era, security has become an important selling point for tenants in many urban markets, none more than New York City.[43] Tenants have typically come to expect increased security precautions from their landlords, who seek to provide security enhancements in the most cost effective manner. Rather than hiring or allocating more employees to perform security-related functions, access control and surveillance technologies enable property owners to deploy their existing staff more effectively.[44] Indeed, these technologies offer the additional benefit of remote operation, which can allow for the consolidation of multiple building monitoring in a single location, reducing costs while increasing efficiency and, ideally, coordinated response.[45]

Access control is a term of art used to describe systems that attempt to restrict unauthorized individuals from entering secured areas.[46] Effectively deployed access control systems identify people by an individual 'tag' or 'identifier,' such as a pin number, card key, or biometric characteristic.[47] Proximity and magnetic swipe cards are examples of access control tags used in many office buildings, typically providing access to lobby turnstiles, doors, or elevators. When a tag or identifier is presented, swiped, or entered into an access control reader, the system determines whether access may be granted to the building or to a specific floor or area therein, and whether or not access is granted, the event is archived into an access control database log. The database thereby maintains a history of tenants' movements into, out of, and throughout the building. In many sizeable buildings, access control logs are not limited to tenants.

Some access control systems govern and record the movements of visitors, who are given temporary key cards or pin numbers upon arrival. Access control systems typically prevent invitees or delivery persons from gaining access to the building or a specific tenant space until they have gone through a check-in procedure, which may

---

[42] Michael Brick, *Disaster Planner Has Lessons From 9/11 to Offer, and Boston Listens*, N.Y. Times, July 10, 2002, at C1.

[43] John Holusha, *A New Interest in Security in Office Buildings*, N.Y. Times, Oct. 28, 2001, § 11 (Real Estate), at 10.

[44] Maria Gonzalez, *Join the Revolution; Access Control and CCTV; Property Management*, 51 Real Estate Weekly 19, at 12S(1) (2005).

[45] Seth Klibonoff, *Integrated Technologies Enhance Building Security*, 52 Real Estate Weekly 51, § B (Construction & Design), at 11C (2006); Steve Morefield, *Access Control Has Come a Long Way*, 14 Security Tech. & Design 6 (2004).

[46] Bonnie Michelman, *Is Access Control a Good Investment*, Access Control & Security Systems Integration, Sept. 1, 1997, *available at* http://securitysolutions.com/mag/security_access_control_good/.

[47] *Little Things Can Be Crucial When RFID Added to Security Effort; Anticipate Need for Backup Access Control, Testing Life of RFID Tags*, Corporate Security, Mar. 15, 2005, at 4.

include signing an entry log and presenting a form of photo identification.[48] Visitor check-in systems may also be independent of tenant access control systems and maintain a separate database of when and where visitors came and went.[49] Some buildings retain only a visitor's name and signature, while others take digital photographs and retain scanned images of a visitor's identification. Note that visitors are not in a position to refuse the information requested by building personnel unless they are willing to forgo entrance.[50] No statutory or common law limitations exist to restrict the type or extent of information a building may require of visitors.

Landlords that issue photo identification cards to their tenants and their tenants' employees generally maintain a database of names, photographs, places of employment, and emergency contact information.[51] Even though tenants presumably do not intend for this information to be provided to third parties other than in the event of an emergency, they expect it to be retained to facilitate the issuance of a replacement identification card. The identification card or separate access control tag, linked to the landlord's database, then permits tenants and their employees to securely ingress, egress, and traverse the building. When such movements are archived by the access control system and recorded by video surveillance, landlords can collect a complete track log of 'who, what, where, and when.'[52] The same may be true for visitors, whose identification is scanned or logged and whose photo is captured either by a specialized visitor check-in system or by surveillance cameras, all linked to a temporary access control tag issued to the visitor.[53]

---

[48] Many buildings prevent open access to visitors – some buildings require tenants to pre-approve visitors and deliveries, some contact tenants on a visitor's arrival to verify their invitation, and others simply issue a temporary card key or pin without tenant verification. *See* Lawrence Van Gelder, *The Last Hurdle to Work: Security*, N.Y. Times, Nov. 24, 2002, § 3 (Money and Business), at 9.

[49] Michael Fickes, *Safeguards on the Rise*, Access Control & Security Systems, July 8, 2006, at 16, *available at* http://securitysolutions.com/mag/security_safeguards_rise/.

[50] I have not encountered any instances of a visitor or his tenant inviter challenging a landlord's access control methods as overly restrictive (e.g., violating the tenant's right to quiet enjoyment). Of note, a search conducted by a hospital's private security personnel of an alleged terrorism suspect while in the presence of police was held not to implicate the civil rights of the individual searched. *Atamian v. Hawk*, 842 A.2d 654 (Del. Super. 2003). Also of note, the legality of casino access control based solely on the "Black Book" has been upheld by the Nevada Supreme Court and the 9th Circuit Court of Appeals. *See* John M. Glionna, *Nevada's 'Black Book' Still Packs A Punch*, L.A. Times, March 13, 2000, at A3.

[51] *See* Michael Fickes, *Snap, Snap Click, Click*, Access Control & Security Systems, Oct. 1, 1999, *available at* http://securitysolutions.com/mag/security_snap_snap_click/.

[52] Klibonoff, *supra* note 45.

[53] Personal information revealed by tenants and visitors to property management or security is not subject to any reasonable privacy protections from the government, as discussed in Section IV of this Note.

As is the case for office building security generally, access control data collection and archiving is unregulated. Tenants and visitors may be subject to passive metal detection or physical search, depending on building policy.[54] There is no federal or state regulation over commercial building security in this context.[55] Even the largest commercial properties are allowed to maintain whatever level of private security their owners and tenants desire, forcing the issue into the landlord-tenant leasing and contractual arena. Only contracts and oral agreements between landlords and tenants limit the scope of access control data collected from tenants, their employees, and visitors and retained by a building owner. Tenants who voice no opinion on the subject provide implied consent to the landlord to deploy access control technologies as they see fit. The same is true of video surveillance systems.

Video surveillance itself has existed for quite some time (decades prior to the proliferation of access control systems in commercial properties), but it has recently become more affordable and recording and archiving technologies have improved significantly.[56] Like access control, video surveillance systems can digitally archive video for days, months, or years. Computer-based video surveillance systems make searching through a footage archive for a specific date or time as easy as calling up an archived access control log from a database.[57] Just as access control systems identify failed access attempts, video surveillance systems can identify motion or even suspicious movements.[58] Cameras may be deployed on the interior as well as the exterior of commercial properties, serving a wide array of safety and security purposes.

Prior to the 1990s, surveillance cameras were predominately deployed in office buildings to deter and combat theft.[59] After incidents such as the 1993 World Trade Center bombing and the 1995 Oklahoma City bombing, video surveillance proved an asset in the pursuit and prosecution of terrorists carrying out attacks against office

---

[54] Holusha, *supra* note 43.

[55] The same is not true of residential property, where basic access control systems such as door intercoms may be statutorily required. *See e.g.*, N.Y. Mult. Dwell. Law § 50-a (McKinney 2006) (stating minimum security requirements for entrance doors, locks, and intercommunication systems for multiple dwelling residences in New York).

[56] Klibonoff, *supra* note 45; *IP Cameras Will Change Your Life*, Security Mag., Apr. 2006, at 62.

[57] Gonzalez, *supra* note 44.

[58] Intelligent camera systems can also be used for facial recognition, but some such systems are still experimental and beyond the budgets of most commercial properties.

[59] John Holusha, *More Attention to Security in Designing Buildings*, N.Y. Times, Mar. 10, 2002, § 11 (Real Estate), at 6 ("In the past, according to a report by Larry Conlon, another security specialist with Cushman & Wakefield, security was 'focused on protecting the building occupants from acts of random street crime, mitigating internal and external theft and the protection of the physical asset.'").

buildings.[60] The events of 9/11 further suggest that external video surveillance could be crucial even during a terrorist attack to help determine the location of fires and safe evacuation routes.[61] Video surveillance upgrades typically accompany any other office building security enhancements in the post-9/11 era, having proven to be cost-effective tools to deter crime and to pursue criminals and terrorists.

Finally, in addition to allowing for the consolidation of security monitoring and recording across multiple properties in one location, reducing manpower and expense, Internet Protocol or "IP-based" access control and video surveillance systems offer monumental improvements in information sharing.[62] IP-based systems can interoperate between or even coexist across servers, linking access control and video data so that when an incident occurs, the right information is delivered or broadcast within minutes to the right people.[63] Thus, advanced systems can be programmed to send an alert message to a local security desk or to wireless, handheld devices of security staff informing them that a door was forced open or an invalid tag was presented at a specific building entrance, alongside a live video feed from the nearest surveillance camera.[64] The incident could simultaneously be digitally recorded and flagged for review.[65] But perhaps more importantly, when video surveillance is digitally recorded on an IP system, images of suspect individuals may be instantaneously "captured" and quickly e-mailed or otherwise distributed to an unlimited number of neighboring buildings, businesses, or law enforcement agencies.[66] The first private security staffs to leverage and truly benefit from information sharing were casinos, which since the 1960s have commonly compiled "Black Book" databases of cheats who are prohibited from gambling.[67] Recent technological advances have enabled casino security staff to search Black Book databases and distribute photographs and descriptions of suspected cheats or blacklisted individuals over proprietary networks and e-mail via the Internet.[68] The casino industry's

---

[60] Quentin Burrows, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance*, 31 Val. U. L. Rev. 1079, 1123 n.355 (1997).

[61] *See* The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States 298 (2004).

[62] *IP Cameras Will Change Your Life*, *supra* note 56, at 62.

[63] Klibonoff, *supra* note 45.

[64] *Id*.

[65] *Id*.

[66] Gonzalez, *supra* note 44; *Credit Digital for Security*, Security Mag., Jan. 2005, at 52.

[67] Glionna, *supra* note 50; Ian Katz, *Where the Jokers Are Wild; Beware, D.C.! Gambling Comes with a Full Deck of Cheaters and Thieves*, Wash. Post, Oct. 19, 1993, at C1.

[68] Randy Southerland, *Almost Venice*, Access Control & Security Systems, Mar. 1, 2001, *available at* http://securitysolutions.com/mag/security_almost_venice/; Daintry Duffy, *Two of a Kind*, CSOonline.com, Oct. 2003, http://www.csoonline.com/read/100103/kind.html.

information sharing network serves as a predecessor and, in certain respects, a model for the geographically-based information sharing networks that have emerged in the real estate and retail industries, which are discussed in the final section of this Note.

Whichever combination of the access control and video surveillance technologies and security practices a commercial property's owner deploys, it is safe to say that far more data is being monitored, retained, and shared, than before 9/11 in and amongst commercial properties. Because this conduct is largely unregulated, ample opportunities for privacy infringement result. As will be discussed in the next section, even though much of the data collected and retained by security technologies does not implicate privacy rights, it is not difficult to envision situations in which private security surveillance can invoke Fourth Amendment protection when state actors enter the equation. Even if constitutional privacy protections are not implicated, tenants can seek policy statements and guarantees from their landlords governing the use of such data.

III. General Privacy Concerns and Rights

The law imposes virtually no limitations on a commercial property owner's deployment or archiving of access control and video surveillance within the lobby and common facilities of a property, or on the building's exterior.[69] By contrast, audio surveillance is regulated by various state and federal regulation, notably the Omnibus Crime Control & Safe Streets Act of 1968 (i.e., the Federal Wiretap Act), which courts have held "does not include silent video surveillance."[70] But the fact that a property owner is allowed to deploy surveillance cameras or access control systems does not entail the loss of all privacy rights. Indeed, absent relevant contractual provisions or adequate notice, tenants and even visitors of office buildings may establish reasonable expectations of privacy in certain situations.

There are three sources from which the conception of privacy rights in the surveillance context emerges: Fourth Amendment constitutional protections, federal and local privacy statutes, and common law tort. The accumulation of access control data and surveillance camera footage obtained and archived for commercial real estate security purposes are not subject to constitutional constraint, even if they are considered "searches," since the Fourth Amendment only applies to government action.[71] A search warrant to obtain an owner's video playback archives, for example, may be subject to the Fourth Amendment, while a subpoena in a civil action would not. Similarly, the collusion between private security and public law enforcement may also be subject to the

[69] As any private property owner or employer, a commercial landlord may be restricted from installing surveillance cameras within stalls or other sensitive areas within restrooms. *See* Burrows, *supra* note 60, at 1120 n.247.

[70] *United States v. Koyomejian*, 970 F.2d 536, 538 (9th Cir. 1992).

[71] *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921); *see generally* Major Gary J. Holland, *Search and Seizure – Situations Where the Fourth Amendment Does Not Apply: A Guide for Commanders and Law Enforcement Personnel*, 1988 Army Law. 57 (1988).

Fourth Amendment, as discussed in the next section. Yet civil plaintiffs who believe building security has violated their personal privacy can turn only to state or municipal privacy statutes, if applicable, and the common law to bring tort actions against property owners.[72]

Of the four classical invasion of privacy torts, three are applicable to a property owner's use (or misuse) of access control and video surveillance data: (1) intrusion into one's seclusion, solitude, or private affairs; (2) public disclosure of private, personal facts; and (3) publicity that places a person in a false light before the public eye.[73] In any privacy cause of action, a plaintiff must establish that a reasonable expectation of privacy existed and was violated by defendant's conduct. Establishing a reasonable expectation of privacy is not an easy task in the office building context. Since it parallels Fourth Amendment reasonableness requirements, it is instructive to turn to constitutional law for guidance concerning the issues of location and notice.

1. *Location*

The Fourth Amendment, as interpreted by the Supreme Court in *Katz v. United States*,[74] provides for a general privacy right where an individual has a reasonable expectation of actual privacy.[75] More recently, the Court has concluded that when invoking privacy protections with respect to a particular location, a defendant "must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable."[76] An initial and potentially determinative factor in a court's evaluation of whether an individual's expectation of privacy was reasonable is the nature of the location – whether the individual was observed within a public, commercial, or private area.

---

[72] *See* Jonathon B. Mintz, *The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain*, 55 Md. L. Rev. 425, 432-33 n.37-39 (1996) ("[Forty-one] states [and the District of Columbia] recognize an invasion of privacy action for the public disclosure of private facts through their common law, but they also address privacy concerns in constitutional and statutory contexts. For example, four states statutorily recognize an individual invasion of privacy action for the disclosure of private facts, ten states have a constitutional right to privacy, and thirty states have rape shield statutes that prohibit the disclosure of identifying information concerning victims of sexual crimes.").

[73] *Id*. at 431-32 (citing William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 389 (1960)).

[74] *Katz v. United States*, 389 U.S. 347 (1967).

[75] Robert D. Bickel, Susan Brinkley & Wendy White, *Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?*, 33 Stetson L. Rev. 299, 307 (2003).

[76] *Minnesota v. Carter*, 525 U.S. 83, 88 (1998).

A. Building Exterior

Properties in major U.S. cities are typically bounded by public sidewalks and streets, and actions in plain-view thereon are generally not afforded any privacy protections, which cannot exist absent a reasonable expectation of privacy.[77] Actions observed by building security personnel or surveillance cameras that take place either on public streets or on private property (regardless of whether on that building's property or an adjacent owner's) are not subject to any privacy right protections so long as they are readily observable by the public.[78] Likewise, access control data logs of individuals entering and exiting a building into a public area, such as a city street, would not be subject to privacy protections because such actions are in plain view of the public. Even if the observation were made through an adjacent building's window with a video surveillance camera's telephoto lens, the subject would not have a reasonable expectation of privacy so long as he could have been observed from somewhere at street level with the naked eye.[79] However, the Second Circuit identified a complication to this rule in *United States v. Paulino*, where the court observed: "what is knowingly exposed to the public through an open door or window in a home or office is not entitled to Fourth Amendment protection; on the other hand what a person, even in a public place, tries to keep private may be entitled to such protection."[80]

Paulino turned on the question of whether a passenger in an automobile has a reasonable expectation of privacy when the subject's furtive movements were readily observable through the vehicle's window.[81] The *Paulino* court implicitly attached great significance to the issue of notice, which is reasonably assumed when actions are visible to the public.[82] While it is clear that in most circumstances an individual does not have a

---

[77] *See United States v. Davis*, 326 F.3d 361, 365 (2d Cir. 2003) ("What a person knowingly exposes to the public . . . does not receive Fourth Amendment protection."); *Rodriguez v. United States*, 878 F. Supp. 20, 24 (S.D.N.Y. 1995) ("As the activity monitored by the video surveillance occurred entirely within a public place, Rodriguez had no reasonable expectation of privacy on the public street.").

[78] *Davis*, 326 F.3d at 365; *Rodriguez*, 878 F. Supp. at 24.

[79] *United States v. Paulino*, 850 F.2d 93, 96 (2d Cir. 1988).

[80] *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 351-52 (1967)).

[81] *Id.* at 94.

[82] Note that some commercial buildings place stanchions, bollards, or planters at varying distances from their superstructures to demarcate property, control traffic, or provide a security buffer from the possibility of vehicular explosive devices (such measures often intrude on public property or would violate zoning restrictions and require municipal approval, while others are erected or financed by the municipality). Though I have encountered no such cases, it is unlikely that a court would draw any distinction between an individual who acts within such a perimeter and one who acts outside it so long as the action is in plain view. *See* Huston Dawson, *Planters and Bollards Make for Safer Buildings*, 52 Real Estate Weekly 51, § B (Construction & Design), at 7C (2006).

reasonable expectation of privacy when outside of a building and observable to the public, whether an individual can be expected to be on notice that his actions are readily observable if inside a restricted access area of the building is less clear.

B. Public Access Lobby Areas

The open-access portions of a commercial office building's lobby (including atriums, concourses, etc.), as opposed to restricted-access common tenant areas within the building's security perimeter, are accessible to the general public just like a retail store or other commercial establishment. Because actions performed in a public access lobby are presumed to be in plain view of passersby, no tenant may reasonably consider a public access lobby to confer privacy rights with regard to the building's security surveillance unless the lease explicitly provides to the contrary. Likewise, no visitor to a public lobby may reasonably presume the conferral of any privacy rights therein, it being common for medium and large commercial buildings in major U.S. cities to maintain some level of lobby surveillance, whether by building personnel, surveillance cameras, or both.

Privacy expectations and protections within a video-monitored public access lobby are similar to those associated with any retail store or other commercial establishment utilizing a video surveillance system. Case law concerning such commercial venues is applicable to open-access lobby areas. In *United States v. Vega*, the Southern District of New York held that an individual is essentially on notice by default in certain commercial venues: "the defendant was present in a public place where commercial transactions were the regular course of business . . . the defendant should have expected to be viewed by anyone who entered" the premises.[83] In *Vega*, the defendants, who were charged with conspiracy to distribute and possess with intent to distribute cocaine, sought to suppress critical video surveillance recorded pursuant to a warrant in a liquor store, arguing they had a subjective expectation of privacy regarding non-verbal actions within the commercial establishment.[84] The court disagreed: "Even if the defendant had a subjective expectation of privacy in the liquor store, it was not a legitimate or reasonable expectation,"[85] thus failing the reasonableness test of *Minnesota v. Carter*.[86]

But the *Vega* court proceeds to raise an issue which points to a potential distinction between a building's lobby and a retail store, citing the Second Circuit's observation that "the court generally considers whether the defendant had any property or possessory interest in the place searched or the items seized,"[87] reasoning that the defendant "did not own the liquor store and he did not work there, facts which might

[83] *United States v. Vega*, 309 F. Supp. 2d 609, 613 (S.D.N.Y. 2004).

[84] *Id.* at 612.

[85] *Id.* at 613.

[86] *Minnesota v. Carter*, 525 U.S. 83, 88 (1998).

[87] *United States v. Osorio*, 949 F.2d 38, 40 (2d Cir. 1991).

otherwise support a claim to a legitimate expectation of privacy."[88] In cases where a lessee has a "property or possessory" interest in the building's lobby, the lessee could make the argument under this case law that he is entitled to greater privacy expectations and protections than a visitor who lacks such an interest. Individuals who successfully establish a property or possessory interest in the lobby could theoretically recover via a tort action for invasion of privacy, but only if they can establish the elements of a cause of action for intrusion into one's seclusion, solitude, or private affairs: that (1) plaintiff had a reasonable expectation of privacy; (2) a privacy intrusion existed that would be offensive to a reasonable person; (3) there was no legitimate business justification for the intrusion.[89]

Plaintiffs are unlikely to establish a cause of action in these circumstances for two reasons. First, it would be very difficult for plaintiffs to establish a reasonable expectation of privacy in a public access lobby. Second, it would also be difficult for plaintiffs to establish that no legitimate business justification for the privacy intrusion exists since there are many valid business justifications for video surveillance in commercial lobbies (e.g., *ex ante* theft deterrence and *ex post* suspect identification).

C. Restricted Access Common Tenant Areas

Areas within the secured confines of an office building such as private lobbies, stairways, hallways, elevators, eateries, lounges, and parking garages are only accessible to tenants and allowed visitors. That tenants and visitors are often unaware of the extent of video recordings and access control logs maintained by commercial buildings within these areas is a complicating factor with respect to privacy rights, because expectations of privacy hinge on whether or not individuals reasonably believe they are being monitored.

Courts have consistently refused to establish reasonable expectations of privacy in the common areas, elevators, escalators, or stairwells of residential buildings.[90] There is generally no reason for a court to distinguish between commercial and residential buildings when determining the reasonableness of a particular individual's privacy expectation in areas freely accessible to others. Three hypothetical situations, however, raise what I believe are valid arguments that reasonable expectations of actual privacy can exist in the common areas of commercial buildings that could not exist in a building's publicly accessible areas. All suggest that the simplest solutions to the problem exist in the landlord-tenant contractual arena and via adequate notice.

---

[88] *Vega*, 309 F. Supp. 2d at 613.

[89] Elizabeth Adelman, *Video Surveillance in Nursing Homes*, 12 Alb. L.J. Sci. & Tech. 821, 833 (2002).

[90] *People v. Farrow*, 642 N.Y.S.2d 473, 475 (Crim. Ct. 1996); *see also In re Application of the U.S. for an Order Directing X to Provide Access to Videotapes*, No. 03-89, 2003 WL 22053105 (D. Md. Aug. 22, 2003) (granting the government access to a private residential building's surveillance archive in order to locate a fugitive because the building's occupants lacked reasonable expectations of privacy concerning their ingress and egress through the building's common entryway and hallway, therefore not implicating the Fourth Amendment).

To illustrate, suppose a tenant's jealous wife suspects her husband of having an affair during business hours with a coworker on a different floor within the building. The wife then bribes the unscrupulous property owner to obtain the building's access control logs and video surveillance footage, detailing her husband's movements between floors within the restricted-access confines of the building. The husband finds out and brings a tort action against the property manager for intrusion into one's seclusion, solitude, or private affairs. He claims that although he was aware that the building maintained and recorded surveillance of people entering and leaving the building, he was not aware such surveillance was conducted or recorded beyond the publicly accessible portion of the lobby. He further contends that had he been aware of the existence of such security systems in the building's interior, he would have insisted on a contractual provision in his lease restricting the property manager's use of the database exclusively to building security matters.

The common law invasion of privacy for unreasonable intrusion upon the seclusion of another is recognized to apply specifically to workplace settings in California, Florida, Pennsylvania, and Texas.[91] Courts typically balance the interests of the parties involved when evaluating a plaintiff's claim in this type of suit as noted above, examining whether the plaintiff has established a reasonable expectation of privacy, an intrusion that would be offensive to a reasonable person, and an absence of a legitimate business justification for the intrusion. The most difficult aspect to prove here is the husband's purported reasonable expectation of privacy with respect to movements that were readily observed by other tenants and building personnel within the building. But assuming the access control system prevented the jealous wife or her agents from entering the building, only the husband's ingresses and egresses to and from the building were in plain view to the public, in contrast to his intra-building movements between floors. Courts have followed this line of reasoning before,[92] as will be further discussed in the ensuing hypothetical.

Next, suppose a tenant's slip and fall, which reveals she was carrying a bag full of syringes and leads onlookers to make false assumptions, is recorded by surveillance cameras in a restricted access common area within a commercial building. Finding the security footage of the incident hilarious, the property manager copies and mails it to a 'Funniest Videos' television show. Horrified to see her embarrassing fall and recognizable face on a major television network, the tenant brings suit against the property owner and manager for defamation and invasion of privacy. The tenant alleges that the defendant's actions resulted in tortious public disclosure of private, personal facts and publicity that places a person in a false light before the public eye.

Even though her fall was readily observable by other tenants and there are virtually no state or federal restrictions on the use of archived commercial surveillance footage,[93] a court could determine that the building's actions here were indeed tortious.[94]

---

[91] Adelman, *supra* note 89, at 833.

[92] *Huskey v. Nat'l Broad. Co.*, 632 F. Supp. 1282, 1288 (N.D. Ill. 1986).

[93] Bob Barr, *A Tyrant's Toolbox: Technology and Privacy in America*, 26 J. Legis. 71, 72 (2000).

Such a determination could follow the reasoning of *Huskey v. NBC*, which held that "visibility to some people does not strip him [plaintiff] of the right to remain secluded from others. Persons are exposed to family members and invited guests in their own homes, but that does not mean they have opened the door to television cameras."[95] The *Huskey* case concerned an incarcerated inmate who was videotaped and appeared in a nationally televised broadcast. A court could reasonably apply the reasoning in *Huskey* to determine that the property manager's actions here were tortious, because the mere fact that an event is observable to certain others does not entail a right to televise the event to the public without an individual's consent since the event was not in plain view of the public. This reasoning would not apply had the slip and fall occurred where it would have been readily observable by the general public, such as the building's lobby or exterior, except in certain situations of improper use or commercial sale of the footage.

In a third and final hypothetical, suppose an employee of a tenant company enters an elevator with his client and, while the elevator is in motion and no other occupants are present, the employee hands a confidential document to his client detailing the financial health of another of the firm's clients. Surveillance footage from an unobtrusive camera in the elevator car, records and archives its images, clearly showing the exchange. The Securities Exchange Commission brings a civil and criminal suit against the employee (as well as the client), claiming that the exchange and subsequent acts constituted insider trading. At trial, the employee's counsel moves to suppress the video surveillance, arguing that the employee had a reasonable expectation of privacy in the elevator and that the government's warrantless search had violated the employee's Fourth Amendment privacy protections.

If the employee received no notice from either his tenant company (which may or may not have known of the elevator surveillance camera) or from the property owner that cameras were deployed in the elevators and, if so, that footage was recorded, his motion may prove successful. If the employee can establish that the camera was not readily observable and hence he had no constructive notice, that he had no actual notice of its existence, and that because the elevator car was moving it was reasonable to conclude that no one could observe the exchange, he may be able to establish a reasonable expectation of privacy. However, absent government involvement in the surveillance, exclusion will not occur. The issue of invoking Fourth Amendment protections when governmental actors conducted or encouraged the surveillance will be discussed in Section IV of this Note.

---

[94] *See, e.g., Sharrif v. American Broadcasting Co.*, 613 So. 2d 768 (La. Ct. App. 1993) (holding musicians filmed falling on stage by an unauthorized cameraman and aired on two "Funniest Home Videos" television shows had stated a valid cause of action for determination by a trier of fact).

[95] *Huskey*, 632 F. Supp. at 1288.

2. *Notice*

Commercial real estate access control and video surveillance remain virtually unregulated. In the commercial context, "the reality is there are virtually no legal restrictions on how a company can monitor its customers and what it can do with the footage. So long as a person's image is not sold commercially, very few, if any, legal protections apply."[96] Office building security has developed in such a manner as to become part of the larger "growth of informational technologies, such as e-mail, data warehousing, the Internet, surveillance systems, and personal identifiers, [that] has far outpaced the development of a legal structure to safeguard personal information from government, criminal, or commercial abuses."[97] One possible solution to the privacy concerns discussed in this section may be accomplished on an individual basis via notice by contract or unilateral notice. An advantage of this solution is that it can be accomplished without regulation and can thus be tailored to meet the range of needs that different landlords and tenants require. The government and criminal context will be discussed in the final section of this Note.

Since commercial leases and lease negotiations already encompass a wide range of issues concerning the landlord-tenant relationship, provisioning for building security requirements, restrictions, and procedures would be a readily accomplishable task. Because the security needs of different tenants and commercial properties vary greatly in stature and threat levels, the interests of both tenants and landlords are best served when freedom of contract is preserved in this area. Even if rules and regulations are promulgated governing certain aspects of access control and video surveillance, it is unrealistic to suppose that such policies will so adequately address relevant security issues as to satisfy tenants and landlords across the board.

In the event a lease does not include security details or provisions, a landlord can eliminate most potential issues and disputes by providing unilateral notice to tenants and visitors of security deployments and policies. A landlord may provide such notice via signage or written notification. It is generally advisable for a landlord to provide unilateral notice regardless of whether security provisions are dealt with contractually, since doing so ensures that all building occupants and guests are notified of a particular building's security policies and procedures. Such notice should mention the existence of access control and video surveillance systems, monitoring and recording procedures, and the approximate duration or permanency of database and footage archives. I am not alone in suggesting this course of action. As Congressman Bob Barr has stated, "private companies that engage in surveillance should be required to notify their targets unless they have a compelling reason not to do so and comply with constitutional safeguards."[98]

Higher educational institutions have taken the lead in providing notice of security surveillance, policies, and procedures to university affiliates and the public. Such unilateral notice policies can serve as models for commercial property owners. For

[96] Barr, *supra* note 93, at 72.

[97] *Id.* at 71.

[98] *Id.* at 87.

example, Johns Hopkins University makes available in hard copy and on the Internet its "Closed Circuit Television (CCTV) Monitoring and Recording: Standard Operating Procedures," in addition to signage giving notice of outdoor video surveillance.[99] The policy details the purpose and use of the video surveillance, as well as the Monitoring Center's responsibilities, procedures, and quality assurance safeguards. Commercial property notice policies need not and should not be uniform. Rather, they should accurately reflect the policies of a given building just as city and state agency surveillance policies vary to meet their unique surveillance programs.[100]

While some may contend that monitoring and archiving policies or other forms of notice undercut the value of the security technology and facilitate evasion, this argument has little basis. Security policies and notice should not divulge the operational specifics of a facility's security deployment. Except in the rare case that a building maintains an armed security force or is such a high-profile target as to incorporate law enforcement officers into its security detachment, the object of access control and video surveillance is to deter criminals and terrorists. While the value of these systems in identifying and apprehending criminals or terrorists *ex post* is important, it is outweighed by the potential value of the systems to deter criminal or terrorist acts from happening in the first place. Notice of security technology is the most practical means of deterrence for most properties and has the potential not only to aid in the recovery of property and apprehension of suspects, but also to save lives.

IV. PRIVACY RIGHTS AND GOVERNMENT ACTION: LAW ENFORCEMENT AND THE WAR ON TERROR

The Fourth Amendment is a cornerstone of privacy protection from local and federal government surveillance, but as discussed above, it is largely inapplicable to private action.[101] However, the distinction between public and private action blurs when private actors actively cooperate with, or assume the role of, government authorities. Two factors have combined in recent years to increase the likelihood of information sharing and collusion between building security and law enforcement: first, the 9/11 attacks encouraged law enforcement agencies to open lines of communication with building security managers;[102] second, the post-9/11 proliferation of technologically-

[99] Johns Hopkins University Campus Safety and Security, http://www.jhu.edu/~security/overview_CCTV.html (last visited Jan. 20, 2007).

[100] *See generally* Burrows, *supra* note 60, at 1124 ("To discourage unauthorized distribution of information, Baltimore, Maryland, destroys or recycles tapes after 96 hours and Tacoma, Washington, does not even use tapes.").

[101] *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921).

[102] Through both the New York City Police Department Area Police/Private Security Liaison (established in the 1990s in limited police precincts in Manhattan, centrally commanded and staffed post-9/11) and the Counter Terrorism Division's NYPD Shield (established in 2004); the A.P.P.L. was incorporated into NYPD Shield in May, 2006.

advanced video surveillance and access control systems offer the potential to provide more accurate and useful footage and data to authorities than ever before.[103]

The Supreme Court has formulated the basic groundwork for determining whether constitutional rights and protections are implicated by ostensibly private searches. The Court first established what has become known as the public function doctrine in *Marsh v. Alabama*, where constitutional restrictions were held to apply to a privately contracted policeman who made an arrest in a company-owned town.[104] The public function doctrine has been applied to private security as follows:

> The public function strand of state action theory states that when a private citizen performs tasks and exercises powers that are traditionally governmental in nature, he will be treated as a government actor. He will be subject to the same restrictions as the government, even in the absence of direct contact between him and a government official or agency . . .
>
> The public function doctrine logically applies to private security cases. Policing is one of the most basic functions of the sovereign. When security personnel who are hired to protect business premises arrest, question and search for evidence against criminal suspects, they perform traditional public police functions.[105]

To determine whether the act of a private person was "essentially a public function"[106] and therefore implicated constitutional protections, the Court in *Coolidge v. New Hampshire* established what has become known as the agent or instrumentality test.[107] In *Coolidge*, a suspect's wife voluntarily gave police incriminating evidence, which the defendant argued was obtained in violation of the Fourth Amendment because at the time the wife "was acting as an 'instrument' of the officials, complying with a 'demand' made by them."[108] The Court disagreed, examining the wife's motivation and determining that she had not acted "as an 'instrument' or agent of the state when she produced her

---

[103] While specifics will not be mentioned here for sensitivity reasons, law enforcement often requests volunteer turnover of archived surveillance from private security – and such requests are usually granted.

[104] *Marsh v. Alabama*, 326 U.S. 501 (1946).

[105] Steven Euller, *Private Security and the Exclusionary Rule*, 15 Harv. C.R.-C.L. L. Rev. 649, 657-58 (1980).

[106] As required by *Marsh*, 326 U.S. at 506.

[107] *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971); Lynn M. Gagel, *Stealthy Encroachments Upon the Fourth Amendment: Constitutional Constraints and their Applicability to the Long Arm of Ohio's Private Security Forces*, 63 U. Cin. L. Rev. 1807, 1822-24 (1995).

[108] *Coolidge*, 403 U.S. at 487.

husband's belongings" because "Mrs. Coolidge described her own motive as that of clearing her husband, and that she believed that she had nothing to hide."[109]

Two hypothetical scenarios display the strengths and shortcomings of applying the public function doctrine and the agent or instrumentality test in the office building security context. First, suppose the Federal Bureau of Investigation (FBI) requests building management to retain recordings until further notice and provide access to archived data for all access control, visitor check-in, and video surveillance systems for a tenant company believed to be affiliated with terrorist organizations. If management agrees, does the government participation in the private security operations of the building trigger Fourth Amendment protections for the "search" of the tenant's employees and visitors?

Consider first the *Coolidge* Court's focus on the motivations that instigate the search. The issue is complex because on the one hand, the government requested the instigation of the surveillance, while on the other hand the data and footage requested would have been recorded regardless of the government's request. Had the Bureau set up its own video surveillance, access control, and visitor check-in systems under the auspices of building security, the action would clearly invoke Fourth Amendment protections. Yet courts have also held acts of private security to constitute *de facto* government actions when private security acted alone but was directed or encouraged to do so by law enforcement.[110] A standard for determining whether government participation in a private search meets the threshold to constitute government action was stated by the D.C. Court of Appeals:

> The decisive factor . . . is the actuality of a share by a federal official in the total enterprise of securing and selecting evidence by other than sanctioned means. It is immaterial whether a federal agent originated the idea or joined in it while the search was in progress. So long as he was in it before the object of the search was completely accomplished, he must be deemed to have participated in it.[111]

This case law suggests that Fourth Amendment privacy safeguards bind the conduct of both the government and private security so long as government actors were involved to some degree (the extent to which remains to be tested) in the search. Thus, evidence obtained by building security technologies will likely be excluded if law enforcement agents participated in surveillance that violated an individual's constitutional privacy protections. But as noted above, exclusion will not occur absent government involvement in the search.

---

[109] *Id.* at 487-89.

[110] *Tarnef v. State*, 512 P.2d 923, 934 (Alaska 1973); Euller, *supra* note 105, at 655.

[111] *Moody v. United States*, 163 A.2d 337, 340 (D.C. 1960) (quoting *Lustig v. United States*, 338 U.S. 74, 79 (1949)).

The hypothetical is distinguishable from *Coolidge*, in which the private actor conducting the search voluntarily did so without suggestion from law enforcement.[112] As in the Ninth Circuit's *United States v. Walther* case, a court could find that there was no legitimate business reason for building security to pay extra attention to the tenant company absent a direct threat to the building's security and, therefore, building personnel had assumed the role of a government agent.[113] Thus, the Bureau's request in the hypothetical would invoke constitutional protections under *Walther* if the building management had no reason to conduct the surveillance aside from the encouragement of a law enforcement agency, because "the government cannot knowingly acquiesce in and encourage directly or indirectly a private citizen to engage in activity which it is prohibited from pursuing [without a warrant] where that citizen has no motivation other than the expectation of reward for his or her efforts."[114] Surveillance within areas of a building closed to the public, conducted or encouraged by the government utilizing or supplementing building security systems rather than obtained via confidential informants, can constitute an intrusion on reasonable privacy expectations.

In the first hypothetical, the government merely encouraged the archiving of data already recorded on a regular basis. Here, the counter-argument that the building management was not conducting any additional data and surveillance recording than was collected from all tenants on a regular basis by the building's access control database, surveillance system, and check-in procedures is bolstered by the Supreme Court's decision in *United States v. Jacobsen*.[115] In that case, the Court held that "federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct" because the search they conducted after being summoned by employees of a private freight carrier did not exceed the scope of the prior private searches that were legally conducted.[116] This line of reasoning has been adopted by the Eighth Circuit[117] and suggests that mere government encouragement of existing private security surveillance does not violate the Fourth Amendment.

Further, the Supreme Court has held that "when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."[118] Thus, neither a tenant nor a visitor who

---

[112] *Coolidge*, 403 U.S. at 489.

[113] *United States v. Walther*, 652 F.2d 788 (9th Cir. 1981).

[114] *Id.* at 793.

[115] *United States v. Jacobson*, 466 U.S. 109 (1984).

[116] *Id*. at 126.

[117] *United States v. Mithun*, 933 F.2d 631 (8th Cir. 1991).

[118] *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984); *see also United States v. Miller*, 425 U.S. 435, 443 (1976) (holding that an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government").

reveals information to a building's security staff can object on privacy grounds should private security provide that information to the government. This rule is clearly applicable to information that an individual "reveals"[119] or "communicates,"[120] such as social security number, contact information, driver's license number, or any other personal information maintained in tenant and visitor databases that has been volunteered to the property management or security staff. The rule is most likely not applicable, however, to access control data and video surveillance footage for two reasons. First, while such systems passively monitor and record behavior, individuals do not actively "communicate" or "reveal" information to them, at least not in the context of the *U.S. v. Miller* and *SEC v. O'Brien* decisions. Second, there is a strong implication in both cases that the information imparted to the third party is done knowingly. In the absence of notice of video surveillance, contractual or posted, it would be difficult to establish that the mere presence of an individual in an area under surveillance would be considered to be revealing information to the building security staff.

A second hypothetical sheds much of the complexity of the first in order to present a clear distinction between government and private instigation of surveillance. Suppose that one of two scenarios occur: either the Bureau requests from building management the access control database and video surveillance footage archives that pertain to a certain tenant company suspected of terrorist affiliations, or the building's security manager begins to suspect a certain tenant of terrorist activities and contacts government authorities. In either scenario, the government has refrained from instigating the search and therefore has not reached the *Coolidge* agent or instrumentality threshold until such time as the Bureau requests or encourages building security to increase its surveillance procedures for the tenant, or for all tenants in the building.

If building management voluntarily hands over access control and video surveillance archives to law enforcement without any request or encouragement to do so, neither the tenant nor its visitors can invoke Fourth Amendment protections because constitutional protections cannot be invoked absent state action.[121] The same is true even if the building's search could be considered unreasonable.[122] This is not to say that neither the tenant nor its visitors could bring a tort action for violation of privacy.[123] When the archived surveillance is requested, however, a reviewing court must examine whether the building management anticipated any reward from government authorities

---

[119] *Miller*, 425 U.S. at 449.

[120] *SEC*, 467 U.S at 743.

[121] *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921); *see also United States v. Feffer*, 831 F.2d 734 (7th Cir. 1987) (holding an employee's voluntary turn-over of company documents to the Internal Revenue Service was purely voluntary).

[122] *United States v. Jacobson*, 466 U.S. 109, 113 (1984); *Walter v. United States*, 447 U.S. 649, 662 (1980).

[123] *See supra* Section I.

for providing the surveillance archives.[124] Should the building management have a legitimate and direct interest in handing the archives over to law enforcement, such as a reasonable belief that other tenants or the building itself is at risk, Fourth Amendment protections could not be invoked. But if a court were to find that the building management had no interests "other than the expectation of reward for his or her efforts," the tenant may be able to invoke Fourth Amendment protections unless the government can establish that (1) it did not instigate the search and (2) the government did not suggest or encourage any search that exceeded the scope of routine building security surveillance and procedures. If the government fails to demonstrate either, the court could find that a "sufficiently close nexus" exists between private activity and state activity to classify the activity as public.[125]

CONCLUSION

The events of 9/11 have had a significant impact on office building security in high-risk areas. To overcome the possibility of negligent security lawsuits, property owners must reevaluate the security provided in their buildings on an ongoing basis. Fortunately, innovations in security technology within the last ten years offer cost-effective means of satisfying security minima for a majority of commercial properties. Access control and video surveillance systems as well as information sharing help to make buildings safer and more secure, and they have already begun to prove invaluable both in terms of *ex ante* deterrence and *ex post* apprehension. Yet the benefits of security technologies must be weighed against potential privacy infringements. Property owners should consider contractual and unilateral notice of security monitoring and recording practices. Furthermore, property owners should balance the need for public-private information sharing with the need to safeguard the privacy rights of building occupants and the public. While with innovations come the potential for misuse, the benefits of security technology substantially further the cause of safety and security in commercial office buildings.

[124] *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971); *United States v. Walther*, 652 F.2d 788, 793 (9th Cir. 1981).

[125] *Jackson v. Metro. Edison Co.*, 419 U.S. 345, 351 (1947).