SURVEY OF ILLINOIS LAW: THE ILLINOIS SUPREME COURT'S ADOPTION OF THE TORT OF INTRUSION UPON SECLUSION

GEORGE BELLAS* AND AYLA ELLISON**

I. INTRODUCTION

Privacy concerns have grown proportionally with the explosive use of the Internet and computers. The Illinois Supreme Court's recent and significant adoption of intrusion upon seclusion, a privacy tort, as well as evolving law in this area and potential settings in which such claims are likely to arise, reflect the continued evolution of the law of privacy. The Court recognized the tort of intrusion upon seclusion and formalized the elements necessary to prove it in the case of *Lawlor v. North American Corporation of Illinois.*[1] *Lawlor* marks the first time the Illinois Supreme Court has recognized the personal privacy tort, though each of the state's appellate districts had previously recognized it. This decision represents an important evolution in Illinois privacy law that will affect businesses, schools, other state and private institutions, and individuals. With the widely-reported Merion School District "WebcamGate" class action settlement as the template, where many high school students in Pennsylvania were given laptops by the school district that could be activated remotely at any time to spy on the students without their

* George Bellas is the senior partner of the law firm of Bellas and Wachowski in Cook County.
** Ayla Ellison is a graduate of Southern Illinois University School of Law and practices law in Chicago, Illinois.
1. Lawlor v. North American Corp. of Illinois, 2012 IL 112530.

knowledge, cyberspace looms as perhaps the most fertile ground for such abuses and the bringing of this tort.[2]

II. HISTORY

Privacy law, in general, has developed through the common law, although the Illinois Constitution recognizes a citizen's right to be free from invasions by the government.[3] While the Illinois Appellate Courts recognized a limited right to privacy in 1952, it was not until 1970 that the Illinois Supreme Court recognized what it described as the right "to be let alone."[4] The privacy clause in the 1970 Illinois Constitution is broad and comprehensive in scope and does not limit in any way the types of privacy intended for protection, as it was added precisely "for the purpose of creating an additional right applicable to situations *not* covered by the search and seizure provision [of same.]"[5] Intrusion upon seclusion is one of four torts generally recognized under the umbrella of the "right to privacy."[6] The other three torts under the umbrella are, (1) public disclosure of embarrassing private facts, (2) publicity which places a person in a false light in the public eye, and (3) appropriation of a person's name, likeness or identity for trade or advertising purposes without consent.[7]

The tort of intrusion upon seclusion is premised upon an invasion on some protected sphere of privacy.[8] Liability derives from the investigation that invades someone's private domain.[9] Thus, in *Price v. Chicago Magazine*, the court determined there was "no violation of a prisoner's privacy where a magazine publicized the prisoner's racist tattoos, which were easily observable by visitors touring the prison."[10] However, the Second District Appellate Court reversed a trial court's summary dismissal of a plaintiff's claim for intrusion upon seclusion, concluding her ex-employer accessing her personal email account from a work-station computer and reading and printing out dozens of emails detailing her anger and dissatisfaction with said employer after she left the company due to alleged sexual harassment could meet the requirements for the tort if the

2. William Bender, *'Webcamgate' Findings*, PHILLYNEWS, May 04, 2010, http://articles.philly.com/2010-05-04/news/24958354_1_screenshots-laptop-report-disputes
3. IL CONST. art. I, § 6.
4. Leopold v. Levin, 259 N.E.2d 250, 254 (Ill. 1970).
5. People v. Caballes, 221 Ill.2d 282, 318-19 (2006) (emphasis in original).
6. Austin Moore, *Illinois Supreme Court Recognizes New Privacy Tort: Intrusion Upon Seclusion*, March 10, 2013, http://www.heplerbroom.com/blog/illinois-supreme-court-recognizes-privacy-tort-intrusion-seclusion.
7. *Id*.
8. Price v. Chicago Magazine, 1988 WL 61170, 4 (N.D. Ill. June, 1 1988).
9. Russell v. American Broad. Co., 1995 WL 330920, 8 (N.D. Ill. May 31, 1995).
10. *Price*, 1988 WL 61170, 4.

actions were intentional in nature.[11] The invasion into a person's privacy is the key to this new Illinois tort. Other examples of conduct that have been found by various courts to constitute an intrusion upon a person's private sphere include entering someone's bedroom without their knowledge, opening another individual's mail,[12] using another person's name to order items they have not requested through the mail,[13] and taking pictures of employees and customers using the restroom through discrete holes in the wall.[14] Still, until *Lawlor,* the Illinois Supreme Court had never formally adopted the tort.

III. *LAWLOR VS. NORTH AMERICAN CORPORATION OF ILLINOIS*

A. Facts of the Case

In *Lawlor v. North American Corporation of Illinois*, Kathy Lawlor (the Plaintiff) left her commission-based position as a successful saleswoman in North American's (the Defendant's) graphic services group, after working there for several years, to join a competitor company, Shamrock Companies, Inc.[15] Lawlor's primary focus at North American was generating business, while others managed the accounts.[16] Before she departed with North American in June of 2005, Lawlor interviewed with Shamrock. Lawlor began working for Shamrock in August of 2005.[17] After she began her new job with Shamrock, North American undertook an investigation to determine whether Lawlor was contacting their customers in violation of her non-compete agreement with the company.[18] North American asked its longtime corporate counsel, Lewis Greenblatt, to spearhead the investigation, assigning its vice president of operations, Patrick Dolan, to act as the contact point.[19] Greenblatt secured the services of Probe, a private investigation agency, and Dolan supplied Greenblatt and Probe's principal with Lawlor's date of birth, social security number, home address, and cellular and home telephone numbers to assist in the investigation.[20]

Probe then hired another investigative entity, Discover, which, using Lawlor's previously supplied personal information, gained access to

11. Borchers v. Franciscan Tertiary Province of the Sacred Heart, Inc., 2011 IL App (2d) 101257, ¶¶ 12-16, 32-33.
12. Thomas v. Pearl, 998 F.2d 447, 452 (7th Cir. 1993).
13. Melvin v. Burling, 490 N.E.2d at 1013-14.
14. Benitez v. KFC National Management, Co., 714 N.E. 2d at 1006.
15. Lawlor v. North American Corp. of Illinois, 2012 IL 112530, ¶ 4.
16. *Id*.
17. *Id*.
18. *Id*. at ¶ 5.
19. *Id*.
20. *Id*.

Lawlor's personal telephone records.[21] These records provided data on dates, times, duration, and numbers called from Lawlor's landline and cellular phone numbers for the relevant periods in 2005.[22] The records obtained by Discover were forwarded to Probe, who then faxed the information to North American. Company employees were then tasked with verifying if any and which of the numbers belonged to North American clients.[23]

In August of 2005, Lawlor filed suit against North American for allegedly outstanding commissions and sought a declaration concerning the enforceability of the non-compete agreement.[24] Subsequent to learning about her ex-employer's investigation, she amended her complaint to include an intrusion-upon-seclusion claim based upon a "pretexting scheme" where someone pretended to be Ms. Lawlor in order to gain access to her telephone records without her permission.[25] North American filed a counterclaim for breach of fiduciary duty, alleging Lawlor had breached her duty of loyalty by attempting to funnel company business to a competitor while under North American's employ and by sharing confidential corporate sales information with a competitor.[26] North American also sought reimbursement for excess commission draw payments it asserted had been made to Lawlor.[27]

A six-day trial on the respective claims of the parties ensued in September of 2009.[28] North American argued it could not be held liable because Probe was an independent contractor acting on its own accord.[29] The jury disagreed and awarded Ms. Lawlor $65,000 in compensatory damages and $1.75 million in punitive damages.[30] The trial judge remitted the jury's punitive damages to $650,000.[31] A bench trial conducted at the same time awarded North American $78,781 in compensatory damages and $551,467 in punitive damages for its breach of fiduciary duty claim.[32]

The Illinois Appellate Court affirmed the judgment on Lawlor's intrusion claim, reinstated the $1.75 million punitive damages award, and reversed the rulings on North American's breach of fiduciary duty claim.[33]

---

21. *Id*.
22. *Id*.
23. *Id.*
24. *Id*. at ¶ 6.
25. *Id.*
26. *Id*. at ¶ 1.
27. *Id.* at ¶ 6
28. *Id.*
29. *Id*. at ¶ 22.
30. *Id*. at ¶ 1.
31. *Id*.
32. *Id.*
33. *Id*.

On appeal, the Illinois Supreme Court upheld the judgment on Lawlor's intrusion upon seclusion claim finding there was sufficient evidence in the record for the jury to conclude North American had set in motion the process by which the investigators used "pretexting" and even posed as Ms. Lawlor in order to obtain her private information.[34] However, the Court did reduce Lawlor's punitive damages award to $65,000 to match the award of compensatory damages.[35] Significantly, the Court also affirmed the appellate court's denial of North American's breach of fiduciary duty counterclaim, agreeing the "record is entirely devoid of evidence to support the judgment in favor of North American."[36]

B. The Court's Reasoning

In recognizing the tort of intrusion upon seclusion, the Illinois Supreme Court officially adopted the Restatement (Second) of Torts definition which provides: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[37] These elements are similar to those used by many other state courts.

Comment b to Section 652B of the Restatement states, in pertinent part:

> The invasion may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the information outlined.[38]

After opening its analysis with these essential lodestars to establishing the tort, the Supreme Court observed since the last case to raise the issue in Illinois—when a failure to plead the elements precluded the necessity to

34. *Id.* at ¶¶ 51, 56, 82 (Kilbride, Chief J., concurring in part and dissenting in part) (neighbors' observations of cars parked outside Lawlor's house for hours at a time and someone impersonating her to get information as well as Lawlor's intense fear and paranoia in objection to the majority's reduction of her punitive damages to $65,000).
35. *Id.* at ¶ 76.
36. *Id*. at ¶ 71.
37. RESTATEMENT (SECOND) OF TORTS § 652B (1977).
38. RESTATEMENT (SECOND) OF TORTS § 652B cmt. b, at 378-79.

confront the tort's merit—all five appellate districts have expressly adopted the tort of intrusion upon inclusion.[39]

Applying a *de novo* review in line with appellate review of motions for directed judgment and motions for judgments *n.o.v.,* the Court first addressed North American's threshold assertion that a finding for vicarious liability was improper.[40] Initially, the Court pointed out there was no evidence North American contested the actions of Probe and others in obtaining Lawlor's phone records without her authorization. The court deemed those actions constituted an intrusion into her privacy and seclusion, as she had a reasonable expectation of privacy as to those records, and such an intrusion would be highly offensive to a reasonable person.[41]

The Defendant asserted there was no evidence in the record that North American personally received said telephone logs or that any agency relationship existed between North American and Probe or Discover.[42]

The Court stated Lawlor's counterargument asserted an adequate basis for imposing vicarious liability due to the evidence heard by the jury that her ex-employer directed the "pretexting activities" by expressly requesting Probe to obtain those logs.[43] Moreover, North American was the source for Lawlor's personal information such as her date of birth, social security number, and private address.[44]

Lawlor also contended the Defendant was bound by a "judicial admission" in Greenblatt's affidavit in which he avers that both Probe and Discover were acting as his agents.[45]

The Court then cited the doctrine of *respondeat superior* for the rule of law that a principal may be held liable for the actions of an agent even though he participated in none of the conduct himself, followed by the general rule that an agent is not liable for the conduct of an independent contractor.[46] Crucially, however, the Court also cited the influential *Holabird & Root* decision for the point of law that the mere status of independent contractor does not bar liability for the principal if the contractor is also acting as an agent.[47]

Touching upon the bedrock principle in agency law that the cardinal factor concerns whether the principal had the right to supervise the manner of the agent's performance, the Court concluded, after consideration of the

39. *Lawlor*, 2012 IL 112530, ¶ 34.
40. *Id*. at ¶¶ 37, 40.
41. *Id*. at ¶ 40.
42. *Id*.
43. *Id*. at ¶ 22.
44. *Id*. at ¶ 41.
45. *Id*. at ¶¶ 40-41.
46. *Id*. at ¶ 42.
47. *Id*. at ¶¶ 42-43.

record, it cannot be said that there was a complete lack of evidence supporting the jury's inference Probe and its subagent Discover were acting within its scope as North American's agent.[48] The Court also referred to the many faxes received by vice president Dolan detailing the information found by Probe and Discover in the phone logs along with follow-up questions by Dolan to Probe as to whether it could make further determinations as to whom the numbers belonged.[49] Ultimately, the Court concluded:

> Our standard of review is a high one, and based upon the evidence presented by Lawlor, it was not unreasonable for the jury to conclude that North American's conduct was consistent with a principal exercising control over its agent by directing it to obtain specific information and providing it with the necessary tools to accomplish the task.[50]

Accordingly, the Court affirmed the Appellate Court's denial of North American's motions for directed verdict and judgment *n.o.v.*, concluding that the jury's finding of an agency relationship cannot be said to be against the manifest weight of the evidence.[51]

Returning again to the Defendant's arguments, it is critical to understand that because no objections, whatsoever to the sufficiency of the Plaintiff's allegations regarding the elements of the tort of intrusion upon seclusion were made, once the agency relationship was established, the Court's analysis as to the tort were done.[52] No analysis of the facts of the case as they are applicable to the elements of the tort of intrusion upon seclusion was undertaken.[53] This is both significant and legally portentous, because it has opened the doors to the use of a new tort, but is also a case that does not include any judicial analysis of the facts of the case within the context of meeting the tort's elements. Unlike other cases of first impression for the Supreme Court where it has set forth a template or blueprint for other courts to follow, this one will simply—at least for now—have to be imagined or gleaned from the few passing kernels, which appear in the opinion, and from the rulings in the appellate courts. For the present time, what is clear is that using investigative entities to do the "dirty work" of rummaging through an ex-employee's personal phone records or other personal information will not pass muster in evading liability.

If there is a part of this ruling in which leaves one lacking, it is the Court's decision to cut down the jury's award of $1.75 million in punitive

48. *Id*. at ¶ 21.
49. *Id.* at ¶¶ 44, 46, 49-50.
50. *Id.* at ¶ 50.
51. *Id*. at ¶ 53.
52. *Id*. at ¶ 50.
53. *Id*. at fn. 3.

damages to $65,000, a tenth of the remittitur of $650,000 the trial court awarded.[54] Citing another case for this principle, *Slovinski v. Elliot,* the *Lawlor* Court justified further reducing the jury's punitive damages of $1.75 million based on findings the offending conduct was "*de minimus,* fairly much, on all criteria[,]" and therefore, entitling Lawlor to punitive damages which at the most could only equal the compensatory damages awarded ($65,000 in this case).[55]

Chief Justice Kilbride, who wrote a separate opinion concurring in all but this one issue, eloquently framed the punchless deterrent value of this award, first summarizing the evidence in support of the traumatic experience and adverse transformation North American's actions had wrought upon Lawlor:

> Indeed, the majority's error is even more evident here because the record establishes that Lawlor, unlike the plaintiff in *Slovinski,* presented evidence showing significant steps she took to alter both her lifestyle and that of her family, as well as to enhance their security, after she learned her phone records had been improperly obtained by pretexting. . . . Lawlor testified that she immediately became hysterical, vomited, and was "[shaken] . . . to the core." She "didn't go outside," alerted her parents and neighbors to a possible security threat in the area, was ill . . . nervous . . . paranoid [, and] didn't trust anyone."[56]

Justice Kilbride cited a litany of radical daily living modifications and emotional reactions to this experience for someone who testified she had never felt such things before, including severely limiting the activities of her three children, curtailing all sports activities, becoming obsessed with security and passwords for her phone and credit cards, and, even four years later, being stressed out in her marriage, uncomfortable being out in public for long periods with her children and, that, "because of what has been done to her, she doesn't trust anyone anymore."[57] Kilbride also pointed out that the trial judge did not find her testimony lacked credibility.[58]

All of this directly contradicts the majority's claim that "there was no evidence of any alteration in her daily activities," as well as those of her family.[59] As for the Court's conclusion that she had also suffered no physical harm, or to the vomiting and intense stress and nervousness, Lawlor also testified that she was previously a sound sleeper through the night, but after the investigation, she never slept through the night again,

---

54. *Id.* at ¶ 65.
55. *Id*.
56. *Id*. at ¶ 82 (Kilbride, Chief J., concurring in part and dissenting in part).
57. *Id*. at ¶ 84.
58. *Id.* at ¶¶ 83-84.
59. *Id*. at ¶ 88.

arising 3-4 times nearly every night. Her husband also testified that she fell ill much more often and incurred more headaches and stress-related stomach issues after the investigation, which continued unabated long afterwards.[60] Kilbride then points out that North American is a $50 million company, and that in addition to the character of the defendant's act and the extent of the harm to the plaintiff, the wealth of the defendant is the third criterion to be considered.[61] It is also noteworthy that, while in *Slovinski*, the case the Court relied on to arrive at such a minuscule punitive damages award, the intrusive conduct was limited to a single instance, in the case at bar the conduct occurred at least six times, involving strange cars parked on the street across from Lawlor's house for hours at a time and people "impersonating" her to try to obtain information.[62] Finally, Kilbride quotes directly from *Slovinski* regarding the purpose of punitive damages: "Punitive damages 'are not awarded as compensation, but serve instead to punish the offender and deter that party and others from committing similar acts of wrongdoing in the future.'"[63]

Justice Kilbride found it further galling that the majority's rationale for reducing the punitive damages to a mere tenth of that awarded by the circuit court came after its affirmation of the Appellate Court's finding that no evidence existed in support of North American's claim for breach of fiduciary duty.[64] The Appellate Court had reinstated the punitive damages to the full $1.75 million, based in substantial part on its finding that the dismissal of the breach of fiduciary duty claim was warranted.[65] The trial court, on the other hand, had ruled in North American's favor on the counterclaim.[66] Justice Kilbride concluded that for the Illinois Supreme Court to find at once that there was no breach by Lawlor and to further reduce the punitive damages award to one-tenth of the circuit court's award not only defies logic but subverts the entire purpose of deterrence punitive damages stand for.[67]

IV. IMPLICATIONS OF *LAWLOR* AND THE INVISIBLE CAMERA

The broad definition recognized by the Illinois Supreme Court would seemingly encompass a wide range of acts and conduct that could be deemed investigatory. Acts such as impersonation, wire-tapping, and opening another's package or mail would clearly meet the elements

60. *Id.* at ¶ 90.
61. *Id.* at ¶ 92.
62. *Id.* at ¶ 82.
63. *Id.* at ¶ 93 (quoting Slovinski v. Elliot, 237 Ill.2d 51, 57-58, 927 N.E.2d 1221, 1224-25 (2010)).
64. *Id.* at ¶ 76.
65. *Id.* at ¶ 95.
66. *Id.* at ¶¶ 96, 98.
67. *Id.*

recognized by the Court. Intruding upon another's personal space where they have a reasonable expectation of privacy would open the door for an intrusion upon seclusion claim. Failure by employers to closely monitor investigatory acts could lead to potential liability under the new privacy tort. "[T]he court's decision underscores the need for employers to tread cautiously when unearthing or even reviewing personal information relating to an employee."[68]

Following *Lawlor*, it is important for employers in Illinois to understand they can be held liable for these types of acts even when performed by a seemingly "independent" investigator. The principle that employers are liable for the tortious conduct of their employees and agents was revisited in *Lawlor*. The Court held that an employer could be held liable for the acts of a non-employee private investigator in an intrusion upon seclusion claim.[69] As a result, it will be incumbent upon Illinois employers and other similarly situated persons to maintain a vigilant eye toward any investigatory acts whether acting on their own behalf or through another.

A. Cyberspace: The Illusion of Privacy

Nowhere is there a medium more conducive to such furtive activity—and ostensibly more anonymously private—than the portal of cyberspace. A general lay of the land will be presented, followed by a look at one of the most shocking and well-known cases of intrusion upon seclusion to come to light in the modern era.

Technology in general and cyberspace in particular, it seems, is nearly nuclear in its infinite capacity for pathways of acquiring knowledge: knowledge of the world, of others, and of ourselves in the world. "Ego-surfing" allows us to search not only for our own individual presence on the internet, but to discover just how deeply down the rabbit hole the privacy of that presence runs. Updates and improvements in *Google Chrome*, for instance, have now for some time been able to supply us with documentation on when and how many times we have visited certain sites we've been to before. This is default information when *Google* history is turned on. When performing searches and reviewing the hits produced by those searches, the words "You last visited this page on X/X/2013" or even "You have visited this page many times" may appear. It is likely that eventually these kinds of features will be a blanket event, and when that occurs, a plaintiff or defendant who is a party to litigation and has her

68. David Haase, et al. *Illinois Supreme Court Recognizes Privacy Tort and Holds Employer Liable Under Agency Law* (Nov. 1, 2012), http://www.littler.com/publication-press/publication/illinois-supreme-court-recognizes-privacy-tort-and-holds-employer-liab.

69. *Id*.

laptop or workstation computer seized for forensic evidence will find it provides a world of evidence that is easy to produce but not so easily rebuttable.

Lawlor involved company employees utilizing agents on their behalf to troll through the brick-and-mortar world of Lawlor's telephone records via "pretexting" and individuals pretending to be her. But how often has the average person "trolled" the internet in search of private information on someone they know: a romantic interest whose telephone number or email address they've misplaced; personal information on someone they are interviewing with for a position if that information is not readily available: the person's age; where he graduated college; or, what town he grew up in. In this era, knowledge is power, and the ability to perform a string of "searches" on an individual has become the norm. A level of personal detail is acquired in a manner of seconds that might in the past have taken weeks of investigation in the brick-and-mortar world of the "private eye."

Today, enterprising, savvy individuals are able to find enough information on their own, potentially, to find someone close to the target and then contact that person under the guise of being someone they're not in order to obtain more personal information. The possibilities are endless. This also means that in many cases the more initially visible brick-and-mortar steps of such an investigation as demonstrated in *Lawlor* will be collapsed into the secluded—and more protected—domain of the living-room search string.

B. WebcamGate: *Robbins v. Lower Merion School District*

Robbins v. Lower Merion School District was a federal class action lawsuit filed in the U.S. District Court for the Eastern District of Pennsylvania in 2010.[70] In October 2010, the case was settled for $610,000.00.

Beginning in the 2009-2010 school year, Merion School District provided many students, including Blake Robbins, an Apple laptop computer to use at home for school purposes. However, unbeknownst to the students who were issued the computers and their parents, the laptops were equipped with a feature that automatically activated the computers' webcams and snapped pictures of whatever was in front of the webcam, including students in their homes.[71]

Blake Robbins and his parents discovered the laptops had the spying feature when Blake was confronted by the administration at his school and

70. Lower Merion School District and Blake Robbins Reach a Settlement in Spycamgate, Forbes, Oct. 11, 2010.

71. *Id*.

accused of doing illegal drugs. The school used a snapshot of Blake that had been taken in his home using the laptop's spying snapshot feature to accuse him of improper activity.[72]

After being confronted with the snapshot, Blake Robbins joined by others, filed a class action lawsuit against the school for invasion of privacy. The plaintiffs claimed the school knew the webcams had the webcam snapshot feature that automatically activated every 15 minutes, and the school's administration used the feature to spy on students and get a look into their private lives.[73]

When confronted with the class action lawsuit, Lower Merion School District administration claimed they knew the webcams on the laptop computers issued to the students could take snapshots of whatever was in front of them, however, they claimed the feature was only activated when there was suspicion a laptop had been stolen.[74] Lower Merion School District denied the webcam snapshot feature was used by the school district to intentionally spy on students or their families.

Lower Merion School District's defense, based on the webcam snapshots being taken as a security feature when laptops were suspected of being stolen did not hold water since after the class action lawsuit was filed, it was discovered the school district was in possession of 56,000 snapshots that had been taken using the webcam feature.[75]

Lower Merion School District's spying activities, widely condemned in the national media, were cited as a cautionary tale of the potential for abuse and encroachment upon privacy and personal autonomy endemic to the Technological Age.[76]

In *Lawlor*, the Illinois Supreme Court officially adopted the Restatement (Second) of Torts definition, which provides: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[77] Applying that standard to the facts of *Robbins*¸ it is clear the school district committed the tort of intrusion upon seclusion. In *Robbins*, the school district intentionally spied on the activities of the Plaintiffs through the use of the remotely activated webcams incorporated into each laptop issued by the school district. The intrusion by the school district was highly offensive, as the Plaintiffs were unaware of the webcam spying capability, and the school district never

72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.*
77. RESTATEMENT (SECOND) OF TORTS § 652B.

received authorization to use the webcams to spy on the students and their families. Individuals have a reasonable expectation of privacy in their homes, and that was violated in *Robbins*. Additionally, the images captured by the school district may have consisted of images of minors and their parents or friends in compromising or embarrassing positions, including, in various stages of dress or undress.[78] The webcam in *Robbins* was in many ways a modern day peephole.

Robbins illustrates the potential for abuse deriving from computer or Internet surveillance far outweighs that of the traditional brick-and-mortar forms of gumshoe investigation or "peepholes" in the balance of cases previously litigated in Illinois for intrusion upon seclusion. Another employer-related application, with potential significance down the line, concerns employers' access to and examination of employee clickstream data in Intranet or Extranet networks. Clickstream data is the aggregated digital information a system generates while a Web user connects to other computers and networks across the Internet.[79] In short, the very same issues of privacy and intrusion at play in *Robbins* common to a population issued laptops and/or access to networks off-site from their private residences are potential sources of litigation here as well. Employers, schools and other institutions must be vigilant in assuring the monitoring of their employees or charges does not cross over into territories for which they can be found liable. Although *Lawlor* occurred in the private realm and *Robbins* occurred in the public realm, as it involved a school district, it is apparent liability may be imposed in both situations.

V. CONCLUSION

Lawlor has ushered in a new era in Illinois privacy tort law. Employers should have an acute awareness of the liability that can be incurred if improper steps to verify the conduct of an ex-employee, agent, or present employee are taken. The mere delegation of such investigatory steps to others will not avoid liability. The limits of liability have yet to be established and stiffer penalties can be expected to effectively deter such conduct. The Internet and cyberspace will almost certainly be the next realm to test the waters of this tort in terms of significant Illinois jurisprudence on the issue.

78. Official: FBI probing Pa. school webcam spy case, *supra note*, 109.

79. *Introduction: Privacy in the Workplace*, Course Materials for Module III: Privacy in the Workplace, Berkman Center for Internet & Society, Harvard Law School, accessed online at http://cyber.law.harvard.edu/privacy/Module3_Intronew.html#_ftn, last visited on April 1, 2014.