International Journal of Economics, Business and Management Research

Vol. 2, No. 04; 2018

ISSN: 2456-7760

THE EVOLUTION OF EMPLOYEE PRIVACY

Clifford Fisher, David M. Pate

Clinical Professor, Krannert School of Management, Purdue University.

Abstract

In the modern workplace, employers obtain, create, and document a vast amount of employee information to be used for a variety of purposes. The pace of technological progress, while exciting, has led to more people asking the extent to which employers are able to reach for information regarding their employees. From addresses and Social Security numbers to medical and salary information, organizations are the gatekeepers of sensitive, private employee information and must adhere to a complicated set of guidelines regarding such information usage and dissemination. It was found that privacy violations, in summary, are deemed illegal when determined to be unreasonable to both the victim and society at large.

Both employees and employers seek this information in a compact, useful, and timely document that summarizes the main aspects of employee privacy. This paper does just that, introducing and explaining privacy mandates from federal and case law on the subjects of (1) employee records and information, (2) employee monitoring and surveillance, and (3) employee investigations.

Keywords: employee privacy, employee information, employee surveillance, investigations, electronic communication, privacy torts

Introduction

Employers utilize Radio-Frequency Identification (RFID) technologies often, and for good reason— their use improves productivity, efficiency, and accuracy in a large number of fields, from logistics to quality control. In some cases, RFID chips can be planted under an employee's skin, allowing those in possession of such chips access to secure premises. Controversy can arise, however, when employers utilize these chips in other contexts; employee location and movement, discipline, and tracking among such tactics of employer curiosity (Pagnattaro). In the modern workplace, employers obtain, create, and document a vast amount of employee information to be used for a variety of purposes. From addresses and Social Security numbers to medical and salary information, organizations are the gatekeepers of sensitive, private employee information and must adhere to a complicated set of guidelines regarding such information usage and dissemination. The guidelines, stemming from the U.S. Constitution's Fourth Amendment, individual statutes by Congress, specific state statutes, and case law, continue to evolve as additional concerns and situations are addressed with the influx of more infiltrative technology. Such advancements in technology introduces a frightening notion for unsuspecting employees— Big Brother is here, in the form of your employer.

When considering employee privacy, employer encroachment can arise from three basic categories:

Vol. 2, No. 04; 2018

ISSN: 2456-7760

1) Employee Records and Information
   Personnel records such as investigative notes and employee biographical information, as well as medical records and drug testing results are included in this category.
2) Employee Monitoring and Surveillance
   "Supervision" has a new meaning in the digital age, as electronic surveillance in the form of video, audio, keyboard, internet, and phone data has risen dramatically.
3) Employee Investigations
   Investigations into both employee and employer actions bring about the possible searches, interrogations, and interviews of employees related to the subject matter in question.

This review provides a brief overview of each category and, as the title suggests, pays special attention to the gradual evolution of privacy rights and violations from the beginning of the republic. Attention will be given to both employee and employer rights, with special analysis of future privacy issues brought about by technology.

The U.S. Constitution

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (U.S. Const.).

While the implications of the Fourth Amendment are vastly different between public and private employers, there exists in all cases the idea of a reasonable expectation of privacy. When considering a government employer, an employee, when attempting to make a successful claim for a privacy violation, must be considered to have had a reasonable expectation of privacy that was thereafter infringed upon by the employer's (government's) actions. A reasonable expectation of privacy contains two requirements: an individual must actively believe and expect privacy to be upheld, and the expectation is one in which the broader society recognizes as reasonable (Lemons). Employers may negate such ideas of reasonable expectations in court by proving the employee knew, or should have known, the limits of their privacy via employment contracts, company policies, and employee handbooks. While not directly providing the legal foundation of privacy claims for private businesses, the Fourth Amendment inspires and guides current common law precedent and statutes regarding employee privacy rights.

Common Law Precedent

Privacy torts have been the traditionally litigated avenue for claims against employers. Courts have recognized the privacy torts of intrusion upon seclusion, public disclosure of private facts, placement in a false light, and appropriation of name or likeness (Citron).

The most common, intrusion upon seclusion, concerns the snooping, prying, and engagement of unwarranted intrusions into private affairs. The intrusion must be a true intrusion (not in the public realm already) and considered "highly offensive" to a reasonable person to fulfill the elements of a claim. There have been successes and failures regarding employee claims in this realm (Restatement). One example includes an employee whose locker and purse

Vol. 2, No. 04; 2018

ISSN: 2456-7760

(inside the locker) was searched on suspicion of theft. The employee provided her own lock, and although the employer regularly performed searches, the employees were not aware of this policy. The jury found that the intrusion was highly offensive (K-Mart). The intrusion must also actually occur to be legally repairable. An employee who refused to hand over private cell phone records was unable to sue successfully due to the attempted, not successful, intrusion of privacy by the employer (Hellanbrand).

A public disclosure of private facts involves the taking of private, sensitive information and dispersing such information to the public without sufficient carefulness. In order to successfully litigate a public disclosure of private facts claim, the intrusion must be truly private, highly offensive, and involve broad disclosure (Restatement). "Broad disclosure" has been interpreted as reaching the level of knowledge by the "public at large", or of the degree that information becomes "substantially certain to become public." Such a definition arises from *Bodah v. Lakeville Motor Express*, where the employer shared the Social Security number of the employee with 12 regional managers. While the employee suspected the information to be broadly shared, the suspicion alone was not enough to constitute a privacy breach, nor the dissemination broadly disclosed to find the employer guilty of offense.

Other less common tort proceedings include placement in a false light and appropriation of a name or likeness. False light resembles defamation claims, but require broad dissemination of characteristics, conduct, or beliefs that are falsely attributed to the employee in question (McKenna). In one example, Wal-Mart Stores claimed that a suspected employee, Lee, was an "admitted thief," and that Lee, an innocent man, claimed false light after a very public search and seizure at the employee's residence that was broadcasted on radio, the television, and included in the local newspaper (Wal-Mart). Appropriation of a name or likeness, defined as the use of someone's prestige and recognition for commercial gain or personal ends, is also a privacy tort (Walsh).

Statutory Protection

A number of statues involve workplace privacy, whether that be the main purpose of the law or simply a minor side note related to the act's intended purpose. Acts that focus on issues other than privacy yet include such legislation are the National Labor Relations Act (NLRA), Americans with Disabilities Act (ADA), Occupational Safety and Health Act (OSHA), Employee Polygraph Protection Act (EPPA), and the Health Insurance Portability and Accountability Act (HIPAA). Statutes that correspond directly to privacy include the Privacy Act of 1974, Stored Communication Act, and the Electronic Communications Privacy Act.

Personnel Records

The exact ways and means employers handle employee records and personnel files depends more on the specific organization's Human Resource policy than on governmental regulations, as the privacy regulations simply create an overall outline of handling and dissemination of such material (Walsh). For federal agencies, there exists a sweeping Privacy Act, which regulates the

Vol. 2, No. 04; 2018

ISSN: 2456-7760

handling of personal records, including any item, collection, or grouping of information about an individual. The act also notes the kinds of information deemed inappropriate for collection (Government). In a shocking case involving candidates for entry-level attorney positions at the Department of Justice, information on political affiliation was utilized to determine job fit, and candidates who did not oblige to a certain style of political philosophy were rejected. This was not only a privacy issue, but a free speech issue as well, suggesting that privacy law can also support the enforcement of other constitutional rights (Gerlich). Such violations must be willful or intentional, and include an adverse employment action that caused damages to employees.

The protections afforded by the Privacy Act do not transfer to private sector employees. Privacy issues are still contested through tort claims and other statutes. Union employees, for example, have protections under the NLRA, which requires employers to bargain in good faith. This good faith clause has been interpreted by the court to require employers to bargain surveillance policies and relay pertinent employee information in negotiations to union representatives. If employees are not union members, there are typically not such good faith requirements. In all cases of employer encroachment, employee consent has been found to be a quality defense (Walsh).

Typical forms of medical information collected by employers include pre-employment medical exams, job-related medical exams, documents relating to the Family Medical Leave Act (FMLA) for appropriate and mandated employee leave, documents regarding disabilities for ADA compliance, and worker's compensation claims. Medical information is regarded as highly sensitive, more so than other information, in the eyes of the law. The ADA mandates quite a bit of such medical documentation, requiring that the requested employee information be job related and necessary for business (whether or not the employee in question is disabled), and the medical information to be filed separately (physically) or on different systems (electronically). Dillard's broke these regulations when requiring employees to provide extremely specific medical reasons for absences; the court found, after Dillard's could not prove the information to be of business necessity, that a simple doctor's note stating "medical reasons" would be sufficient (EEOC v. Dillard's). It is important to also note that voluntarily contributed information from an employee is not subject to such stringent privacy requirements. There are multiple cases where information was presented to a company without request, and such information shared without laws broken. After responding to an email requesting an excuse for a work absence with extreme medical detail, the sender was surprised to find that, legally, the information could be shared with other employers when on the job hunt. This request was not a medical inquiry, and the information was offered voluntarily, which the laws and courts will permit (EEOC v. Thrivent).

Employers have specific rights related to retrieving job related medical information under the Occupational Safety and Health Act (OSHA). As a public safety concern, the law requires employers to maintain exposure records of toxic substances and harmful physical agents for certain occupations (29 USCS). In almost all medical information discussions, the Health Insurance Portability and Accountability Act (HIPAA) is brought up as a legitimate legal

Vol. 2, No. 04; 2018

ISSN: 2456-7760

concern, and rightly so. Under HIPAA, employers that receive protected health information from outside parties like insurers and healthcare providers must limit the dissemination of such information within the company and the public as a whole. A "need to know" basis, when sharing personal medical information, is an acceptable rule of thumb when considering HIPAA. Companies must also train employees to handle such information legally, notify employees of their medical privacy rights, and designate a "privacy officer" whose sole responsibility is compliance with the law (45 CFR).

Monitoring and Surveillance

Video surveillance has not become a highly litigated issue in the employment privacy realm. Generally, employers have discovered little legal concerns when filming employees, so long that the information obtained is already in public view (Walsh). A public agency was recently sued for Fourth Amendment violations after installing a camera system. The court found that the Fourth Amendment rights of the employees were not insulted due to the public nature of the cameras, the notification to employees of their being, and the limitation of the cameras to visual footage. Employers are more than welcome to electronically observe what they "lawfully can see with the naked eye" (Vega-Rodriguez). In some cases, video surveillance has been found to be illegal, although not for typical privacy reasons. An employer who was found to have videotaped union activities (distribution of literature outside the plant) was in violation of the NLRA (Timken).Other cases where video surveillance has been deemed illegal involve the privacy tort of intrusion upon seclusion. In Koeppel v. Speirs, an employer was charged with installing a hidden camera in a bathroom. The defendant, Speirs, claimed the video camera was not working, and such an argument was considered by the court to be substantive, yet this opinion of the defense was remanded by a later court. There is still a likely division in courts today as to whether an unsuccessful attempt at an intrusion of privacy constitutes legal protection. A majority of courts believe the simple installation of such equipment to be considered an intrusion, citing a violation of the plaintiff's peace of mind and expectation of privacy, whereas others would require intrusive information to be collected successfully to win a case (Koeppel).

Electronic communications monitoring has become a highly litigated issue in the employee privacy realm. The bulk of litigation stems from the Electronic Communications Privacy Act (ECPA), segments of which concern employer obtainment of electronic communication information. Employers are prohibited from both intercepting and storing information received through the use of electronic, mechanical, or other devices, and disclosing such information. There are, however, exceptions to these guidelines when considering the "ordinary course of business", referring to routine, legitimate business interests such as monitoring employee call quality in a call center (Walsh). Interestingly, personal calls can be monitored until discovered that the call is personal, at which the employer must conclude surveillance (Smith).

A hot topic regarding employee privacy today pertains to the social media accounts of employees. In *Ehling v. Monmouth-Ocean Hospital Services Corp*, the social media platform of

Vol. 2, No. 04; 2018

ISSN: 2456-7760

Facebook came into the spotlight. An employee sued for a privacy breach under Title II of the ECPA, formally known as the Federal Stored Communications Act (SCA). The facts of the case include the plaintiff posting on her private Facebook wall a comment about the performance of paramedics in a nearby town (the plaintiff was also a paramedic). The plaintiff, not friends with hospital managers, was friends with coworkers, who could then see the posts the plaintiff created and shared to her friend group. A coworker took a screenshot of said post and shared it with hospital management. Management found the post to be in bad taste and subsequently suspended the plaintiff with pay. Under legal argument, the plaintiff cited SCA as a protection against such surveillance because of the private setting of her Facebook account. To be covered under SCA, the communication must meet four criteria:

(1) Be an electronic communication
(2) That was transmitted via an electronic communication service
(3) Under electronic storage
(4) And not publically available

Although the SCA was created before the invention of the web, the statute has remained helpful when being implemented in social media matters of privacy. The plaintiff, in this case, met all four criteria as her Facebook wall was set to a private mode. Unfortunately, the plaintiff was ultimately unsuccessful in her claim due to a special technicality. The exception to SCA protection considered whether the privacy breach was both authorized and voluntarily supplied. The plaintiff lost because the defendant did not request the information from the plaintiff's coworker (voluntary) and the coworker was a Facebook friend and therefore authorized to view the allegedly private material. In general however, Facebook wall posts on accounts that are set to "private" are protected against employer monitoring and surveillance (Ehling).

Investigations

Investigations of employee conduct and work are vital to the proper functioning of a free business society. In many cases, employers are required to perform investigations. Examples of this include sexual harassment claims, discrimination cases, and criminal law cases such as embezzlement and assault. Some investigations require a search of employee belongings to reveal evidence. Searches, because they are not in plain view, are considered an invasion of privacy if they are not limited by the Fourth Amendment (for governmental agencies) and privacy torts (for private businesses) (Walsh).An example in which such guidelines were not adhered to is Wal-Mart Stores v. Lee, where the plaintiff was coerced into the search, believing a loss of employment would ensue if he did not comply, and the search was overly exaggerated from the initial claim of the searchers. Interviews and interrogations are also a necessary evil in the workplace. Employers can invite trouble when committing false imprisonment during an interrogation (Dietz). Employers are not permitted to physically restrain an individual through barriers, force, threat of force, or duress (Walsh).

Conclusion

New technologies regarding surveillance, communication, and personal identification are at the forefront of widespread commercialization. RFID chips, genetic information, location

Vol. 2, No. 04; 2018

ISSN: 2456-7760

technologies, social media accounts, and search engine information have the potential to change work environments for better or worse, and the legal system must keep up with such advancements, adhering to the tested traditions of the Fourth Amendment in its search for justice. From addresses and Social Security numbers to medical and salary information, organizations are the gatekeepers of sensitive, private employee information and must adhere to a complicated set of guidelines regarding such information usage and dissemination. The guidelines, stemming from the U.S. Constitution's Fourth Amendment, individual statutes by Congress, specific state statutes, and case law, continue to evolve as additional concerns and situations are addressed with the influx of more infiltrative technology. The workforce, evolving as it may, still requires consistency and evenness in the law. While changing technology may introduce new mediums, the tenants of privacy law will generally remain stagnant and applicable.

Works Cited

29 USCS § 654
45 CFR § 160

AmericanswithDisabilitiesAct. 42 USC §12101 *et seq.*

Bodah v. Lakeville Motor Express, Inc., 663 N.W.2d 550, 2003 Minn. LEXIS 362, 31 Media L. Rep. 1884 (Minn. June 26, 2003)

Citron, Danielle Keats. Mainstreaming Privacy Torts, 98 Cal. L. Rev. 1805 (2010).

Dietz v. Finlay Fine Jewelry Corp. 754 U.S. 958. Court Appeals of Indiana, Third District. 2001. LexisNexis Uni. Web.

EEOC v. Dillard's Inc., 2012 U.S. Dist. LEXIS 16945, 25 Am. Disabilities Cas. (BNA) 1610, 15 Accom. Disabilities Dec. (CCH) P15-032, 2012 WL 440887 (S.D. Cal. February 9, 2012)

EEOC v. Thrivent Fin. For Lutherans. 700 U.S. 1044. United States Court of Appeals for the Seventh Circuit. 2012. LexisNexis Uni. Web.

Ehling v. Monmouth-Ocean Hosp. Serv. Corp. 961 U.S. 659. United States District Court for the District of New Jersey. 2013. LexisNexis Uni. Web.

Electronic Communications PrivacyAct. 18 USC § 2510 *et seq.*
EmployeePolygraph Protection Act. 29 USC § 22 *et seq.*

Gerlich v. United States DOJ. 404 U.S. 256. U.S. Court of Appeals D.C. Circuit. 2013. LexisNexis Uni. Web.

Government Organization and Employees, 5 USCS § 5521 (2004).

Vol. 2, No. 04; 2018

ISSN: 2456-7760

Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191. Stat. 1936. Web.

Hellanbrand v. Nat'l Waste Assocs., LLC. Connecticut Superior Court. 2008. LexisNexi Uni. Web.

"H.R. 1— 103rd Congress: Family and Medical Leave Act of 1993." www.GovTrack.us. 1993. March 22nd, 2018.

K-Mart Corp. Store No. 7441 v. Trotti. 677 U.S. 632. Court of Appeals of Texas, First District, Houston. 1984. LexisNexis Uni. Web.

Koeppel v. Speirs, 2010 Iowa App. LEXIS 25 (Iowa Ct. App. January 22, 2010)

Lemons, B. R. (2004). Public Privacy: Warrentless Workplace Searches of Public Employees. U. Pa. Journal of Labor and Employment Law. Vol. 7:1

McKenna, Bruce A. False Light: Invasion of Privacy, 15 Tulsa L. J. 113 (2013).

National Labor Relations Act. 29 U.S.C. §§ 151-169

Occupational Safety and Health Administration. "Toxic and Hazardous Substances." *U.S. Department of Labor, Occupational Safety and Health Administration.* OSHA, 2012.

Pagnattaro, Marisa. "Getting Under Your Skin – Literally: RFID In the Employment Context." *LexisNexis Uni.* Fall, 2008. Web.

Privacy Act of 1974, 5 U.S.C. § 552a (1974).

Restatement of the Law, Second, Torts, § 652

Smith v. Mike Devers & Mike Devers Ins. Agency, Inc. 2002 U.S. Dist. LEXIS 1125, 2002 WL 75803 (M.D. Ala. Jan. 17, 2002)

Stored Communication Act. 18 USC § 2701-2712

Timken Co. v. NLRB, 29 Fed. Appx. 266, 2002 U.S. App. LEXIS 2059, 171 L.R.R.M. 3215, 82 Empl. Prac. Dec. (CCH) P41,110 (6th Cir. February 04, 2002)

U.S. Const. am. 4.

Vega-Rodriguez v. Puerto Rico Tel. Co. 110 U.S 174. 1997. LexisNexis Uni. Web.

Wal-Mart Stores v. Lee. 348 U.S. 707. Arkansas. 2002. LexisNexis Uni. Web.

Walsh, David J. *Employment Law for Human Resource Practice*. 5th ed., Cengage Learning, 2016.