UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 81 ● Winter 2019

NOTES

YOU'RE ON [POST]DID CAMERA: THIRD PARTIES' EXPANSION OF EMPLOYEES' DIGITAL FOOTPRINT

Elizabeth L. Hitt

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

NOTES

YOU'RE ON [POST]DID CAMERA:[1] THIRD PARTIES' EXPANSION OF EMPLOYEES' DIGITAL FOOTPRINT

Elizabeth L. Hitt[*]

INTRODUCTION

The recognition of new rights arises with changes in the political, social, and economic climate, necessitating common law to grow to meet the demands of society.[2] "That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection."[3] The advent of

[1] "You're on [Post]did Camera" is a play on the catchphrase, "Smile, You're on Candid Camera," from the popular and long-running American television show, *Candid Camera*, in which concealed cameras captured ordinary people being confronted with unexpected situations and their subsequent spontaneous responses. *See About Candid Camera*, CANDID CAMERA ONLINE, https://www.candidcamera.com/cc2/cc2a.php (last visited Oct. 6, 2019).

[*] Candidate for J.D., 2020, University of Pittsburgh School of Law; B.S. in Business, Marketing, 2013, Miami University; M.A. in Fashion Brand Management, Polimoda International Institute of Fashion Design and Marketing, 2014. I am very grateful to my parents who provided invaluable support and feedback throughout the entire note-writing process. I also thank Juliet Astbury and Martin McKown for comments on an earlier draft. Many thanks also to Mallorie McCue for the brainstorming session which led to the selection of this topic.

[2] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[3] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

social media[4] calls for the expansion and clarification of privacy rights as social media increasingly penetrates and becomes engrained in the lives of contemporary America.[5]

Though social networking between humans dates back hundreds of thousands of years, it was the inception of the Internet in the early 1980s and the mainstreaming of the World Wide Web that provided an optimal medium for social networking[6] through social media.[7] As technology and social media evolve, the constructs of social establishment continue to morph. Human beings are social animals[8] and continuously seek to "control others' impressions of them through performances within spatially defined social establishments,"[9] where social establishments are defined as "any place surrounded by fixed barriers to perception in which a particular kind of activity regularly takes place."[10] It is through these performances that humans create and tailor their social identities, targeting particular audiences.[11] For these performances to succeed, each performance audience must be segregated where "an individual must 'ensure that those before whom he plays one of his parts will not be

[4] "The term 'social media' encompasses any online platform that allows individuals to communicate, create content, and interact socially. Social media encompasses the following: blogs, wikis, podcasts, photos and video sharing, virtual worlds, and social networking sites such as Linkedln, Facebook, Instagram, and Twitter." Susan Park & Patricia Sánchez Abril, *Digital Self-Ownership: A Publicity-Rights Framework for Determining Employee Social Media Rights*, 53 AM. BUS. L.J. 537, 538 (2016).

[5] *See, e.g.*, J. Clement, *Percentage of U.S. Population with a Social Media Profile from 2008 to 2018*, STATISTA, https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/ (last updated Aug. 9, 2019) (finding that, in 2018, seventy-seven percent of Americans in the United States had social media profiles).

[6] A social networking service, or simply social media, is an "online vehicle for creating relationships with other people who share an interest, background or real relationship." *Social Networking Service—SNS*, INVESTOPEDIA (Mar. 30, 2018), https://www.investopedia.com/terms/s/social-networking-service-sns.asp. Users of these services create a profile, often including personal information and photos, where individuals form connections with other profiles. *Id.* These connections grow through commenting, sharing, messaging, and/or simply "liking" a network connection's content. *Id.*

[7] *The Advent of Social Media*, LOGICLOOP BLOG (Feb. 6, 2018), https://www.logicloopdigital.com/blog/advent-social-media/.

[8] *Id.*

[9] Patricia Sánchez Abril et al., *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63, 63 (2012).

[10] *Id.* (citing ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 238 (1959).

[11] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

the same individual before whom he plays a different part in another setting.'"[12] To preserve audience segregation, individuals follow each social situation's rules of decorum by censoring the personal information they provided to such audience.[13] When the veil of audience segregation is pierced, social disruption arises.[14] "The disclosure of information to unintended audiences discredits the construction of roles and identities within the group and causes 'difficult problems in impression management.'"[15]

Audience segregation and impression management are further complicated by technological advancements in handheld electronic devices.[16] Specifically, smartphone devices are now equipped with photographic and video capabilities, Internet access, and mobile applications. Access to these features by third parties increasingly threatens an individual's ability to achieve audience segregation. When a third party intrudes on an individual's social establishment by capturing and sharing it with unintended audiences, that individual's intended audience segregation is consequently shattered.

The traditional workplace performance is the language of professionalism,[17] which demands audience segregation between an employee's professional and private lives.[18] The boundaries between the professional and personal have become

[12] *Id.* (citing GOFFMAN, *supra* note 10, at 49).

[13] *Id.* at 63–64.

[14] *Id.* at 64.

[15] *Id.* (citing GOFFMAN, *supra* note 10, at 139). Conversely, one could argue that social media is causing traditional expectations of privacy to fade. Generations that grew up regularly experiencing unintended disclosures of social information now may expect and accept that it occurs. *See* V. John Ella, *Employee Monitoring and Workplace Privacy Law*, A.B.A. NAT'L SYMPOSIUM ON TECH. IN LABOR & EMP. LAW 2 (Apr. 6–8, 2016), https://www.americanbar.org/content/dam/aba/events/labor_law/2016/04/tech/papers/monitoring_ella.authcheckdam.pdf (comparing Millennials to older generations who are more sensitive to privacy intrusions). Although, to that end, difficulties of impression management would still be prevalent where, in order to preserve audience segregation, individuals would be engaging in constant censorship thereby discrediting the roles and identities they play before audiences.

[16] Abril et al., *supra* note 9, at 64.

[17] "[Professionalism] includes conduct and appearance that demonstrate good judgment, a respectable stature, and the maintenance of 'an air of competency and a general grasp of the situation.'" *Id.* (citing GOFFMAN, *supra* note 10, at 47). As social media is ingrained in the culture of new generations, when those individuals become hiring managers, the traditional workplace language of "professionalism" may start to diminish or rather evolve into a modern definition of "professionalism." This progression further warrants the issuance of privacy laws nimble enough to confront the evolution of privacy threats.

[18] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

more porous[19] with advancements in technology blurring the line between the private and the public, as well as the line between the home and the workplace.[20] "Personal blogs, social media profiles, Tweets, and other online fora allow individuals to publicly express multiple facets of themselves, including their private lives and opinions."[21] Segregated private information is now often easily accessible by potentially unintended audiences, such as current and future employers, clients, and recruiters.[22] With digital information's infinite transferability and social media's ubiquity,[23] unintended access to content has enormous effects on personal privacy and self-expression.[24] Employers are becoming increasingly privy to details surrounding their employees' off-duty conduct,[25] where a pre-hire Google search will provide recruiters with personal information about an applicant, human resources may receive a report from a coworker that he or she is offended by something posted on a colleague's social media page, or "an employer may become aware of a 'Tweet' by an employee that is critical of the company or publicizes embarrassing or inappropriate behavior by another employee."[26] The permanent and pervasive nature of the availability of this material presents threats to an employer's interest that did not exist when "communications were limited to in-person interactions and traditional ephemeral media such as television, radio, and newspaper

[19] *Id.*; *see also* Karin Eldor, *Why Every Company Needs a Workplace Social Media Policy*, MONSTER, https://hiring.monster.ca/hr/hr-best-practices/workforce-management/improving-employee-relations/workplace-social-media-policy.aspx (last visited Feb. 23, 2019); June D. Bell, *Firing for Online Behavior*, SHRM (Aug. 24, 2018), https://www.shrm.org/hr-today/news/hr-magazine/0918/pages/firing-for-online-behavior-.aspx (adding that as more workers friend and follow their colleagues, it further obscures the boundaries between individuals' personal and professional lives).

[20] Abril et al., *supra* note 9, at 64.

[21] *Id.*; *see* Park & Abril, *supra* note 4, at 538 ("For individuals, social media can be the digital representation of the self online. Social media profiles are fora for communication, self-expression, identity creation, and relationship-building in front of audiences of few or many.").

[22] Abril et al., *supra* note 9, at 64.

[23] For example, a University of Tampa visiting assistant professor, Kenneth Storey, lost his job days after his Tweet suggested that the victims of Hurricane Harvey in Texas were experiencing instant karma for voting Republican. While Storey deleted the Tweet, it had gone viral prior due to screenshots. Bell, *supra* note 19.

[24] Abril et al., *supra* note 9, at 64.

[25] "Off-duty conduct" is that which an employee engages after completing their assigned shift.

[26] Jeffrey A. Dretler & Richard A. Millisor, *806-Adverse Employment Actions and Off-Duty Conduct*, A.B.A. 1 (2015), https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2017-2018/2018-sac/written-materials/eight-hundred-six-adverse-employment-actions.pdf.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

publications."[27] The proliferation of social media has increased liability and reputational risks for employers, causing potentially significant damage to a firm's brand value, goodwill, and reputation.[28] Accordingly, an employee's off-duty conduct on social media has become a prevalent source of both evidence for allegations of employee misconduct and, further, grounds for discipline and termination.

In nearly every assessment of privacy under American law lies the evaluation of whether a reasonable expectation of privacy exists.[29] "The reasonable expectation of privacy analysis, which is endemic to privacy jurisprudence, is firmly rooted in the experience of physical space and its surrounding normative circumstances."[30] However, it has taken common law and statutory law nearly 100 years to address an employer's infringement of the privacy rights of off-duty employees.[31] Despite privacy rights becoming more defined in recent decades, large discrepancies in the law still exist, creating "many unsettling questions about employers' use of their employees' off-duty conduct in making employment decisions."[32] Where employer liability and effective business operations are at issue, employers are able to undermine an employee's reasonable expectation of privacy[33] through review of an employee's *personal* expression(s) via social media, consequently permeating the privacy threshold of an employee's off-duty conduct.

Typically, the employer reviews an employee's expression as communicated through the employee's own, *personal* social media and may respond as it deems to be appropriate. However, what if an employer instead considers taking an employment action based on a third party's social media expression which clearly depicts one of their employees? Consider these hypothetical scenarios as potential situations that may confront an employer:

---

[27] Jessica A. Magaldi & Jonathan S. Sales, *Exploring the NLRB's Jurisprudence Concerning Work Rules: Guidance on the Limits of Employer Policy to Regulate Employee Activity on Social Media*, 52 U.S.F. L. REV. 229, 230 (2018).

[28] *Id.* at 230–31.

[29] Abril et al., *supra* note 9, at 65.

[30] *Id.* at 64–65; *see* U.S. CONST. amend. IV.

[31] Marisa Anne Pagnattaro, *What Do You Do When You Are Not at Work?: Limiting the Use of Off-Duty Conduct As the Basis for Adverse Employment Decisions*, 6 U. PA. J. LAB. & EMP. L. 625, 626 (2004).

[32] *Id.*

[33] *Id.* at 628; 5 U.S.C. § 7513(a) (2018) (delineating that a government agency may only take action against an employee for such causes that will promote the efficiency of service).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

(1) Charlotte and Amelia attend an event celebrating the LGBTQ community. Charlotte captures numerous photos of them together at the event. Charlotte asks Amelia which photo of them she should post on social media. Charlotte posts the photo approved by Amelia. One of Amelia's co-workers sees Charlotte's post and brings it to the attention of their employer, a deeply conservative religious organization.

(2) Kaitlyn, an elementary school teacher, goes on a weekend trip to Las Vegas with friends. While out with her friends one evening, one of them documents portions of the evening using her smartphone, which includes photos of Kaitlyn posing for the camera while engaged in what might be considered promiscuous behavior. Without Kaitlyn's knowledge, her friend breaks the agreed rule that "what happens in Vegas, stays in Vegas" and posts the photos of Kaitlyn on Facebook. When parents of Kaitlyn's students discover the photos, they bring the photos to the school board's attention.

(3) While at a coffee shop, James is seen on his phone yelling at a customer service operator for his/her "incompetence" while using racial slurs and making discriminatory comments. As James's call proceeds, a bystander captures the racially insensitive comments on video and then posts the video on Instagram because "ignorant people need to be stopped." James's supervisor sees the Instagram post.

(4) Numerous friends and acquaintances gather at Samantha's house, consuming alcoholic beverages. One of her acquaintances video records an interaction between Samantha and her cat. The video depicts Samantha abusing her cat by repeatedly kicking and throwing the animal to the ground. The acquaintance posts the video on Facebook to call attention to animal cruelty and the video was ultimately brought to Samantha's employer's attention.

To what extent should the employer be able to act in each hypothetical? Does it matter if the employee is a willing and active participant in the creation and/or posting of the material? What if the employee is depicted as engaging in an illegal act? Would or should any of these factors change the analysis? With these questions in mind, this Note examines the law of privacy as it pertains to an employee's off-duty conduct and proposes a threshold framework for determining when an employer has the ability to pursue adverse employment action based on a third party's posting of the off-duty conduct of an employee. An employee's participation in the content creation and subsequent expression on social media, regardless of whether it is expressed on their own personal platforms, is foundational to the threshold analysis. The proposed framework considers the following four general categories:

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

(1) The employee is a willing, active participant in the content creation and subsequent posting of that content on social media.

(2) The employee is an active participant in the content creation except that the images were posted without the employee's knowledge or consent.

(3) The content was created and posted without the employee's cooperation, knowledge or consent.

(4) The posting depicts an illegal action by the employee.

Arguably, as one moves further away from actions in which the employee was an active participant in the content creation and posting, the employer's ability to react and, accordingly, its level of redress, decreases. However, when an employee is captured engaging in illegal actions, the level of participation on behalf of the employee would likely be inconsequential as it is evidentiary proof of a criminal act and the employer should be able to pursue adverse employment actions without concern about the privacy rights of the employee.

This Note is organized into three sections. Section I reviews the current landscape of the law as it pertains to employees' privacy interests in social media compared with employers' right to impede on those interests by examining federal legislation. Section II expands the privacy analysis to third-party social media posts of employees, proposing a threshold analysis for when an employer can rightfully take adverse employment action for such third-party posting. Finally, Section III summarizes the patterns discussed in this Note.

I. A DOUBLE-EDGED SWORD: EMPLOYER AND EMPLOYEE INTERESTS

The rise of social media created a new arena in which employees can claim workplace privacy rights. Employees have a right to use social media in their personal lives,[34] although employers are permitted to enact policies to monitor employees' social media,[35] and if necessary, pursue disciplinary actions with regard to employees' social media use. Business leadership typically looks to their core

[34] *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017) (stating that a fundamental principle of the First Amendment is an individual's right to access places where they can share and listen, with one of the most important "places" to exchange ideas being cyberspace, in particularly social media).

[35] Ella, *supra* note 15, at 4 ("Methods of electronic monitoring range from occasional email audits to sophisticated software enabling employers to count keystrokes, record time and activities online, view computer screens in real time, and to record use of company networks.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

company values when determining which off-duty behaviors violate organizational principles.[36] This evaluation process could begin before any conduct occurs or, as is more often the case, when an employer is made aware of a potentially problematic post. Because there is no statute of limitations for information made publicly available on the Internet, the posting date is irrelevant.[37]

An employer should engage in a balancing analysis when investigating and monitoring an employee's off-duty conduct in which the employer weighs its legitimate business interest against an employee's reasonable expectation of privacy.[38] However, difficulty arises when an employer attempts to conduct this analysis as there is no uniform standard in the United States for determining when an employer can rightfully use the off-duty conduct of an employee as the basis for adverse employment decisions.[39] State laws vary widely, and federal statutes do not explicitly protect employees from adverse employment action based on off-duty conduct.[40] Judicial precedent has established some instances in which employers have a legitimate interest in monitoring and investigating the off-duty conduct of employees.[41]

The focal point for an employer's determination of when monitoring or investigation is appropriate is to consider whether and to what extent they have a legitimate business interest to protect.[42] The following are examples of some compelling business reasons for employers to monitor and investigate employee

[36] Bell, *supra* note 19.

[37] *Id.* For example, James Dunn, director of "Guardians of the Galaxy," was fired in July of 2019 for comments that resurfaced involving pedophilia and rape, which he had written on Twitter several years prior. *Id.* Despite regretting his prior actions, it was not enough to save his job. *Id.*

[38] *See infra* 412–13.

[39] Pagnattaro, *supra* note 31, at 683.

[40] *Id.*; *see also* Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy*, 126 HARV. L. REV. 2010, 2036 (2013) ("[T]he lack of prophylactic privacy laws in the United States causes unraveling, public choice, and attitudinal dynamics that make subsequent privacy regulation quite unlikely." [Alternatively,] "[t]he presence of prophylactic European privacy laws such as the Data Protection Directive and the Convention on Human Rights means that new threats to privacy are likely to be stifled before they can take root.").

[41] *See infra* 428–30.

[42] Jason Habinsky et al., *XpertHR Employment Law Manual 2154*, XPERTHR, https://www.xperthr.com/employment-law-manual/employee-privacy-federal/2154/ (last visited Dec. 17, 2019).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

activities, both on and off the employer's property:[43] maintaining a productive and efficient workplace,[44] quality control of employee work,[45] preventing discrimination and harassment lawsuits,[46] protecting relationships with clients and customers,[47] maintaining the security of trade secrets and confidential information,[48] protecting the employer's reputation,[49] and preventing employee theft and misconduct.[50] Nevertheless, employers must weigh these business reasons against the following potential impingements on the employee's rights that may result from monitoring or investigation: expectations of privacy, right to engage in protected concerted activity, right to safeguard personal information, and right to be free from false publicity or defamatory statements. Additionally, the employer should consider its own interests in maintaining employee morale[51] and avoiding high monitoring costs.[52] Overall, when assessing the legality of investigating an employee's conduct, the Court primarily examines whether the employee had a reasonable expectation of privacy.[53] Consequently, it is vital for an employer to effectively manage and balance employee expectations of privacy against its legitimate business interests.[54]

A. Reasonable Expectation of Privacy

The "reasonable expectation of privacy" analysis is derived, historically, from the Fourth Amendment, which operates to shield individuals, along with their homes, papers, and effects, from unreasonable searches and seizures by the government.[55]

---

[43] *Id.*

[44] *Id.*; Ella, *supra* note 15, at 2.

[45] Habinsky et al., *supra* note 42.

[46] *Id.*

[47] *Id.*

[48] *Id.*; Ella, *supra* note 15, at 2.

[49] Habinsky et al., *supra* note 42.

[50] *Id.*; Ella, *supra* note 15, at 2.

[51] Habinsky et al., *supra* note 42; *see also* Ella, *supra* note 15, at 3 ("Opponents of monitoring argue that a loss of trust and respect for employees may lead to higher turnover, loss of productivity and initiative, and the decay of a positive work culture.")

[52] Habinsky et al., *supra* note 42.

[53] *Id.*

[54] *Id.*

[55] U.S. CONST. amend. IV.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

Traditionally, the Fourth Amendment search and seizure doctrine was linked to common law trespass and a determination of whether the information was obtained through physical intrusions by the government.[56] The United States Supreme Court, more recently, has recognized that violations under the Fourth Amendment are not exclusive to property rights.[57] Rather, the Fourth Amendment protection extends to people, not places.[58]

In the context of social platforms, government searches of information shared on social media are limited to reasonable searches supported by probable cause; however, the government can still access vast amounts of social data without triggering the "search" threshold of the Fourth Amendment.[59] The Supreme Court has interpreted a "search" to occur when an expectation of privacy that society recognizes as reasonable is infringed upon.[60] Therefore, "[w]hen it comes to social media data, the extent to which individuals have a reasonable expectation of privacy in their social network publications determines whether courts will consider government searches of social data information 'unreasonable' and therefore protected by the Fourth Amendment."[61] "As Justice Harlan explained in his *Katz* concurrence, there are two elements to assessing the reasonableness of expecting privacy: a subjective and objective component."[62]

The third-party doctrine, however, severely undercuts the protections of the Fourth Amendment by acting as an exception to the "reasonableness" standard.[63] Under the third-party doctrine, when an individual provides a third party with information and voluntarily agrees to share the information, that individual eviscerates any reasonable expectation of privacy in that disclosed information.[64] This doctrine is transferable to social media information as agents can presumably

[56] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (citing United States v. Jones, 565 U.S. 400, 405, 406 n.3 (2012)).

[57] *Id.* (citing Soldal v. Cook County, 506 U.S. 56, 64 (1992)).

[58] Katz v. United States, 389 U.S. 347, 351 (1967).

[59] Brian Mund, *Social Media Searches and the Reasonable Expectation of Privacy*, 19 YALE J.L. & TECH. 238, 240 (2017).

[60] *Id.* at 241.

[61] *Id.* at 242.

[62] *Id.* at 241 (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

[63] *Id.* at 243.

[64] *Id.* (citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

access posted social media content without first meeting the probable cause requirement.[65] Consider "wall-to-wall" type conversations between users, here "the rest of the users' social network functions as third parties to whom the content publisher and recipient have voluntarily disclosed information. If the third-party doctrine governs social media behavior, then published content voluntarily shared among connections within a private social network loses all reasonable expectation of privacy. . . ."[66] Sharing information on the Internet in today's world is equivalent to sharing information in the center of a public street which society is ill-equipped to reasonably protect.[67] Accordingly, this public information cannot be expected to be protected as the publisher deliberately left this data in "plain view of all [I]nternet users."[68] The government did not need to partake in a "search" to discover it.[69]

While a discussion of privacy rights under the Fourth Amendment is not directly applicable to the employer-employee context, prior court decisions that affirm protections provided by the Bill of Rights are likely to be useful in predicting the outcome of decisions by courts and other administrative reviews of claims that arise. As noted above, the concept of a "reasonable expectation of privacy" in American law is largely based on Fourth Amendment jurisprudence. It seems inevitable that Fourth Amendment interpretations and precedent will be considered in developing a working framework for dealing with issues related to the usage of social media in the employer-employee relationship.

B. Employment Classification

One factor impacting this "reasonableness" analysis is the contractual relationship between the employer and employee. The at-will employment doctrine is common in the private sector, however the same cannot be said about the public sector.[70] "Many public employees are afforded additional protections in the areas of

---

[65] *Id.* at 244.

[66] *Id.*

[67] *Id.* at 248 (citing People v. Harris, 949 N.Y.S.2d 590, 594 (N.Y. Crim. Ct. 2012)).

[68] *Id.* (citing California v. Greenwood, 486 U.S. 35, 41 (1988)).

[69] *Id.*

[70] Allison B. Williams, *How Discipline and Discharge of Public Sector Employees Differs from That of Private Sector Employees*, LEXISNEXIS (Aug. 17, 2015), https://www.lexisnexis.com/legalnewsroom/labor-employment/b/labor-employment-top-blogs/posts/how-discipline-and-discharge-of-public-sector-employees-differs-from-that-of-private-sector-employees.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

discipline and discharge that private sector employees simply are not afforded[71] absent a collective bargaining agreement, an employee-friendly handbook, or other contract."[72] Hired by government agencies on a permanent basis, public-sector employees are automatically granted additional rights provided by federal and state statutes applicable to government employees.[73] Although, determining "whether public employees are at-will employees or have this protected status depends upon how they are classified and under which statutory scheme they are employed."[74] Nonetheless, for at-will employees, whether public or private, the analysis is simpler as the employment relationship, by its nature, allows for an employer to dismiss an employee for any reason and without warning, provided that the reason for dismissal is not illegal.[75] Whereas, in the context of the dismissal of an employee whose relationship is contractually governed, an employee's conduct "[may] not serve as grounds for discipline or dismissal in the absence of a showing of some nexus between the conduct and the performance of the employee's duties or responsibilities," often referred to as the Adverse Effect Doctrine.[76] The nexus requirement's primary purpose is that of establishing that an employee is unfit to continue in a position, making it vital to fully and completely state the grounds for discipline or dismissal in the notice of employee charges provided to the employee.[77]

C. Limitations on an Employer's Right to Monitor

Generally speaking, when an employer has clearly informed an employee that the employee's activities may and will be monitored, employees do not have a reasonable expectation of privacy.[78] It is permissible for employers to require

---

[71] The private sector is free from direct government regulation where "[s]tatutory exclusions explicitly omit individuals from the definition of 'employee' who are employed as: 'agricultural laborers, domestic workers of any family or person at his home, individuals employed by a parent or spouse, independent contractors, supervisors, and individuals employed by an employer subject to the Railway Labor Act.'" Christina Jaremus, *#Fired for Facebook: The Case for Greater Management Discretion in Discipline or Discharge for Social Media Activity*, 42 RUTGERS L. REC. 1, 7 (2014). The determination of whether an individual is an "employee," "supervisor," or "independent contractor" is outside the scope of this Note.

[72] Williams, *supra* note 70.

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] 2 JAMES A. RAPP, EDUCATION LAW § 6G.01 (Release No. 69, 2019).

[77] *Id.*

[78] Habinsky et al., *supra* note 42.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

employees, as a condition of employment, to subject themselves to monitoring of daily online activities in the workplace.[79] If an employer chooses to monitor at least some portion of its employees' activities, an employer must comply with various federal and state laws.[80] While there are no federal statutes that explicitly prohibit an employer from disciplining employees' off-duty behavior, some federal statutes do protect aspects of an employee's personal life from undue scrutiny by the employer.[81] These statutes also require employers to notify employees of certain types of monitoring.[82] In the context of limiting the investigation of off-duty conduct in connection with adverse employment decisions, seven statutes are of particular interest: Title VII of the Civil Rights Act of 1964; the Privacy Act of 1974; the Electronic Communications Privacy Act of 1986; the Employee Polygraph Protection Act of 1988; the Patriot Act of 2001; the Defend Trade Secrets Act of 2016; and the National Labor Relations Act of 1935.[83] While none of these statutes specifically address the issue of a third-party posting or publication of an employee's conduct, they do set forth the current state of legislation with respect to an employer's ability to monitor and take employment related actions based on the employee's social media activities. Accordingly, this Note sets forth a brief description of each of these statutes below.

It should be noted that the majority of states have statutory notice requirements that are similar to, or more stringent than, the federal standards, discussed below; however, the applicable reasonableness standard varies by state.[84]

1. Title VII of the Civil Rights Act of 1964

The Civil Rights Act of 1964 ("CRA") restricts employers from discrimination related to off-duty conduct of employees and applicants.[85] Specifically, the CRA provides that "[i]t shall be an unlawful employment practice for an employer . . . to discriminate against an individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color,

[79] *Id.*

[80] *Id.*

[81] Pagnattaro, *supra* note 31, at 670.

[82] Habinsky et al., *supra* note 42.

[83] *See infra* 424–28.

[84] Habinsky et al., *supra* note 42.

[85] Pagnattaro, *supra* note 31, at 675.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

religion, sex or national origin."[86] Broadly speaking, the inquiry under anti-discrimination statutes is whether an employer's decision to terminate or discipline an employee was motivated, in part, by an unlawful purpose.[87] The employer would have the opportunity to demonstrate that there was a legitimate nondiscriminatory reason for the employee's discipline or termination.[88] Once this showing is established, the employee is given the opportunity to show that the proffered reason(s) were "pretext" for unlawful discrimination.[89] A common demonstration of "pretext" is establishing that the plaintiff was subjected to more severe discipline than a similarly situated employee outside their class for a comparable infraction.[90] This analysis is heavily fact-dependent. For example, in the realm of discrimination and social media "[a]n employee might claim that he or she is the victim of race discrimination at work based on some race-related off-duty activity."[91] Title VII further protects off-duty conduct in the area of interracial associations.[92] An employer can be subjected to an action by an employee for: "discrimination against a white woman because of her relationship with a black man; firing a white man because of his marriage to a black woman; and firing a white worker because of her non-marital relationship with a minority co-worker."[93]

[86] Civil Rights Act of 1964, 42 U.S.C. § 2000e–2(a)(1) (2018).

[87] *Id.* § 2000e-2(m).

[88] McDonnell Douglas Corp. v. Green, 411 U.S. 792, 802 (1973) (explaining that once an employee proves a prima facie case of discrimination, "[t]he burden then must shift to the employer to articulate some legitimate, nondiscriminatory reason for the employee's rejection").

[89] *Id.* at 804.

[90] U.S. DEP'T. OF JUSTICE, TITLE VI LEGAL MANUAL, SECTION VI: PROVING DISCRIMINATION—INTENTIONAL DISCRIMINATION 20, https://www.justice.gov/crt/case-document/file/934826/download (providing an illustration in which a discrimination inquiry must focus on whether there was a nondiscriminatory reason for the difference in treatment between two similarly situated students).

[91] Pagnattaro, *supra* note 31, at 675.

[92] *Id.*

[93] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

2. Privacy Act of 1974

Under the Privacy Act of 1974, public sector employers are required to protect certain employee information[94] created through four procedural and substantive rights in personal data.[95] Examples include:

- Public sector employers are required to have security systems in place to prevent the unauthorized release of personal records.[96]
- Public sector employers are permitted to obtain only employee information which is relevant and necessary to their agency's specific purpose.[97]
- Public sector employers are prohibited from disclosing any employee records without the written consent of employees, subject to some exceptions.[98]

Overall, the Privacy Act creates four safeguards in personal data.[99] First, government agencies are required to show individuals any records kept about them.[100] Second, when gathering and handling data, agencies must follow certain principles called "fair information practices."[101] Third, there are restrictions placed on how agencies can share an individual's data with other people and agencies.[102] Fourth and finally, individuals are permitted to sue the government for violations of their protected rights.[103]

---

[94] Habinsky et al., *supra* note 42.

[95] The Privacy Act of 1974, 5 U.S.C. § 552a (2018).

[96] Habinsky et al., *supra* note 42.

[97] *Id.*

[98] *Id.*

[99] 5 U.S.C. § 552a.

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

3. Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 ("ECPA")[104] amended the federal Wiretap Act of 1968,[105] which addressed interception of conversations using "hard" telephone lines, but it did not apply to the interception of conversation through computer and other digital and electronic communications.[106] As amended, the ECPA prohibits public and private employers from intercepting communications while those communications are being made, are in transit, or when they are stored by a service provider; whether they take the form of a wire, oral, or electronic communication.[107] The ECPA, however, provides the following exceptions allowing an employer to monitor the emails and phone calls of employees without violating the law:[108]

- Provider Exception: This allows for communication service providers to monitor communications on its services.[109]
- Consent Exception: When a sender has expressly or implicitly consented to interception, an individual may intercept the electronic communication.[110] An employer must announce its policy concerning monitoring employee's electronic communication in advance of implementing the policy in order to take advantage of this exception.[111] Because these types of policies may be insufficient to show implied consent without a written acknowledgment by the employee, it is best

[104] "The Electronic Communications Privacy Act and the Store Wired Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986." *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–2523*, U.S. DEP'T OF JUSTICE, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (last updated Apr. 23, 2019) [hereinafter *Electronic Communications Privacy Act of 1986 (ECPA)*]; *see* Habinsky et al., *supra* note 42.

[105] *See* 18 U.S.C. § 2510 (2018).

[106] *Electronic Communications Privacy Act of 1986 (ECPA)*, *supra* note 104; *see also* Habinsky et al., *supra* note 42.

[107] *Id.*

[108] Habinsky et al., *supra* note 42; *see also Electronic Communications Privacy Act of 1986 (ECPA)*, *supra* note 104.

[109] Habinsky et al., *supra* note 42.

[110] *See id.*

[111] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

practice for employers to have employees acknowledge the policies in writing.[112]

- Business Use Exception: Permits an employer in the ordinary course of its business to use any "telephone or telegraph instrument, equipment or facility" provided by its wire or electronic communication service to monitor the electronic communications of its employees.[113] As this exception is narrow, employers should be wary of relying upon it, particularly in connection with phone calls.[114] Upon the realization that an employee is making a personal call, the employer must immediately stop monitoring the call.[115]

Federal law does not preempt more stringent state regulation.[116] For example, many states require that the employers notify employees that their business-related calls will be monitored, even though the ECPA does not require this.[117]

4. Employee Polygraph Protection Act of 1988

Generally, the Employee Polygraph Protection Act of 1988 ("EPPA") prohibits an employer engaged in interstate commerce from the use of lie detector tests whether in pre-employment screening or during the course of employment.[118] The EPPA, however, provides for the following limited exceptions:

- In the occurrence of a workplace incident that resulted in an identifiable, ongoing economic loss to the employer, employees who are reasonably suspected of involvement can be subjected to a lie detector test.[119]

---

[112] *Cf. id.*

[113] 18 U.S.C. § 2510(5)(a) (2018); Habinsky et al., *supra* note 42.

[114] Habinsky et al., *supra* note 42.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] U.S. DEP'T OF LABOR, WAGE & HOUR DIV., FACT SHEET #36: EMPLOYEE POLYGRAPH PROTECTION ACT OF 1988 (July 2008), https://www.dol.gov/whd/regs/compliance/whdfs36.pdf; Habinsky et al., *supra* note 42.

[119] U.S. DEP'T OF LABOR, *supra* note 118; Habinsky et al., *supra* note 42; Pagnattaro, *supra* note 31, at 676.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

- Prospective job applicants at security guard firms, or pharmaceutical and other firms authorized to manufacture, distribute, or dispense controlled substances may also be subjected to lie detector tests.[120]

Unless one of the exceptions applies, private employers are prohibited from requiring employees to take a polygraph test, and are prevented from discharging, imposing discipline, or discriminating against employees or applicants who refuse to take such a test.[121]

5. Patriot Act of 2001

The Patriot Act of 2001 was intended to target and prevent terrorism.[122] Enforcement of the Patriot Act presents unique challenges for employers[123] where employers may not be aware of government surveillance of their employees, or may not have a choice but to allow their employees' private communications to be accessed by the government.[124] Title II of the Patriot Act enhances the federal government's ability to conduct workplace surveillance while simultaneously limiting an employer's ability to monitor the workplace.[125] Title II "coordinates intelligence gathering and the collection of evidence for criminal proceedings, and expands the government's ability to utilize wiretaps and computer surveillance."[126] Consequently, federal law enforcement agencies may require employers to provide access to electronic systems or personal records to assist with investigations.[127] An employer's receipt of and compliance with federal law enforcement orders for

[120] U.S. DEP'T OF LABOR, *supra* note 118; Habinsky et al., *supra* note 42.

[121] Habinsky et al., *supra* note 42.

[122] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S. Code).

[123] Vance O. Knapp, *United States: The Impact of the Patriot Act on Employers*, MONDAQ (Oct. 15, 2003), http://www.mondaq.com/unitedstates/x/22891/The+Impact+Of+The+Patriot+Act+On+Employers.

[124] Clare M. Sproule, *The Effect of the USA Patriot Act on Workplace Privacy*, http://files.ali-aba.org/thumbs/datastorage/lacidoirep/articles/pl_sprouletpl0302_thumb.pdf (last visited Feb. 26, 2019).

[125] Knapp, *supra* note 123.

[126] *Id.*

[127] Habinsky et al., *supra* note 42.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

information must not be disclosed.[128] Often this requirement is in direct conflict with employment policies which typically state that "employers will respond only to an outside party's request for verification of employment information."[129]

With only cursory judicial authorization, the federal government may tap phones, monitor Internet use, or seize voicemails and emails where the subject of the action may not be notified.[130] With the permission of the owner or operator, the government is also able to intercept computer use without written authorization provided it is relevant to an ongoing investigation.[131] The actual user must authorize this interception of computer use, unless the user is a "computer trespasser," meaning "anyone who accesses a computer without authorization (e.g., any employee who uses a company computer to transmit a personal message without employer permission or uses company voicemail to receive personal messages) and therefore has no reasonable expectation of privacy."[132] This interception could reasonably extend to the individual responding to the personal message.[133]

6. Defend Trade Secrets Act of 2016

The Defend Trade Secrets Act of 2016 ("DTSA") allows employers to protect and remedy misappropriations of trade secrets by employees.[134] "While it is critical

---

[128] *The U.S. Patriot Act and Its Implications for Employers*, COMPENSATION.BLR.COM (Feb. 6, 2003), https://compensation.blr.com/whitepapers/HR-Administration/Employee-Records/The-U.S.-Patriot-Act-and-Its-Implications-for-Empl/#.

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Id.*

[134] Bret Cohen et al., *Recourse for Trade Secret Misappropriations Under the Federal Defend Trade Secrets Act*, LEXISNEXIS (Apr. 18, 2018), https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2018/04/18/recourse-for-trade-secret-misappropriation-under-the-federal-defend-trade-secrets-act.aspx.

> Before the enactment of the DTSA, in the absence of diversity jurisdiction, employers seeking redress had no choice but to sue in state court. While most states have adopted and codified some version of the Uniform Trade Secrets Act (UTSA), which provides uniform definitions and remedies for trade secret misappropriation, these laws nevertheless tend to differ from state to state both in the text of the laws themselves and in their application.

Id.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

for employees to protect an employer's confidential and proprietary information and trade secrets, under the [DTSA], an employee will be immune for the disclosure of a trade secret when reporting a suspected violation of law and/or in an anti-retaliation lawsuit."[135] For an employer to be entitled to protect information as a trade secret under the DTSA, the employer has to have "taken reasonable measures to keep such information secret" and the information must derive "independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."[136] Additionally, the DTSA requires employers to give notice to their employees, independent contractors, and consultants in any contracts or agreements that govern the use of trade secrets or confidential information.[137] Without notice, the remedies available to employers are far more limited.[138]

7. National Labor Relations Act of 1935

While the other federal statutes discussed above address primarily permitted monitoring and investigation activity by an employer, the National Labor Relations Act of 1935 ("NLRA") deals far more comprehensively with the relationship between an employer and an employee. The National Labor Relations Board ("NLRB" or "Board") considers the countervailing interests of employers and employees under the NLRA.[139] The NLRA specifically tasks the NLRB with balancing "'the undisputed right of self-organization assured to employees' against 'the equally undisputed right of employers to maintain discipline,'" while ensuring efficient operations in their establishments.[140] In maintaining this balance, the NLRB is to determine whether an employee's social media post(s) constitute "protected

[135] Habinsky et al., *supra* note 42.

[136] 18 U.S.C. § 1839(2) (2018).

[137] *Federal Defend Trade Secrets Act Imposes New Notice Obligations on Employers*, JONES DAY (May 2016), https://www.jonesday.com/Federal-Defend-Trade-Secrets-Act-Imposes-New-Notice-Obligations-on-Employers-05-13-2016/#.

[138] *Id.*

[139] Magaldi et al., *supra* note 27, at 230.

[140] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

concerted activity," such that an employee cannot be terminated or otherwise disciplined by an employer for such posting.[141]

Under Section 7 of the NLRA, the NLRB has held that most private sector employees'[142] rights include the right to use "social media to communicate with each other and the public" for the purpose of improving their terms and conditions of employment, regardless of whether a union is present.[143] A critical distinction is that an employee merely complaining about some aspect of work is not considered to be necessarily engaging in a "concentrated activity,"[144] rather the employee must have some purpose that is related to a group action, "or seek to initiate, induce, or prepare for group action, or bring a group complaint to the attention of management."[145] Therefore, the key questions are: "(1) whether the post(s) involved workplace concerns . . . and (2) whether the postings involved concerted activity as opposed to mere individual grip[ing], a distinction that is not always clear."[146]

Employee activity that is made with knowledge of falsity or with reckless disregard for the truth,[147] or that publicly disparages the employer's products or services without relation to labor or controversy complaints are not protected under the NLRA.[148] It is important to note that an employer may violate the NLRA, even if an employer is conducting general monitoring of employee activities in accordance with other laws.[149]

---

[141] CARRIE E. COPE ET AL., CYBER RISKS, SOCIAL MEDIA AND INSURANCE: A GUIDE TO RISK ASSESSMENT AND MANAGEMENT § 3.04 (Aug. 2018–Aug. 2019 ed.).

[142] Despite the limited scope of the NLRA to private employees, many states have enacted statutes protecting public employees' right to organize, with almost verbatim language to Section 7 of the NLRA. Jaremus, *supra* note 71, at 8. In states with these similar statutes, unfair labor practice violations are to undergo the same analysis for constraining social media activity. *Id.*

[143] COPE ET AL., *supra* note 141 (citing Three D, LLC, 361 N.L.R.B., at *1 (2014)).

[144] *Social Media*, NLRB, https://www.nlrb.gov/rights-we-protect/whats-law/employees/i-am-represented-union/social-media (last visited Mar. 4, 2019).

[145] *Id.*

[146] Kerry W. Langan & Katherine Ritts Schafer, *2011–2012 Survey of New York Law: Labor & Employment Law*, 63 SYRACUSE L. REV. 829, 847 (2013).

[147] COPE ET AL., *supra* note 141 (citing 361 N.L.R.B. 31, at *5 (2014)).

[148] NLRB, *supra* note 144.

[149] Habinsky et al., *supra* note 42.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

Under the following circumstances, employees were found to have engaged in protected concerted activity on social networking sites:

- Employees of a clothing store posted complaints on their Facebook pages about their supervisor's conduct and her refusal to address their concerns regarding working late at night in a dangerous neighborhood. The NLRB noted that the employees would have still been protected even if they had not complained to their superiors prior to posting the comments.[150]
- A bus tour company employee attempted to organize a union through posting messages on Facebook to third parties raising concerns about employment conditions. Although the employee's statements were harsh, they were found not libelous as virtually all of the statements were true.[151]
- Employees of a sports bar complained on Facebook about their employer's failure to correctly deduct taxes from their paychecks, which resulted in two employees' unlawful termination—one for clicking "like" on the initial status posted by a former employee and another for using profanity to describe the employer, which did not amount to the "knowledge of falsity, or with reckless disregard for the truth" standard.[152]

In other circumstances, however, the NLRB found the employees' conduct to fall outside of the protected "concerted activity" shield, generally in factual scenarios involving social media postings constituting personal complaints or abusive rants:

- An employee communicated in a private Facebook chat to another employee about an exchange with a supervisor complaining that the supervisor should "'back the freak off;' that the employer was 'full of shit;' and that the employer should 'FIRE ME . . . Make my day.'" These messages only amounted to an "individual gripe" showing personal contempt for a supervisor with no sharing of concerns over terms or conditions of employment.[153]

[150] COPE ET AL., *supra* note 141 (citing 359 N.L.R.B. 96 (2013), *aff'd*, 361 N.L.R.B. 79 (2014)).

[151] *Id.*

[152] *Id.* (citing 361 N.L.R.B. 31 (2014)).

[153] Advice Memorandum from Barry J. Kearney, Assoc. Gen. Counsel, N.L.R.B. Div. of Advice to Dennis Walsh, Reg'l Dir., Region 4 (May 8, 2013), https://www.theemployerhandbook.com/ files/2015/01/04_ CA_094222_05_08_13_.pdf.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

- A bartender complained about his employer's tipping policy on Facebook and months later had another conversation labeling customers as "rednecks" and stating, "I hope they choke on glass," but he did not discuss his posting with co-workers.[154]
- A factory worker left work, drove across the street, and accessed his Facebook account from his phone where he posted a comment suggesting that he was "a hair away from setting it off,"[155] in reference to blowing up the employer's premises.

However, an employee's use of egregiously offensive[156] or abusive language alone does not necessarily preclude a finding that the terminated employee had engaged in "protected concerted activity."[157] For example, in *Pier Sixty, LLC*, a catering company employee was found to have engaged in "protected concerted activity" in the context of a Facebook post stating: "Bob [the employee's supervisor] is such a NASTY MOTHER F***** don't know how to talk to people!!!! F*** his mother and his entire f****** family!!!! What a LOSERZ!!!! VOTE YES for the UNION!!!!!!"[158] The NLRB, in evaluating the employee's post, applied a "totality of the circumstances approach"[159] finding: (1) the employer demonstrated anti-union hostility; (2) the employee's supervisor provoked his comments followed by the employee's protest of disrespectful treatment by managers; (3) the post was made after working hours; (4) similar profanity was common at the employer's business;

[154] Memorandum OM 11–74 from Ann Purcell, Assoc. Gen. Counsel, N.L.R.B. Div. of Operations-Mgmt. to All Reg'l Dirs., Officers in Charge, and Resident Officers (Aug. 18, 2011) (Report of the Acting General Counsel Concerning Social Media Cases); *see also* Habinsky et al., *supra* note 42.

[155] Memorandum OM 12–31 from Ann Purcell, Assoc. Gen. Counsel, N.L.R.B. Div. of Operations-Mgmt. to All Reg'l Dirs., Officers in Charge, and Resident Officers (Jan. 24, 2012) (Report of the Acting General Counsel Concerning Social Media Cases) [hereinafter *Memorandum OM 12-31*].

[156] NLRB, *supra* note 144.

[157] COPE ET AL., *supra* note 141.

[158] *Id.* (citing Pier Sixty, LLC, 362 N.L.R.B. 505 (2015), *enforced*, 855 F.3d 115 (2d Cir. 2017)).

[159] *Id.* (examining the following factors: "(1) [w]hether the record contained any evidence of the Respondent's antiunion hostility; (2) [w]hether the Respondent provoked [the employee's] conduct; (3) [w]hether [the employee's] conduct was impulsive or deliberate; (4) [t]he location of [the employee's] Facebook post; (5) [t]he subject matter of the post; (6) [t]he nature of the post; (7) [w]hether the Respondent considered language similar to that used by [the employee] to be offensive; (8) [w]hether the employer maintained a specific rule prohibiting the language at issue; and (9) [w]hether the discipline imposed upon [the employee] was typical of that imposed for similar violations or disproportionate to his offense").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

and (5) an incidence of similar conduct by another employee was met with a write-up of the employee's conduct, not termination.[160]

To distinguish from the NLRB's prior decisions, in which personal complaints were found to be unprotected, the Facebook posting in *Pier Sixty, LLC* was "made in the context of an ongoing union election and after multiple unfair labor practices had been committed by the employer."[161] Further, while the post included vulgar language, it was not construed as threatening violence.[162] Finally, while similar vulgar language is ordinarily grounds for termination in most businesses, the Board justified the use of such language based on the common use of similar language within the employer's business, emphasizing the employee's punishment was more severe than those who were engaged in similar conduct.[163]

Even if an employee's statements implicate Section 7 rights, such otherwise protected conduct will not be granted protection if it is so "opprobrious" as to forfeit the employee's NLRA protections.[164] In determining whether conduct merits the loss of an employee's Section 7 rights, the NLRB applies a four-part test: "(1) the place of the discussion; (2) the subject matter of the discussion; (3) the nature of the employee's outburst, and (4) whether the outburst was provoked by an employer's unfair labor practice."[165] This four-part test was applied in *Detroit Medical Center*, when due to his co-worker's complaints, an employee at a facility where a majority of the employees were African Americans made a Facebook post complaining about "jealous ass ghetto people that I work with," and asserted that his union had protected "generations of badlazy piece of sh*t workers."[166] The NLRB concluded that the following reasons weighed against protection under the NLRA and recommended a dismissal of the employee because: (1) the place of discussion, Facebook, resulted in wide circulation and weighed against protection because the post caused a major workplace disruption; (2) the employee's use of racial slurs and stereotyping

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] *Id.*

[164] *Id.* (citing Advice Memorandum from Barry Kearney, Assoc. Gen. Counsel, N.L.R.B. Div. of Advice to Ray Kassab, Acting Reg'l Dir. (Jan. 10, 2012), https://www.nlrb.gov/case/07-CA-006682).

[165] *Id.* (citing Advice Memorandum from Barry Kearney, Assoc. Gen. Counsel, N.L.R.B. Div. of Advice, to Ray Kassab, Acting Reg'l Dir., at *4 (Jan. 10, 2012), https://www.nlrb.gov/case/07-CA-006682).

[166] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

significantly harmed the workplace by increasing racial tensions; and (3) the employee was not provoked by an unfair labor practice.[167]

D. Employer's Valid Interests

Employers are faced with a potential minefield of liability resulting from delving into an employee's personal life. In order to protect themselves against unlawful conduct by an employee, employers have a valid interest in monitoring and investigating their employees' conduct.[168] Moreover, employers may be legitimately concerned about an employee's off-duty conduct to the extent that it adversely affects the company or the business environment.[169] Commonly, when an employer has potential liability for an employee's off-duty conduct, employer intervention is permissible.[170] Specifically, there are three contexts of potential liability where an employer's interest may outweigh an employee's right to privacy: negligent hiring or retention, discrimination, and sexual harassment.[171] In these instances, it is reasonable that an employer would want to fully investigate the conduct of an employee and, if appropriate, take adverse action against that employee for the employee's conduct.[172]

A fundamental claim that can be asserted by an employee against an employer is for negligent hiring and retention arising in a variety of contexts.[173] For example, there was a shooting at a Mississippi plant causing six fatalities where a plant employee, Doug Williams, allegedly made racist threats against other employees in the workplace prior to the incident and wore a bootee on his head resembling a Ku Klux Klan hood.[174] Concerns regarding Williams's behavior were expressed by one of the victims stating "they keep letting him come back in, but he's going to kill

---

[167] *Id.*

[168] Habinsky et al., *supra* note 42.

[169] Pagnattaro, *supra* note 31, at 627.

[170] *Id.*

[171] *Id.* at 629; *see also* Habinsky et al., *supra* note 42 (listing the following unlawful conduct as additional potential concerns for employers: disclosure of confidential and proprietary employer information and trade secrets, cyberbullying, pornographic, vulgar and offensive postings, defamation, computer crimes and introduction of harmful viruses, intellectual property rights, and potential lawsuits from third parties).

[172] Pagnattaro, *supra* note 31, at 627.

[173] *Id.* at 677.

[174] *Id.* (citing *A Nightmare on the Job*, NEWSWEEK (July 21, 2003), https://www.newsweek.com/nightmare-job-139315).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

us."[175] Most states permit an employer to be sued on the basis of negligent hiring and negligent retention claims.[176] Had the plant investigated Williams's behavior, both in the workplace and off-duty, the attack may have been averted.[177] However, performing such an investigation requires a balancing act as an employer could potentially face an invasion of privacy lawsuit brought by the employee whose behavior is in question.[178]

Another potential source of employer liability for employee off-duty conduct is where off-duty comments by a supervisor may become admissible in discrimination cases.[179] In *Cooley v. Carmike Cinemas, Inc.*, the court affirmed a verdict in favor of the employee based on two off-duty statements made by Michael Patrick, the President, CEO, and principal shareholder of Carmike, when an employee sued Carmike for age discrimination.[180] Patrick expressed displeasure about spending Thanksgiving with his parents and grandmother because he did not "like to be around old people."[181] Patrick's second statement was made when he was eighteen years old, and after seeing a movie allegedly said, "everybody over 30 years old needs to be put in a pen. Yeah, if they don't want to be put in a pen . . . they should be confined to a concentration camp."[182]

The last potential context for employer liability from employee off-duty conduct involves Title VII with regard to claims of sexual harassment. Often, to avoid behavior that could potentially lead to sexual harassment claims, companies will implement non-fraternization policies.[183] Such policies are typically upheld as reasonable by courts and not in violation of public policy.[184] Provided that there is a "legally sufficient nexus between the employment relationship and the act of harassment," work-related sexual harassment that occurs off-site may be

[175] *Id.*

[176] *Id.* at 677–78.

[177] *Id.* at 678.

[178] *Id.*

[179] *Id.*

[180] *Id.* (citing Cooley v. Carmike Cinemas, Inc., 25 F.3d 1325, 1327, 1329 (6th Cir. 1994)).

[181] *Id.*

[182] *Id.*

[183] *Id.* at 679.

[184] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

actionable.[185] The key factor in determining the employer's liability is whether evidence produced during discovery can reveal the transpiring acts.[186] For example, one court required a videotape to be produced depicting a party attended by employees, strippers, and prostitutes to support the employee's claim.[187] Similarly, evidence of an employer's knowledge of an employee's sexual misconduct outside the workplace can potentially be used as evidence against the employer in sexual harassment cases.[188]

These contexts exemplify situations where it may be reasonable for an employer to investigate the off-duty conduct of employees in an attempt to avert claims and preserve a safe work environment.

II. A WATCHFUL EYE: THIRD-PARTY DEPICTIONS OF EMPLOYEES

Having established the current legal principles applicable to the social media environment in the context of the employer-employee relationship, this Note turns to addressing the gap in coverage under the current authorities in relation to the challenges presented by third-party social media postings. While the law currently addresses, to some degree, an employee's social media activities with respect to an employer's ability to monitor and take employment related actions, it fails to address the issue of third-party posting or publication of an employee's conduct. The key link between the applicable statutes is the theme of "privacy" and to what extent an employee should have a reasonable expectation of it, offering various levels of protection to employees.

When using social media content as grounds for adverse employment action, an employer is normally relying on an employee's own postings. There is a logical inference here that the employee themselves actively participated in the content creation and its subsequent posting, adding validity and assurance to the employer's reliance. However, not all content on an individual's page is always proffered by that individual. Most social networks are equipped with features allowing users to comment, share, and "like" another's content, further intermingling user-generated and third-party generated information. This blurring of the content source has the potential to impact the ability and extent of an employer's reliance on an employee's social network page. When a third party posts on another's page, that posting does

[185] *Id.*

[186] *Id.*

[187] *Id.* (citing Warnell v. Ford Motor Co., 183 F.R.D. 624, 627 (N.D. Ill. 1998)).

[188] *Id.* at 680.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

not necessarily constitute an endorsement by the employee of that particular third party's activities or political, economic, social, or moral views. Conversely, when a third party posts a video or photo of another individual (i.e. an employee), one could reasonably assume the individuals clearly depicted endorse the content portrayed as they chose to engage in that particular behavior.

The ascendency and proliferation of handheld devices allows individuals to capture videos and photos within seconds, which could have paramount consequences in the employment context. The ability to "capture a moment" by posting a picture or a video is available not just to the person who is depicted but also to third parties, without regard to whether the subject was aware of, much less consented to, the photo or video representation. Indeed, sometimes, the person at issue is not the focus of the picture or video, but merely is caught in the background of the posted material. This type of content could then be posted on that third party's social network(s) and brought to the attention of a vast number of people, including an employer. An employer would legitimately be interested in such content if it adversely affects the employer's business,[189] but as the current law stands, employers have no clear standard setting forth their rights of action based on reliance upon a third-party posting.

In an attempt to bridge the gap, this Note proposes a threshold framework for determining when an employer has the ability to pursue adverse employment action based on a third party's posting of the conduct of an employee. The proposed framework encompasses the following four general categories:

(1) The employee is a willing, active participant in the content creation and subsequent posting of that content on social media.

(2) The employee is an active participant in the content creation but the images were posted without the employee's knowledge or consent.

(3) The content was created and posted without the employee's cooperation, knowledge, or consent.

(4) The posting depicts an illegal action by the employee.

Foundational to the threshold analysis is the degree of an employee's participation in the content creation and any resulting expressions on social media. An employer's ability to react and their level of redress should decrease as an employee's active participation in the content creation and posting decreases. Conversely, the level of employee participation is inconsequential where the employee is captured engaging

[189] *See* Pangattaro, *supra* note 31, at 627.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

in illegal actions as it establishes evidentiary proof of a criminal act, which should permit an employer to pursue adverse employment actions without concern about the privacy rights of the employee.

A. Voluntary Participation and Posting Consent

Where the employee is a willing, active participant in the content creation and consents to the third-party posting, the right to pursue adverse employment action by an employer would be subjected to the same analysis as now applies when the employee posts the content on their personal social networks.[190] Similar to the consent exception in the ECPA[191] or third-party doctrine,[192] once an employee has consented, either expressly or implicitly, to the publication of content, an employee would be deemed to have waived their "reasonable expectation of privacy" rights. An appropriate exception should be considered for content created during an individual's teenage or adolescent years. A case could arise where an individual was a willing, active participant in creating the offensive content as an immature youth. Years later, that content could be released and tarnish the reputation of a now older and wiser individual. Consequently, it is suggested that the employer should give deferential weight to when the content was created and the time lapse before the subsequent posting on social media.

B. Voluntary Participation Without Posting Consent

The grounding idea behind this category is that generally when an employee memorializes something, whether it be in writing, video, or photo, there is an intention to create a reference to that fixed point in time. Once documented, the risk of that content becoming known to others increases as the idea or memory no longer only resides in the partaking individual's mind. Therefore, an employee's reasonable expectation of privacy decreases upon the creation of publishable content and the employee will have a difficult time raising a privacy-based defense. Moreover, when an employee consents to content participation and allows a third party access to such content, the employee will likely be found to have waived any privacy consent defenses. In this second context, facts and circumstances should be relevant in determining whether the employee has retained some level of expectation of privacy, including such factors as the nature of the relationship between the third party and the employee, whether the content was "produced" in a way that would have made it clear that it was readily suitable for sharing, the location where the content was

[190] *See supra* 413–30.

[191] *See supra* 419–21.

[192] *See supra* 414–15.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

captured (i.e., a public or a private space), and the media in which the content was created.

C. Involuntary Participation Without Posting Consent

This scenario is analogous to a "hidden-camera" situation where the third party is operating the hidden camera and the employee has not participated in the content creation and has no knowledge of the third party's posting intention or the subsequent posting itself. This category can be a slippery slope for employers and requires a sliding scale. The reasonable expectation of privacy analysis should be applicable, but deeply connected to where the content was created. Where an employee has a reasonable expectation of complete privacy—such as the home, in which the areas with the greatest degree of protection would likely include bedrooms and bathrooms[193]—employers should be prohibited from using any captured content as the basis for an adverse employment action. Permitting the use of such content against an employee would cause audience segregation to cease to exist, creating a "fish bowl" culture.

Conversely, an employer would likely be able to use content captured by third parties in spaces where an individual would have no reasonable expectation of privacy, for example outside the home. Drawing a parallel from surveillance law, it is generally permissible to record surveillance video in public places—retail stores, places of business, parks, shopping malls, or city streets.[194] The expectation of privacy rights should only be extended to public places in rare circumstances, specifically "private" areas like hotel rooms, restrooms, or locker rooms. This privacy shield would likely extend to other public environments where individuals would expect their interactions and conversation to be protected; for example, a conversation between two individuals dining at a restaurant. Again, facts and circumstances should be relevant to situations where privacy protection is not automatic, including situations in which the employee has or has not taken action to ensure the confidentiality or privacy of the recorded content.

There is an underlying public policy argument that, for the benefit of society, individuals should conduct themselves respectfully and properly, particularly in

---

[193] Joseph G. Cook, *The Standing Requirement—Searches and Seizures*, 3 CONST. RTS. ACCUSED 3D § 12:13 (Aug. 2019).

[194] Hon. James G. Carr et al., *Electronic Surveillance Without a Court Order*, 1 LAW ELECTRONIC SURVEILLANCE § 3:76 (Apr. 2019); *Know Your Rights When Taking Photos and Making Video and Audio Recordings*, ACLU PA., https://www.aclupa.org/en/know-your-rights/know-your-rights-when-taking-photos-and-making-video-and-audio-recordings (last visited Oct. 26, 2019); *What's Legal and What's Not When Placing Hidden Cameras in Your Home, Your Office or in Public Places?*, BRICK HOUSE SEC. (Apr. 20, 2017), https://www.brickhousesecurity.com/hidden-cameras/laws/.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

public settings so as to not disrupt or endanger others. If one chooses to act otherwise when entering the public arena, individuals are deemed to have been put on notice that their actions, whether viewed by others directly or via social media, are subject to review by interested parties such as employers and law enforcement officials.

D. Illegal Actions

Individuals often leave small clues about their lives all over social media, just like fingerprints, allowing employers to use content to pursue adverse employment actions in the same manner as officials use such clues to glean evidence to help solve crimes. Analogously, law enforcement has long relied on the community's eyes and ears to help identify suspects, conduct investigations, and capture fugitives. The interconnectivity of today's world and the predominance of technology has aided this process such that social media has become a prevalent crime-fighting tool for law enforcement agencies.[195] In criminal cases, social media can assist in proving someone's innocence, irrevocably showing guilt, effectively corroborating witness testimony or contradicting it.[196] The same should hold true within the employment context for employers when off-duty employees are caught through social media posts by third parties engaging in illegal acts.

However, hacking, skimming, and other manipulative tactics threaten the authenticity and admissibility of evidence ascertained through handheld devices, which is transferable to any user's content on social media, whether videos, photos, or statements. Akin to criminal investigations, an employer wishing to utilize social media content for adverse employment decisions must determine the source of the content, how it was captured, its authenticity, who maintains the equipment, and how it relates to relevant circumstances to properly and effectively use the content in making employment decisions with regard to an employee.

As previously demonstrated, privacy laws in the realm of digital information is a clouded area of the law, and practically non-existent in the context of third-party posts. An individual's protections under the Fourth Amendment are forfeited when one shares online content with others.[197] Consequently, in the context of third-parties' depiction of the illegal acts of another, the perpetrating individual has no

---

[195] Heather Kelly, *Police Embrace Social Media as Crime-Fighting Tool*, CNN (Aug. 30, 2012), https://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html.

[196] *See, e.g.*, *id.*

[197] *See supra* 413–15.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

expectation of privacy when partaking in an illegal act.[198] In this respect, the online and offline world similarly allow third parties to capture evidence or provide information regarding an employee to their employer in the same manner as they can provide such information to police officers.

It should be inconsequential whether an individual posts information about himself or herself engaging or having engaged in an illegal activity or whether the source of that information is a third party. In either situation, the posted material is proof of an illegal act that occurred, which would support disciplinary action, similar to a police officer's or prosecutor's use of such content.

III. CONCLUSION

The dominance of social media has caused once personal beliefs and closely-held opinions to be edged into the public realm. Many employees now utilize social media as their predominant form of communication for posting information or opinions. Such postings may implicate their employers' interests, causing employers to regulate and monitor certain aspects of employees' social media activity. Restricting employees' social media activity is grounded in the desire of employers to protect their ability to operate as commercial enterprises through exercising their legitimate interests. However, as established herein, it has become increasingly challenging to retain a bright line between workplace and non-work activities. Employers must tread carefully when deciding whether to refuse to hire, discipline, or terminate candidates or employees for off-duty social media activity. Federal and state constitutions and statutes provide certain levels of protection with regard to an employer's ability to monitor and take employment-related actions based on an employee's social media activity, though none specifically addresses third-party postings or publication of an employee's conduct. The proposed analysis for determining whether an employer can act in response to a third-party posting of an employee relies on a different framework that attempts to reflect and expand upon the current state of the law. Specifically, in addressing third-party content an employer should engage in a threshold analysis centered on the employee's participation and consent to the posting. As the employee's participation and consent decrease, so does the employers right to discipline or discharge the employee for the third-party posted content. An exception to this rule, as presented in this Note, is for

[198] *See* California v. Greenwood, 486 U.S. 35, 41 (1988) ("[P]olice cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public."); *see also* Mund, *supra* note 59, at 249 (discussing that, when publishing content, a social media publisher takes a risk that: (1) his network connections will direct the content to law enforcement or (2) an undercover agent is actually posing as one of their network connections).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu

illegal actions of the employee, where no such balancing of interests should be necessary.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.678
http://lawreview.law.pitt.edu