LABORING TOWARDS NEW PRIVACY PROTECTIONS IN THE WORKPLACE

Jairo R. Villalobos*

ABSTRACT

Employers undoubtedly have an interest in monitoring workplace activity to gather information. However, the rapid development of new technology and subsequent erosion of technological constraints on employee monitoring has magnified the invasiveness of employer surveillance activities. Coupled with a decline in labor union membership throughout the country and mobilization of the workforce, these changes have made it much more difficult for employees to object to unfair and abusive privacy practices by their employer. This Note analyzes the shortcomings of the existing privacy protections for employees and the ways in which big data analytics allow employers to circumvent existing privacy protections and harm employee privacy interests. Villalobos argues that more rigorous protections of employee data are needed. By examining the existing legal privacy landscape in the employment context, Villalobos proposes a general framework for thinking about federal privacy legislation through a fictitious Federal Privacy Law that protects the privacy rights of employees and all Americans. Villalobos argues this proposal will best serve the interests of employees who have been left unprotected by existing privacy laws.

* J.D. (2021), Washington University School of Law.

INTRODUCTION

The California Consumer Privacy Act (CCPA) is a sweeping privacy law that went into effect in 2018.[1] The goal of this legislation was to enhance consumer control over the personal information that businesses collected about them. Various questions about the scope of the act emerged after its passing, including whether employees were considered "consumers" under the Act. If so, this effectively meant that the data employers collect on their employees would be covered.[2] In a compromise to business interests, the California legislature passed Assembly Bill 25 in 2019 to exempt employers for one year from the law's coverage on data collected from employees and job applicants for purposes solely related to employment.[3]

The controversy surrounding the CCPA's coverage of employee data and the business community's hard push for Assembly Bill 25 raise broader policy questions about the status of existing protections, or lack thereof, for such data. What privacy protections, if any, exist for employees? Should more rigorous protections of employee data exist? Existing privacy laws applicable in the employment context are narrowly focused and deal extensively with the intrusiveness of data-gathering methods, the sensitive nature of the original data directly collected from employees, or both.[4] The narrow focus between both spheres has resulted in a patchwork of outdated

1. The California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100.

2. *Id.* ("(n) 'Person' means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert . . . (o) (1) 'Personal information' means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.").

3. *See* CAL. CIV. CODE § 1798.145(h)(1)(A) ("This title shall not apply to any of the following . . . Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business."). *See also* Anthony J. Oncidi & Cole D. Lewis, *Employees Will Be Exempted from Most Requirements of the Amended California Consumer Privacy Act … For Now*, NAT'L L. REV. (Sept. 24, 2019), https://www.natlawreview.com/article/employees-will-be-exempted-most-requirements-amended-california-consumer-privacy-act [https://perma.cc/4R3K-UBFN].

4. Pauline T. Kim, *Data Mining and the Challenges of Protecting Employee Privacy under U.S. Law*, 40 COMP. LAB. L. & POL'Y J. 405, 412 (2019). "This emphasis on indignity and mental suffering means that the common law right to privacy comes into play when the method of *gathering* information is unduly intrusive or the nature of the information *collected* is particularly sensitive." *Id.* (emphasis added).

protections ill-equipped to protect privacy interests in the twenty-first century. Not only are employees unaware of what data employers collect and store from them, but they generally have no rights to contest the data's accuracy or know how it is being used.[5] Even worse, an employer can easily overcome any existing procedural protection by simply issuing a notice to the employee.[6] Such employer collection and use of employee data with de facto impunity is harmful because employees lose control over their personal information, which undermines their autonomy, and derive no benefit from such activity. At minimum and in all fairness, employers should not benefit from collecting employee data—whether it be through selling such data to third parties or improving their internal efficiencies—without providing some benefit to the employees themselves, whether that be better employment benefits or increased compensation.

Privacy protections are even more imperative in today's society, where technology allows employers to amass more information from its employees than ever before through opaque or seemingly non-intrusive methods. Though most data collected today is non-sensitive in nature, which in part explains the lack of outcry for more privacy protections in the workplace, powerful big data analytic tools, such as predictive analytics, data mining, and machine learning, allow employers to *use* facially innocuous employee data to *infer* private information about those very same employees. Utilization of such advanced data analytic tools allows an employer to circumvent already dispersed and weak privacy protections.[7] The capability to derive private information from seemingly harmless data exacerbates the harm described above because employees are oblivious to what employers are actually doing with their data and how employers benefit from it. This lack of accountability in turn emboldens employers to be more aggressive in their data collection activities. This Note focuses on examining the existing legal privacy landscape in the employment context, including how big data analytics upends an already inadequate assortment

5. Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979 (2011). "Employers are free to eliminate actual employee privacy expectations through detailed, specific notices and deploy even highly intrusive monitoring technologies . . . ." *Id.* at 1034.

6. *Id.*

7. *See* Kim, *supra* note 4, at 407. "With data mining, individual privacy may be threatened not by the types of information actually collected, but because of what can be inferred from that information after it is aggregated and analyzed with other data." *Id.*

of privacy protections, and proposes new ways to think about updating privacy protections through a fictitious Federal Privacy Law (FPL) statute.

Part I provides a history of employer data gathering in the United States, specifically the way employers collect and use employee data, the evolution of employer data collection and related advances in technology, and the new threat posed by big data analytic tools. Moreover, Part I takes stock of the existing privacy protections in the common law, federal statutes, the CCPA, and those bargained for in the union context. Part II analyzes the shortcomings of existing privacy protections for employees and how big data analytics allow employers to circumvent existing privacy protections in ways that harm employee privacy interests. Part III proposes a general framework for thinking about federal privacy legislation that fully protects the privacy rights of employees and all Americans.[8]

PART I: HISTORY

A. Employer Data Gathering in Contemporary America

Employers undoubtedly have an interest in controlling the workplace and extracting the most value from its labor. Monitoring workplace activity to gather information is crucial to the employer for three reasons. First, collecting the right amount and type of information is necessary to make proper management decisions,[9] including data-driven decisions to improve efficiency and productivity. Second, an employer has an interest in protecting its assets and preventing confidential and proprietary information from being disclosed by employees either purposely or inadvertently.[10]

8. Two clarifications are in order before proceeding. First, this Note focuses on private employees, which are workers that are neither unionized nor publicly employed at any government level. Therefore, unless stated otherwise, use of the word "employee" throughout this note means a non-unionized, non-governmental worker. Nonetheless, this Note will consider negotiated privacy protections in the collective-bargaining context in addition to statutory protections specific to public employees to introduce different frameworks for thinking about privacy protections for non-unionized private employees. Second, this Note focuses on information the employer collects from an employee during that employee's employment term rather than data collected during a hiring process or purchased through third party entities.

9. Laura B. Pincus & Clayton Trotter, *The Disparity Between Public and Private Sector Employee Privacy Protections: A Call for Legitimate Privacy Rights for Private Sector Workers*, 33 AM. BUS. L.J. 51, 86 (1995).

10. *See* Determann & Sprague, *supra* note 5, at 982–83.

Third, an employer has an interest in shielding itself from liability.[11] For example, an employer might be concerned that "some employees may be downloading music, movies, and other materials in violation of copyright laws, which could result in the employer facing vicarious liability through the doctrine of respondeat superior"[12] or that employees might engage in "inappropriate e-mail and text messages and internet use [that] could spur [a] hostile work [environment]."[13] The rise of new technology, the changing labor markets, and the increasing use of big data analytics have enhanced the capability and interest of employers regarding gathering data from employees.

1. Technological Advancements in Data Gathering

Technological advancements have impacted the scope and effectiveness of employer data gathering. Early monitoring tools used for collecting employee data were restricted by the technological limitations of the time—not even Henry Ford's wealth and power could overcome these constraints.[14] Today, the "rapid erosion of technological . . . constraints on employee monitoring has magnified the invasiveness of surveillance activities" through an "advent of almost ubiquitous network records, browser history retention, phone apps, electronic sensors, wearable fitness trackers, thermal sensors, and facial recognition systems" that allow for limitless worker surveillance.[15] The technology today is ubiquitous enough that even small employers can afford it. Every keystroke, email message, wearable gadget, and practically any activity on computerized hardware

11. *Id.* at 984.
12. *Id.*
13. *Id.* at 985.
14. Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735, 741–42 (2017) ("As early monitoring of employees had to be conducted by human supervisors, such surveillance was hindered by both economic and technological limits. For example, in the early twentieth century, Henry Ford stalked the factory floor with a stopwatch, timing his workers' motions in a push for higher efficiency . . . Even with the help of the Sociological Department, Ford was constrained by what his human investigators could observe and record. Ford did not have access, for example, to remote technologies that could surveil his workers after hours, nor to the highly accessible genetic testing that was developed in the 1990s, which can now detect whether a worker has a higher than usual propensity for a particular disease.").
15. *Id.* at 743.

represents a datum point that is tracked, collected, and added to a seemingly endless data stockpile.[16]

2. Contemporary Labor Market Changes

Compounding this technology-driven excess in employer data collection is the changing nature of the labor market in the United States. First, the decline in labor union membership throughout the country has made it much more difficult for employees to object to unfair and abusive privacy practices by the employer.[17] Related, almost all non-unionized employees are "at-will"—meaning the employer can terminate the employee at any time for any reason—which inevitably pressures job applicants and current employees to accept employer data policies that undermine their own privacy interests.[18]

Second, the labor market became more mobile in the second half of the twentieth century and into the twenty-first century, which inadvertently increased the amount of data that employers collect from an increasing number of job applicants and employees hired for revolving entry-level positions within their companies.[19] The rise in data collection caused by this

16. Don Peck, *They're Watching You at Work*, THE ATLANTIC (Dec. 2013), https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/ [https://perma.cc/E239-JF2R] ("Torrents of data are routinely collected by American companies and now sit on corporate servers, or in the cloud, awaiting analysis. Bloomberg reportedly logs every keystroke of every employee, along with their comings and goings in the office. The Las Vegas casino Harrah's tracks the smiles of the card dealers and waitstaff on the floor (its analytics team has quantified the impact of smiling on customer satisfaction).").

17. *See* Ajunwa, Crawford & Schultz, *supra* note 14, at 741–42 ("The [*Electronic Supervisor: New Technologies, New Tensions*] report [from the U.S. Office of Technology Assessment] found that advances in computer monitoring had raised questions about fairness and privacy in regard to employer surveillance of employees. The report generally noted that because of declines in unionization, employees had little power to object to what they considered 'unfair or abusive monitoring.'").

18. *Id.* at 748.

19. *See* Matthew Bidwell, Forrest Briscoe, Isabel Fernandez-Mateo & Adina Sterling, *The Employment Relationship and Inequality: How and Why Changes in Employment Practices are Reshaping Rewards in Organizations*, 7 ACAD. MGMT. ANNALS 1 (2017) (describing, in part, the various dynamics that have moved the U.S. employment model from a closed, internal system to one more open to external markets and institutional pressures). "Stable long-term exchanges between employers and employees have been replaced by more flexible arrangements that allow organizations to adapt to environmental demands for their goods and services by restructuring, downsizing, and outsourcing." *Id.* at 6. Although new hires and predictive analytics is the focus of this Note, it is important to point out this change in labor to paint the broader picture that changes in the labor market have created a tremendous amount of data extraction from employees.

new labor market fluidity is further exacerbated by the fact that one in three Americans today are contract or freelance workers, who in many instances are required to wear or carry monitoring devices that intentionally and undeniably feed data to companies.[20]

Lastly, the lines between work and private life are being obscured. The increasing trend of "Bring-Your-Own-Device" to work (BYOD)[21] is blurring work-related and personal data together in the same device. Increasing BYOD policies allow the employer to "install applications and interfaces on the personal device that track not only work emails but personal texts, phone calls, downloads, and browser history."[22] Thus employers can snag personal information in their efforts to collect work-related information. Overall, the decline in union membership, increase in labor market mobility, and BYOD represent changes in the labor market that have increased the volume of employee data collection.

3. Big Data Analytics

The ever widening and unchecked scope of employer data collection is unprecedented in the United States. However, much of the data collected is innocuous in nature. Given this situation, one might wonder how collecting innocuous data affects employee privacy interests. For example, how can tracking and recording the number of keystrokes from an employee violate their privacy? Even with more complicated data content, such as work emails that provide more nuanced information, surely an employer does not have the time and resources to dig through and analyze every email generated by employees? The answer is that employers have "altered their investments in certain technologies and practices in light of constraining legal frameworks," so that instead of gathering a small amount of mundane personal information, employers are "acquiring unprotected and largely

20. *See* Ajunwa, Crawford & Schultz, *supra* note 14, at 746.

21. Patrick J. Beisell, *Something Old and Something New: Balancing "Bring Your Own Device" to Work Programs with the Requirements of the National Labor Relations Act*, 2014 U. ILL. J.L. TECH. & POL'Y 497, 500–01 (2014) ("In 2011, the Aberdeen group surveyed 415 companies across the globe and reported an even more significant acceptance of BYOD. Of the companies surveyed, seventy-five percent allowed employees to use their personal device for and at work. Also in 2011, Forester Research surveyed roughly 1,600 US information technology workers and reported that forty-eight percent of respondents were allowed to purchase the smartphone of their choice and use it for work.").

22. *Id.* at 520–21.

unregulated proxies and metadata, such as wellness information, search queries, social media activity, and outputs of predictive 'big data' analytics."[23]

Big data tools, such as predictive statistical analysis normally applied to stock-price movements on Wall Street or online marketing, are being applied to the labor market in ways that can alter the way millions of people are hired and evaluated.[24] Data mining—the process of analyzing large datasets to uncover new information—has allowed employers to extrapolate information that can be offensive and harmful to employees, indirectly but significantly undermining privacy interests of employees. In large part, "the vast increase in the range and depth of information that's routinely captured" through technological advancements we take for granted—from online job applications to everyday tools such as email or tracking hardware devices—has resulted in large data sets that have enabled predicative analytics to be effective and valuable.[25] For example, email is now commonplace in the workforce, and it presents a rich treasure trove of data that can be mined for insights to measure and evaluate success or failure in particular job roles.[26] As a result of the growing use of predictive analytics, analytics teams are now common in human-resource departments in companies of all sizes.[27]

B. Existing Privacy Protections in America

What legal protections exist to address potential employee data abuses? What sort of balance can be achieved to leverage all the benefits that advancements in technology and use of big data tools offer while repurposing and modifying privacy protections to be more effective in a digitized workplace? Before considering these questions, it is important to take stock of existing privacy protections in the United States.

---

23. *See* Ajunwa, Crawford & Schultz, *supra* note 14, at 739.

24. *See* Peck, *supra* note 16.

25. *Id.* ("By one estimate, more than 98 percent of the world's information is now stored digitally, and the volume of that data has quadrupled since 2007. Ordinary people at work and at home generate much of this data, by sending e-mails, browsing the Internet, using social media, working on crowd-sourced projects, and more—and in doing so they have unwittingly helped launch a grand new societal project.").

26. *Id.*

27. *Id.*

1. Common Law Privacy Protections

Privacy protections in the common law were developed in the twentieth century as courts began to provide remedies for certain invasions of privacy.[28] The Restatement of Torts attempted to provide some clarity by determining four invasion of privacy torts: (1) intrusion upon seclusion, (2) appropriation of name or likeness, (3) public disclosure of private facts, and (4) placing a person in false light,[29] with (1) and (3) dominating claims in courtrooms.[30]

The tort for intrusion upon seclusion "imposes liability on a defendant 'who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be *highly offensive* to a reasonable person.'"[31] Many courts have held that this highly offensive standard is a threshold requirement.[32] Courts have found it easy to apply the intrusion upon seclusion tort in cases involving secretive observation of employees in traditionally private spaces such as locker rooms or restrooms.[33] The intrusion upon seclusion claim, however, has been a limited remedy in practice because courts have often held that employees have a lower expectation of privacy in the workplace,[34] or that

28. *See* Kim, *supra* note 4, at 411–12. Another source of privacy protection for American workers is the common law invasion of privacy tort. This tort is rooted in Samuel Warren and Louis Brandeis' well-known 1890 article, in which they argued for recognition of a right to privacy. In their view, the right to privacy rested on a principle of "inviolate personality" and redressed dignitary harm by compensating for "mental pain and distress." *Id.* at 411 (footnotes omitted) (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196, 205 (1890)).

29. RESTATEMENT (SECOND) OF TORTS §§ 652A–652E (AM. LAW INST. 1977). "(1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other. (2) The right of privacy is invaded by (a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or (b) appropriation of the other's name or likeness, as stated in § 652C; or (c) unreasonable publicity given to the other's private life, as stated in § 652D; or (d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E." *Id.*

30. *See* Kim, *supra* note 4, at 411–12.

31. *Id.* at 412 n.37 (quoting § 652B) (emphasis added).

32. *See, e.g.*, K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. App. 1984).

33. *See, e.g.*, Koeppel v. Speirs, 808 N.W.2d 177 (Iowa 2011) ("In light of the policies underlying intrusion upon seclusion and our prior holdings, we conclude . . . [that an] electronic invasion occurs under the intrusion on solitude or seclusion component of the tort of invasion of privacy when the plaintiff establishes by a preponderance of evidence that the electronic device or equipment used by a defendant could have invaded privacy in some way.").

34. *See, e.g.*, Terrell v. Rowsey, 647 N.E.2d 662 (Ind. Ct. App. 1995) ("[The trial court considered] Terrell's diminished privacy interest while on Red Giant's property, Red Giant's rule

employers are justified in such intrusions due to legitimate business reasons.[35]

The tort for publicity to private life imposes liability "when a defendant 'gives publicity to a matter concerning the private life of another . . . if the matter publicized is of a kind that (a) would be *highly offensive* to a reasonable person, and (b) is not of legitimate concern to the public.'"[36] The threshold question for this tort is whether the matters disclosed are in fact private.[37] Whether disclosed facts are considered private is influenced by the way courts interpret the meaning of "publicity," which is very difficult to define and results in a case-by-case basis determination through a fact-intensive inquiry.[38] Since publicity of private life is the twin privacy tort of inclusion upon seclusion, it is interpreted similarly and shares many of the same limitations and concerns about its efficacy. Recognizing the difficulty and limitations of applying the common law privacy tort in the employment context, the Restatement of Employment Law attempts to provide guidance by preserving the basic structure of the common law privacy tort, while incorporating business and public interest considerations to provide a better approximation of today's workplace reality.[39] Importantly, the Restatement

---

against drinking on company property, which includes the right to require chemical screening tests, Red Giant's obligation to provide employees a safe workplace, and the momentary entrance of Terrell's car with no physical contact with Terrell. We agree with the trial court that, as a matter of law, Rowsey's actions do not offend a person of ordinary sensibility. Terrell was on his employer's property and he admitted to drinking alcohol, despite Red Giant's policy against drinking. Furthermore, Rowsey acted out of responsibility for the safety of Terrell and his fellow employees and the intrusion was minimal. For the foregoing reasons we affirm the judgment of the trial court.")

35. *See, e.g.*, Jennings v. Minco Tech. Labs, Inc., 765 S.W.2d 497 (Tex. App. 1989) (rejecting an employee's request for injunctive relief against an employer's urinalysis drug testing because the at-will status allows the company to apply modifications to the employment at any time). "In any case, her privacy interest will not be invaded without her consent, which is to say it will not be invaded by the company unlawfully so as to require and justify the injunctive relief she requested." *Id.* at 502.

36. *See* Kim, *supra* note 4, at 412 n.37 (emphasis added) (quoting § 652D).

37. *See* Borquez v. Robert C. Ozer, P.C., 923 P.2d 166 (Colo. App. 1995), *aff'd in part, rev'd in part*, 940 P.2d 371 (Colo. 1997) (holding that attorney had privacy interest in dissemination of information that he was homosexual and that his companion had been diagnosed with AIDS).

38. *Compare* Beyene v. Hilton Hotels Corp., 815 F. Supp. 2d 235, 254 (D.D.C. 2011) (ruling private facts at issue must be committed to the public at large and not just a single person or even small group of people), *aff'd*, 573 Fed. Appx. 1 (D.C. Cir. 2014), *with* Karch v. BayBank FSB, 794 A.2d 763, 769, 774 (N.H. 2002) (recognizing that disclosure of private facts to even a small group of colleagues can satisfy the element of publicity).

39. RESTATEMENT OF EMP'T LAW § 7.06 (AM. LAW INST. 2015).

> "(a) An employer is subject to liability for a wrongful intrusion upon an employee's protected privacy interest if the intrusion would be *highly offensive* to a reasonable person under the circumstances. (b) An intrusion is highly offensive

attempts to flesh out legitimate employee interests at stake that can be adversely affected by privacy protections.[40]

Notwithstanding all the common law difficulties mentioned above, some state courts have tried to strengthen privacy protections by extending other existing protections to the data privacy sphere.[41] For example, *Dittman v. UPMC* is a Pennsylvania case involving an employer's duty to protect its employees' data.[42] In that case, employees were injured through the loss of all their data and filed a class action against UPMC asserting claims of negligence and breach of implied contract.[43] The Supreme Court of Pennsylvania held that employers have a duty to exercise reasonable care to protect employees against unreasonable risk of harm arising out of the collection and storage of employee data.[44] Furthermore, the Pennsylvania Supreme Court explicitly stated that it could apply "an existing duty to a

---

> under subsection (a) if the nature, manner, and scope of the intrusion are clearly unreasonable when judged against the employer's legitimate business interests or the public's interests in intruding.

Id. (emphasis added) (cross-references omitted).

40. *Id.* at § 7.03 ("(a) An employee has a protected privacy interest against employer intrusion into: (1) the employee's physical person, bodily functions, and personal possessions; and (2) physical and electronic locations, including employer-provided locations, as to which the employee has a reasonable expectation of privacy. (b) An employee has a reasonable expectation in the privacy of a physical or electronic work location provided by the employer if: (1) the employer has provided notice that the location or aspects of the location are private for employees; or (2) the employer has acted in a manner that treats the location or aspects of the location as private for employees, the type of location is customarily treated as private for employees, and the employee has made reasonable efforts to keep the employee's activities in that location private. (c) An employer intrudes upon an employee's protected privacy interest under this Section by such means as an examination, search, or surveillance into the locations discussed in subsection (a).").

41. *See, e.g.*, Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739 (S.D.N.Y. 2017).

> Employees ordinarily have no means to protect that information in the hands of the employer, nor is withholding their PII a realistic option . . . Employees—much more than employers—suffer the harmful consequences of a data breach of the employer. Potential liability in the absence of reasonable care provides employers with an economic incentive to act reasonably in protecting employee PII from the threat of cyberattack.

Id. at 748. *Cf.* Enslin v. Coca-Cola Co., 136 F. Supp. 3d 654, 677 (E.D. Pa. 2015) (holding, *inter alia*, that no special relationship existed between employer and employee, whose personal information was stolen from employer's laptops, and thus employee's negligence claim was barred by economic loss doctrine), *aff'd*, 739 Fed. App'x. 91 (3d Cir. 2018).

42. Dittman v. UPMC, 196 A.3d 1036, 1047 (Pa. 2018).

43. *Id.* at 1039.

44. *Id.* at 1047. "Thus, we agree with Employees that, in *collecting* and *storing* Employees' data on its computer systems, [the Employer] owed Employees a duty to exercise reasonable care to protect them against an unreasonable risk of harm arising out of that act." *Id.* (emphasis added).

novel factual scenario, as opposed to the imposition of a new, affirmative duty,"[45] thereby extending negligence liability to an employer's handling of employee data and demonstrating a way in which existing common law protections can be modified to cover societal changes underpinned by advances in technology.

2. Federal Statutory Protections

Beyond the common law, a patchwork of federal statutes advance protections on employee data. Federal privacy protections are scattered across different statutes because such privacy protections were ancillary features in the achievement of other statutory goals, not necessarily because privacy itself was the concern these statutes tried to address.[46] The following paragraphs provide a non-exhaustive look at the patchwork of existing privacy protections at the federal level.

The Fair Credit Report Act (FCRA) restricts the use of consumer credit information for employment purposes by regulating the manner in which employers can request, receive, and use background checks from third parties.[47] Employers must also notify job applicants or employees in writing and get written consent from them before accessing their consumer report for employment purposes.[48] An applicant or employee is also entitled to a "pre-adverse action disclosure" if the employer decides to take adverse

45. *Id.* at 1046.

46. *See* Ajunwa, Crawford & Schultz, *supra* note 14, at 747 ("There are no federal laws that expressly address employer surveillance or limit the intrusiveness of such surveillance. The federal laws that have been created for the benefit of workers focus instead on protecting them from employment discrimination while largely disregarding privacy claims. When federal laws have proscribed worker surveillance, such proscription has been incidental to curtailing employment discrimination of protected minority groups.").

47. 15 U.S.C. § 1681b(b).

48. § 1681b(b)(2)(A).

> **Disclosure to consumer**. . . Except as provided in subparagraph (B), a person may not procure a consumer report, or cause a consumer report to be procured, for employment purposes with respect to any consumer, unless-- **(i)** a clear and conspicuous disclosure has been made in writing to the consumer at any time before the report is procured or caused to be procured, in a document that consists solely of the disclosure, that a consumer report may be obtained for employment purposes; and **(ii)** the consumer has authorized in writing (which authorization may be made on the document referred to in clause (i)) the procurement of the report by that person.

Id.

action because of the person's credit report.[49] The disclosure includes a copy of the consumer report and information about the applicant's right to dispute the information on the consumer report.[50] If an investigative report was requested from a third party for an applicant or employee, the employer must tell the applicant or employee about their right to a description detailing the nature and scope of the investigation.[51]

The Health Insurance Portability and Accountability Act (HIPAA) applies to entities including "health plans, healthcare clearinghouses, and any healthcare provider that transmits health information in electronic form in connection with certain transactions affected by HIPAA" or "entities that act on behalf of, or provide certain services to" the aforementioned entities.[52] HIPAA limits use and disclosures in the following six areas:

> (1) disclosures to the individual, unless required for access or accounting of disclosures; (2) as required for treatment, payment, and care operations; (3) where individuals agree to disclosure; (4) where disclosure is "incidental" to an otherwise lawful disclosure; (5) for public interest purposes; and (6) where information is disclosed as part of a "limited data set."[53]

49. § 1681b(b)(3)(A) ("**Conditions on use for adverse actions**. . . Except as provided in subparagraph (B), in using a consumer report for employment purposes, before taking any adverse action based in whole or in part on the report, the person intending to take such adverse action shall provide to the consumer to whom the report relates – **(i)** a copy of the report; and **(ii)** a description in writing of the rights of the consumer under this subchapter, as prescribed by the Bureau under section 1681g(c)(3) of this title [i.e. summary of rights to obtain and dispute information in consumer reports and to obtain credit scores].").

50. *Id.*

51. 15 U.S.C. § 1681d(b) (1997). ("**Disclosure on request of nature and scope of investigation**. Any person who procures or causes to be prepared an investigative consumer report on any consumer shall, upon written request made by the consumer within a reasonable period of time after the receipt by him of the disclosure required by subsection (a)(1), make a complete and accurate disclosure of the nature and scope of the investigation requested. This disclosure shall be made in a writing mailed, or otherwise delivered, to the consumer not later than five days after the date on which the request for such disclosure was received from the consumer or such report was first requested, whichever is the later.").

52. Stuart L. Pardau, *The California Consumer Privacy Act: Towards A European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68, 80 (2018).

53. *Id.*

Other statutes provide more limited privacy protections to disclosed or collected employee data. The Genetic Information Nondiscrimination Act (GINA) constrains the employer's ability to obtain genetic information about its employees or their family members.[54] As the statute title makes obvious, the purpose of GINA is to prevent discrimination based on genetic traits in employment practices such as hiring or termination, terms and conditions, compensation, and privileges related to employment.[55] The Americans with Disabilities Act (ADA) prevents an employer from discriminating against people with respect to their disabilities when it comes to employment, compensation, terms and conditions, advancement, or termination.[56] With respect to hiring, the ADA restricts employers from making inquiries into the job applicant's potential disabilities[57] or requiring a medical examination before an employment offer is made.[58] Recognizing the need to provide employers with some flexibility, the ADA allows inquiries that relate to the applicant's ability to perform "job-related functions"[59] and permits a medical examination request after an employment offer has been made.[60] GINA and ADA privacy protections are narrow and situational to the specific harms both statutes attempt to address, specifically discrimination at large. Therefore, GINA and ADA are

54. *See* 42 U.S.C. § 2000ff-1(b) (2008). "**Acquisition of genetic information.** It shall be an unlawful employment practice for an employer to request, require, or purchase genetic information with respect to an employee or a family member of the employee . . . ." with some exceptions provided. *Id.*

55. *See* § 2000ff-1(a) ("**Discrimination based on genetic information**. It shall be an unlawful employment practice for an employer – **(1)** to fail or refuse to hire, or to discharge, any employee, or otherwise to discriminate against any employee with respect to the compensation, terms, conditions, or privileges of employment of the employee, because of genetic information with respect to the employee; or **(2)** to limit, segregate, or classify the employees of the employer in any way that would deprive or tend to deprive any employee of employment opportunities or otherwise adversely affect the status of the employee as an employee, because of genetic information with respect to the employee.").

56. 42 U.S.C. § 12112(a) (2008). "**General rule**. No covered entity shall discriminate against a qualified individual on the basis of disability in regard to job application procedures, the hiring, advancement, or discharge of employees, employee compensation, job training, and other terms, conditions, and privileges of employment." *Id.*

57. § 12112(d)(1). "**In general.** The prohibition against discrimination as referred to in subsection (a) shall include medical examinations and inquiries." *Id.*

58. § 12112(d)(2)(A). "**Prohibited examination or inquiry**. Except as provided in paragraph (3), a covered entity shall not conduct a medical examination or make inquiries of a job applicant as to whether such applicant is an individual with a disability or as to the nature or severity of such disability." *Id.*

59. *See* § 12112(d)(2)(B).

60. *See* § 12112(d)(3).

circumstance-specific remedies only available for protected classes covered under those statutes.

Not only are certain privacy protections exclusive to specific classes of people, but some statutory protections are exclusive to public employees.[61] The Freedom of Information Act (FOIA) of 1966, enacted to allow more transparency and greater public access to government-controlled information, is governed by five basic principles that secure and protect privacy rights:

> 1) privacy is a fundamental right; 2) protection against the government's intrusions into an individual's private affairs is guaranteed by the right to privacy; 3) an informed electorate is essential to safeguard privacy; 4) publicity is a protection against the potential of government official misconduct; and 5) secrecy is an essential part of bureaucracy but may not be a beneficial facilitator of bureaucratic efficiency.[62]

Acknowledging that the importance of ensuring free access to government data still requires protecting privacy rights of individuals, FOIA was amended through the Privacy Act of 1974:

> With certain exceptions, the [Privacy Act of 1974] provides that agencies' records may only contain relevant and necessary information. Second, agencies should attempt to collect information directly from the subjects of the records rather than from third parties. Third, when information is requested on individuals, they must be informed of the purpose of its collection and the uses to which the information will be put. Fourth, individuals must be afforded an opportunity to review their files upon request, and individuals may request amendment of a record (and other requirements similar to the

61. Public employees also enjoy Fourth Amendment protection. *See* O'Connor v. Ortega, 480 U.S. 709 (1987) (recognizing that searches and seizures by government employers or supervisors of private property of their employees are subject to Fourth Amendment restrictions).

62. *See* Pincus & Trotter, *supra* note 9, at 70.

> FCRA). Fifth, records about an individual should not be disclosed to third parties without the subject's written consent, unless the disclosure is for a "routine" use, and a record of all disclosures made about an individual must be made available to him or her upon request. Finally, individuals may sue for damages and injunctive relief for violations of the above provisions. [63]

The balance that FOIA attempts to achieve can serve as a model for the balance that should be attained between employer interests in growth and innovation with legitimate employee privacy interests generally.

3. California Case Study

The 2018 California Consumer Privacy Act (CCPA), considered the strictest state level privacy law in the United States against companies that collect personal information from consumers,[64] mirrors the European Union's General Data Protection Regulation (GDPR) in many ways.[65] In emulating the GDPR, the CCPA provides consumers, which includes employees,[66] with the right to "demand records from a company on the personal data which is maintained by the company," including the right to "demand that a company delete personal data and refrain from selling

63. *Id.*

64. *See* Jessica Guynn, *California Passes Nation's Toughest Online Privacy Law*, USA TODAY (Jul. 6, 2018), https://www.usatoday.com/story/tech/2018/06/28/ca1ifornia-lawmakers-pass-tough-new-online-privacy-rules-could-model-other-states/743397002/ [https://perma.cc/A2XV-UX6H].

65. Blake A. Klinkner, *Understanding the Changing Landscape of Data Protection Laws*, WYO. LAW., February 2019, at 44. For summary information on recent privacy law activity at the state level, *see* Cynthia Brumfield, *11 New State Privacy and Security Laws Explained: Is Your Business Ready?*, CSO (Aug. 8, 2019), https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html [https://perma.cc/L4JZ-HU2X] (state statutes include, among others, Nevada Senate Bill 200 Online Privacy Law and Maine Act to Protect the Privacy of Online Consumer information). *See also* Samuel D. Goldstick, Jennifer L. Rathburn & Aaron K. Tantleff, *Ringing in 2019 with New State Privacy and Data Security Laws Impacting Data Brokers*, NAT'L L. REV. (Jan. 10, 2019), https://www.natlawreview.com/article/ringing-2019-new-state-privacy-and-data-security-laws-impacting-data-brokers-and [https://perma.cc/LMY5-H78D].

66. *See* CAL. CIV. CODE § 1798.100.

personal data to other entities."[67] Businesses are also required to provide privacy policy disclosures and "grant a consumer the right to opt-out of the sale of personal information."[68] Moreover, the CCPA prevents business discrimination against people who exercise the rights it grants in order to prevent a chilling effect.[69] The CCPA also provides the following remedies in a civil action: "(1) statutory damages from $100 to $750 per consumer per incident, or actual damages, whichever is greater; (2) injunctive or declaratory relief; or (3) [a]ny other relief the court deems proper."[70] Even as the strongest state privacy law in the United States, the CCPA has its shortcomings. For starters, the CCPA "excludes certain personal information covered by federal privacy laws" such as the FCRA.[71] Also, CCPA subjects consumers to several requirements which include providing the business with thirty days' written notice about the violation and an opportunity to cure.[72]

4. Bargained-For-Protections

Outside of the common law and statutory spheres, collective bargaining has been another mechanism by which employees have historically secured privacy protections. *Colgate-Palmolive Co.* was an important decision by the National Labor Relations Board (NLRB) that involved an employer's placement of hidden cameras in a restroom and fitness center, which "clearly raise[d] a concern over an individual's privacy and intrudes into employee's personal and private lives, even if it occurs on what is nominally company property."[73] In making its decision, the NLRB relied on *Ford Motor Co. v. NLRB*.[74] In *Ford Motor Co*., the U.S. Supreme Court reasoned

67. Klinkner, *supra* note 65, at 44. CCPA is different from the GDPR, however, in that it "it permits businesses to charge special fees to consumers if those consumers request that their personal data not be sold, as a method of recovering lost revenues from the sale of personal data." *Id.*

68. *See* Pardau, *supra* note 52, at 98.

69. *See* CAL. CIV. CODE § 1798.125(a)(1).

70. *See* Pardau, *supra* note 52, at 99.

71. *See id.* at 93. *See also, e.g.*, CAL. CIV. CODE § 1798.145(d)(1) (stating that "title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code").

72. *See* Pardau, *supra* note 52, at 99–100.

73. Colgate-Palmolive Co., 323 N.L.R.B. 515, 519 (1997).

74. *Id.* at 515.

that mandatory subjects of bargaining are those "plainly germane to the working environment" and "not among those managerial decisions, which lie at the core of entrepreneurial control."[75] Using this framework, the NLRB held that installation of surveillance cameras in the workplace was germane to the working environment, and thus a mandatory subject of bargaining, by analogizing installation of such cameras to "physical examinations, drug/alcohol testing requirements, and polygraph testing."[76] Moreover, it held that the "installation and use of surveillance cameras in the workplace are not among that class of managerial decisions that lie at the core of entrepreneurial control" and is thus "not fundamental to the basic direction of the enterprise, and impinges directly on employment security."[77] Therefore, privacy concerns are a proper subject of collective bargaining, which could very well include the use of big data tools and information gathered from them.

PART II: ANALYSIS

Although recent advancements in technology have made data gathering and usage more tenable and economical, "there have been no sweeping legal changes to address these new technological advancements in surveillance."[78] Existing privacy protections have not kept pace with the rapid changes in both technology and a labor market that has undergone a change from a an "authoritarian regime"—where employers directly surveil employees to collect data—to a "participatory regime"—where employees provide data through everyday tools such as email and productivity apps.[79] Put differently, the nature of gathering employee data has changed from an intentional undertaking by the employer to one that is "participatory" insofar as employee usage of new technologies generates data for the employer to later analyze. The participatory paradigm is underscored by the

75. *Id.* (internal quotation marks omitted).
76. *Id.*
77. *Id.*
78. *See* Ajunwa, Crawford & Schultz, *supra* note 14, at 739–40.
79. *Id.* at 739. "Similarly, Amazon, perhaps the largest retailer in America, requires their workers to carry electronic tablets that record both their speed and efficiency as the workers retrieve merchandise to fulfill orders by online shoppers; and in some hospitals, nurses now wear electronic badges that track how often the nurses wash their hands." *Id.* at 744 (citing *The Rise of Workplace Spying*, WEEK (July 5, 2015), http://theweek.com/articles/564263/rise-workplace-spying [https://perma.cc/NKP9-VSJZ]).

fact that, in many instances, employees may be unaware of the extent to which their employer is collecting data from their daily activities.[80] In part, this could explain the absence of public concern or employee outrage over ways in which the modern workplace adversely impacts privacy interests through its method of collecting and using information obtained from employees.

Even putting aside the elevated concerns of personal data being collected due to BYOD policies, work-related data that seems benign and inconsequential on the surface poses a threat to privacy in large part because of big data analytical tools. Big data tools can present various issues at work—from anxiety to disparate impact results in hiring decisions—and employee privacy interests are particularly implicated in ways that existing protections, both narrow and scarce, are not equipped to address in today's world.[81] The "highly offensive" standard embedded in both the intrusion upon seclusion and publicity privacy torts, which maintains a central role in the Restatement of Employment Law, regulates "not privacy, but outrage" which results in the protection of "freedom from emotional distress, not freedom of informational control."[82] Collection of innocuous data, such as employee health data gathered through workplace wellness programs, would not be classified as "highly offensive." By itself, collecting such information does not seem like an outrageous activity, and so it would not reach the level of a privacy tort. However, when all available 'innocuous' data is combined and analyzed using big data tools, employers may be able to extrapolate highly offensive information, such as a private medical

80. *Id.* at 743.

81. *See* Peck, *supra* note 16 ("These aspects of people analytics provoke anxiety, of course. We would be wise to take legal measures to ensure, at a minimum, that companies can't snoop where we have a reasonable expectation of privacy—and that any evaluations they might make of our professional potential aren't based on factors that discriminate against classes of people."). *See also* Pauline T. Kim, *Bid Data and Artificial Intelligence: New Challenges for Workplace Equality*, 57 U. LOUISVILLE L. REV. 313 (2019) (arguing that the law should be interpreted in ways that create incentives for employers to audit their data-driven HR processes for discriminatory impact while being critical of third-party algorithms advertised as neutral and legal). "Many big data and artificial intelligence tools rely on extensive data gathering about applicants and employees, which raises significant concerns about privacy. Those concerns warrant separate attention, so I will only mention here that while there are some legal limits on employers' ability to collect personal information, existing privacy laws are quite limited and are unlikely to slow collection of the types of information used to build workplace algorithms. As a result, employers' reliance on big data and algorithms to make personnel decisions is likely to grow." *Id.* at 315.

82. Matthew W. Finkin, *Employee Privacy, American Values, and the Law*, 72 CHI.-KENT L. REV. 221, 228 (1996).

condition. This second stage would fall outside the gambit of privacy torts altogether. Some have argued that privacy protections should cover employer actions that are systematically invasive—such as genetic, drug, and psychological testing—but that fall short of satisfying the "highly offensive" threshold standard, like reading an employee's email or peeking into the restroom.[83]

An argument can be made that courts have the flexibility to adjust existing common law causes of actions to address new privacy concerns connected to changes in technology.[84] However, relying on courts to develop or modify existing common law remedies to new and evolving methods of employee privacy invasion is insufficient for two reasons. First, courts will always have to play catch-up to rapid and evolving methods of privacy invasion due to institutional forces. For starters, development of common law remedies is limited by their adherence to caselaw precedent (stare decisis). Even if the courts become more aggressive in granting damages for intrusion upon seclusion claims and less swayed by business justification arguments, courts can only adjudicate cases that come before them (i.e., cases that the alleged harmed party brings). Given that most private employees are at-will and can be discharged at any time without cause, workers are hesitant to raise legitimate intrusion upon seclusion claims due to fear of potential employer retaliation.[85] Moreover, even if employees are undeterred, courts do not have the remedial tools to make an employee whole again. As demonstrated in the *Dittman* case above, employees were already injured by the data loss, and they were ultimately harmed in a manner that monetary compensation will not truly remedy because their personal information has been stolen.[86]

Second, common law privacy torts such as intrusion upon seclusion are substantively inadequate because they focus on the wrong aspect of today's privacy issues. As mentioned, the ways in which non-offensive data provided by employees in the new participatory regime is being *used* to implicate privacy interests is not the primary focus in common law.[87] But

83. *Id.* at 228–29. Arguing that the law should protect situations in which "an employer acts in a systematically invasive fashion in what it takes to be a legitimate business interest." *Id.*

84. Elizabeth D. De Armond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 40–42 (2008).

85. *See* Ajunwa, Crawford & Schultz, *supra* note 14, at 748.

86. *See supra* Section I.B.i.

87. *See* Ajunwa, Crawford & Schultz, *supra* note 14, at 739. Employers have also altered their investments in certain technologies and practices in light of constraining legal frameworks. As a result,

the new threat in the twenty-first century workplace exists in the way employers *use* rather than *collect* employee data.[88] Data mining can "alter the meaning and significance of personal information in ways that render traditional employee privacy protections largely ineffective."[89] Specifically, data mining and other analytic tools allow employers to extrapolate highly personal information from mundane, trivial employee datasets that alone are unlikely to be considered highly offensive.[90] In effect, employee privacy is threatened through the *extrapolation* of highly personal information rather the *collection* of it, allowing employers to circumvent common law privacy protections focused on *collection* activities by *using* data analytics tools to obtain personal information in derivative fashion. These issues are exacerbated by the judiciary's approach to privacy tort cases and the omnipresent deterrence that prevents at-will employees from even filing a claim in court, which inevitably work to undermine the efficacy of privacy protections arising out of common law.[91]

The slow pace in modifying common law privacy protections, as illustrated in the *Dittman* case, makes the statutory route a more appealing direction. Statutes are not limited by the same institutional challenges that common law privacy torts face. However, existing statutes do not properly address privacy concerns in today's world because, similar to common law privacy protections, they are not properly focused. Specifically, the problem with existing statutory privacy protections of employee data is that the focus remains on the *collection* and *management* of employee data. For example, GINA prevents an employer from requesting, requiring, or purchasing genetic information.[92] But an employer can gather this same data by using predictive analytics to *extrapolate* information about either an employee's likely genetic disposition or predisposition, or even illegally make employment decisions on compensation or terms and conditions based on aggregate information where genetic traits are subsumed in that aggregate

there has been a shift in focus from collecting personally-identifying information, such as health records, to wholly acquiring unprotected and largely unregulated proxies and metadata, such as wellness information, search queries, social media activity, and outputs of predictive "big data" analytics. *Id.*

88. *See* Kim, *supra* note 4, at 415.

89. *See id.* at 406.

90. *See id.* at 415–16.

91. For a survey of the recognition of intrusion upon seclusion in the fifty states, see Eli A. Meltz, *No Harm, No Foul? "Attempted" Invasion of Privacy and the Tort of Intrusion Upon Seclusion*, 83 FORDHAM L. REV. 3431, 3440 (2015).

92. *See* 42 U.S.C. § 2000ff-1(b) (2008).

dataset.[93] Datasets allowing this type of inference are ever more attainable with employer-sponsored wellness programs that provide insurance discounts in exchange for health data provided through wearable fitness devices.[94]

Additionally, most federal privacy protections are ancillary means in furtherance of other policy objectives, which means that the availability and applicability of such provisions is narrowed to specific societal contexts. For example, while the ADA prohibits employers from requiring job applicants to undergo medical exams prior to receiving an offer, it allows employers to request medical examinations after making an offer under limited circumstances.[95] FCRA is the most privacy centered statue explored in this Note. However, FCRA provides rights and protections in procedural, rather than substantive, form. For example, the disclosure mechanisms allow an affected party to dispute reported information, but it does not grant a right to force the data holder to delete the affected party's data.[96] Put differently, a party can dispute the content of their personal data through the procedure established by the FCRA, but that same party does not have a right to the ownership and use of that data. Therefore, the federal privacy protections are insufficient in today's society because not only are they not available in every context, but they are designed to be ancillary to other policy objectives; and they are procedural rather than substantive in nature. As a prominent scholar noted, "[n]o comprehensive statutory scheme supplements the common law to provide protection for employees' privacy or even simply from employer monitoring."[97]

Protections in the collective bargaining context are only an option if they are able to be bargained for in the first place. Today, employees lack

93. *See* Kim, *supra* note 4, at 406–07.

94. Stephanie O'Neil, *As Insurers Offer Discounts For Fitness Trackers, Wearers Should Step With Caution*, ASPEN NAT'L PUB. RADIO (Nov. 19, 2018), https://www.npr.org/sections/health-shots/2018/11/19/668266197/as-insurers-offer-discounts-for-fitness-trackers-wearers-should-step-with-cautio [https://perma.cc/3C3K-Z8HU] (investigating the insurance discount incentives millions of Americans utilize by wear fitness devices that "track an assortment of personal information — everything from movement and sleep patterns to blood pressure and heartbeats per minute"). *See also* Tara Siegel Bernard, *Giving Out Private Data for Discount in Insurance*, N.Y. TIMES (Apr. 8, 2015), https://www.nytimes.com/2015/04/08/your-money/giving-out-private-data-for-discount-in-insurance.html [https://perma.cc/RX2Y-KF8J].

95. *See* 42 U.S.C. § 12112 (d)(2)(A), (d)(3) (2008).

96. *See* 15 U.S.C. § 1681b(b)(2)-(3).

97. Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J.L. & PUB. POL'Y 609, 620–21 (2009).

individual bargaining power to negotiate for such protections. Notwithstanding the decline in union membership,[98] "increased employer surveillance . . . can have a chilling effect" on union activity if "employees will reasonably fear that the surveillance has been implemented in order to facilitate later retaliation by the employer."[99]Advanced analytics such as big data tools and their augmentation through "increasingly sophisticated, subtle, and effective means of surveilling their employees' actions, communications, and even attitudes, both inside and outside of work"[100] have deterred unionization efforts. Use of "closed circuit cameras" that allow an employer to know when an employee walks away from their computer, or "radio-frequency identification badges" that create "a log of each employee's locations throughout the day," did not exist at the time *Colgate-Palmolive* was decided, but the underlying concern over implementing surveillance programs to deter union organizing remains the same.[101] At minimum, employees should be able to bargain not only on the collection of their data, but also the utilization of that data via predictive analytic tools that can infer personal information from data collected at the workplace and, at an increasingly alarming rate, private spaces.[102]

98. *See* Ajunwa, Crawford & Schultz, *supra* note 14, at 741–42.

99. Charlotte Garden, *Labor Organizing in the Age of Surveillance*, 63 ST. LOUIS U.L.J. 55, 63 (2018).

100. *Id.* at 57.

101. *See id.* at 62.

102. Beisell, *supra* note 21, at 520–21. "With a BYOD policy in place, the employer can install applications and interfaces on the device that track not only emails but texts, phone calls, downloads, and browser history" from personal devices that can snag personal information in addition on top of work-related information. *Id.*

PART III: PROPOSAL

Protecting employee privacy interests from employer violations through use of sophisticated big data tools requires that the aforementioned shortcomings be addressed. Unlike the existing patchwork of ancillary privacy protections furthering different statutory objectives, Congress should pass a Federal Privacy Law (FPL) that is focused on creating new privacy protections for all Americans and include a separate title or section that specifically addresses employee interests and the unique challenges they face in the workplace. A balance must be achieved where employers can adopt, implement, and use big data technology in a way that improves and enhances the services they provide to society without undermining the privacy interests of their employees.

First, the FPL can make use of the CCPA as a statutory blueprint, especially in devising substantive protections. Procedural rights allowing employees to demand a record of their personal data from their employer—also present in FCRA's more diluted disclosure protections—and the substantive right to terminate or place restrictions on the sale and use of their data are required. Such protections would allow employers to leverage big data analytic tools to provide better goods and services without harming their employees by violating their privacy. Although it is reasonable and anticipated that the FPL will include legitimate business use exemptions, employers should have to meet a high standard to qualify for such exemptions, or else such a provision will serve as a workaround that can undermine the FPL's overall objective. In contrast to the CCPA, the FPL should provide stronger remedies that encourage people to litigate meritorious cases whenever possible.

Secondly, the FPL can buttress its substantive privacy rights by strengthening existing privacy protections in other laws. One way is to explicitly state that personal data is germane to the working environment and thus a mandatory subject of bargaining. Notwithstanding the decline in union activity, new or existing unions can bargain for enhanced privacy protections that are tailored to their specific work environment and go beyond those that will be provided by the FPL. In this vein, the law should unequivocally forbid contracting away the privacy rights it grants. The National Labor Relations Act (NLRA) can thus be leveraged via the FPL to force employers to bargain for privacy protections in applicable contexts

without being bogged down by its own precedent. The FPL should not only govern ways in which data is collected but also dedicate provisions to deal with *derivative* data extracted from large data sets through big data analytic tools. Doing so would force the federal courts to also focus on this derivative data and develop case law on for it.

Additionally, the FPL can cultivate societal norms around privacy protections. For example, by creating a legal avenue for people to control the sale and use of their personal information, standard terms around such sale and use will begin to develop. These norms can eventually influence state courts to evolve their common law to be responsive towards derivative data collection by expanding and modifying today's antiquated and insufficient privacy torts, thus allowing harmed parties to bring privacy tort claims in state court that cover use of big data analytics tools. In doing so, courts can provide a common law route that can serve as a supplementary or alternative legal remedy alongside the FPL.

Identifying and assessing the ways in which the FPL might implicate, undermine, or contradict existing federal laws with privacy provisions is beyond the scope of this Note. However, the proposed FPL is a helpful blueprint and starting point for thinking about a general framework that a nationwide privacy statute should embody. The FPL should be a baseline for states to build on by crafting and providing stronger privacy protections that may be needed to address statewide, and even local, needs.

CONCLUSION

Privacy matters because it takes "notice of the personhood of each individual" while recognizing "a respect for the individual's 'inviolate personality,' freedom, and autonomy."[103] This Note focused on examining the existing legal privacy landscape in the employment context, the way in which big data analytics upends an already weak and dispersed assortment of privacy protections, and proposed approaches to thinking about new privacy protections and propping up existing ones.

It cannot be overstated that privacy protections are even more important now than in the past. The changes in technology and the labor market that have been presented and analyzed in this note illustrate a new kind of threat

103. *See* Armond, *supra* note 84, at 23. "If dignity recognizes the right of each individual to his or her own, unique 'inviolate personality,' privacy allows that personhood to develop." *Id.* at 23.

to employee privacy interests that is less obvious than ever before. In particular, big data analytic tools allow employers to effectively subvert and circumvent already antiquated case law and statutory privacy protections that focus on the nature and collection of original data rather than derivative data obtained from large data sets that are not facially offensive or threatening. With respect to common law protection, its misplaced focus allows employers to collect and use their employees' personal data with near immunity. Regarding statutory law, privacy protections serve as ancillary features of laws whose objectives were not, for the most part, about securing and enhancing privacy interests. These ancillary privacy protections were furthered weakened by other provisions that made exceptions to their application. Increased surveillance that violates privacy interests has also made it harder for employees to secure protections in collective bargaining, which is necessary given the at-will employment status of most workers and the collection action issues they would face individually.

Not only would a comprehensive federal privacy law create newer and stronger privacy rights nationwide, but it would empower federal courts to create a privacy conscious jurisprudence. Simultaneously, a federal privacy law would cultivate societal norms around privacy expectations, which in turn can influence state-level case law to develop new uses for existing privacy torts. Additionally, a federal privacy law can allow other federal statutes to be utilized in ways that can supplement privacy protections, such as the NLRA and bargained for protections. Through such a federal privacy bill, dignity and personhood can be protected. After all, "the right of a [person] to the protection of [their] own reputation . . . reflects no more than our basic concept of the essential dignity and worth of every human being--a concept at the root of any decent system of ordered liberty."[104]

104. *Id.*