2019

# Data Mining and the Challenges of Protecting Employee Privacy Under U.S. Law

Pauline Kim
*Washington University in St. Louis School of Law*, kim@wustl.edu

# DATA MINING AND THE CHALLENGES OF PROTECTING EMPLOYEE PRIVACY UNDER U.S. LAW

Pauline T. Kim†

Worker advocates and legal scholars have long been concerned about the impact of employer monitoring and surveillance on employee rights. Tools like RFID badges, GPS tracking devices, and computer monitoring software allow employers to track their employees' movements and activities throughout the day and sometimes during off-work hours as well.[1] As these tools have become more common, concerns have focused on the threats they pose to workers' privacy and autonomy interests. These technologies can be deployed in ways that are excessively intrusive and undermine workers' dignity.[2] Constant surveillance can increase stress, affecting mental and physical health,[3] as well as deterring workers from speaking up about workplace conditions or engaging in other socially valued forms of speech.[4]

Concerns about employee privacy have only intensified with the introduction of data analytic tools in the workplace. While electronic monitoring technologies offer the possibility of continuous surveillance, the application of data mining techniques to employee data raises additional

† Daniel Noyes Kirby Professor of Law, Washington University School of Law, St. Louis, Missouri. Many thanks to Adam Hall and Theanne Liu for research assistance.

1. *See* Michael L. Tushman et al., *Email and Calendar Data Are Helping Firms Understand How Employees Work*, HARV. BUS. REV. (Aug. 28, 2017), https://hbr.org/2017/08/email-and-calendar-data-are-helping-firms-understand-how-employees-work?autocomplete=true (computer monitoring software); *see also* Kaveh Waddell, *Why Bosses Can Track Their Employees 24/7*, ATLANTIC (Jan. 6, 2017), https://www.theatlantic.com/technology/archive/2017/01/employer-gps-tracking/512294/ (GPS tracking of employee smart phones through employer-mandated apps); Ceylan Yeginsu, *If Workers Slack Off, The Wristband Will Know. (And Amazon Has a Patent for It.)*, N.Y. TIMES (Feb. 1, 2018), https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html (RFID devices).

2. *See, e.g.*, Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379, 379-412 (2000) (arguing legal protections from electronic surveillance for workers should derive from the concept of human dignity rather than privacy).

3. *See* Esther Kaplan, *The Spy Who Fired Me: The Human Costs of Workplace Monitoring*, HARPER'S MAGAZINE 31, 31-40 (Mar. 2015); M. J. Smith et al., *Employee Stress and Health Complaints in Jobs With and Without Electronic Performance Monitoring*, 23 APPLIED ERGONOMICS 17, 23-27 (1992) (finding that electronic performance monitoring adversely affected employees' perception of job stressors and levels of physical and psychological strain).

4. *See* Pauline T. Kim, *Electronic Privacy and Employee Speech*, 87 CHI.-KENT L. REV. 901, 901-32 (2012).

challenges. Data mining is simply the process of analyzing large datasets to uncover patterns in the data.[5] These techniques can sometimes reveal surprising relationships between variables, allowing the data processer to make inferences about unknown characteristics of individuals based on available data. In the employment context, employers can now readily access detailed data about workers' online behavior or social media activities, purchase background information from data brokers, and collect additional data from workplace surveillance tools.[6] When data mining techniques are applied to this wealth of data, it is possible to make inferences about worker characteristics and to try to predict future job performance.

Although workforce analytic tools might appear to be merely extensions of previously available monitoring and surveillance techniques, their development raises threats to employee privacy that are different in kind. The inferences drawn from these tools may not always be accurate or may be biased in ways that produce discriminatory employment outcomes, issues that I have explored at length in other work.[7] Here, I focus on a different challenge, namely that data mining tools can alter the meaning and significance of personal information in ways that render traditional employee privacy protections largely ineffective. As many legal scholars have noted, U.S. law offers few limits on employer monitoring and surveillance.[8] Nevertheless, it has provided some protection against the most egregious information gathering practices, often by shielding particularly sensitive information from employer access and scrutiny. The application of data mining techniques to employee data, however, renders these traditional approaches largely ineffective.

---

5. Bart Custers, *Data Dilemmas in the Information Society: Introduction and Overview*, *in* DISCRIMINATION AND PRIVACY IN THE INFORMATION SOCIETY: DATA MINING AND PROFILING IN LARGE DATABASES 3, 9 (Bart Custers, Toon Calders, Bart Schermer & Tal Zarsky eds., 2013).

6. *See* Kaplan, *supra* note 3; Olivia Solon, *Big Brother Isn't Just Watching: Workplace Surveillance Can Track Your Every Move*, GUARDIAN (Nov. 6, 2017), https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology.

7. *See, e.g.*, Pauline T. Kim, *Big Data and Artificial Intelligence: New Challenges for Workplace Equality*, 57 U. LOUISVILLE L. REV. (forthcoming 2019); Pauline T. Kim, *Auditing Algorithms for Discrimination*, 166 U. PA. L. REV. 189, 189-203 (2017), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1212&context=penn_law_review_online (arguing that auditing is an important tool for detecting discriminatory algorithms); Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 857-936 (2017) (exploring the risks of discriminatory algorithms and how employment discrimination law might apply); Pauline T. Kim & Erika Hanson, *People Analytics and the Regulation of Information Under the Fair Credit Reporting Act*, 61 St. Louis U. L.J. 17, 18-19 (2016) (discussing risks of unfairness from inaccurate information or unjustified inferences).

8. *See, e.g.*, Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735, 735-76 (2017) (arguing current laws are insufficient to constrain employer monitoring and tracking of workers); Robert Sprague, *Orwell was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83, 83-135 (2008) (arguing that privacy doctrine and technology have eroded employees' expectations of privacy not only in the workplace but jeopardized employee privacy in the home).

Electronic monitoring tools can amass vastly more information than a human observer, but by themselves, they are simply data collection tools. Data mining, however, allows that same information to be analyzed to infer *additional* information about the data subjects beyond what is directly observed. For example, an employer might examine workers' social media activities on Facebook, which would reveal their social connections and what they "Liked." When analyzed as part of a larger dataset, however, that information can also be used to infer characteristics like sexual orientation or personality traits.[9] Similarly, information obtained through workplace wellness programs can be aggregated and analyzed to uncover additional information—for example, if an individual has certain health conditions or is pregnant.[10] Thus, because data analytic tools can be used to draw inferences, the meaning and significance of any given piece of personal information is not fixed, but can change depending upon what other information it is aggregated with and how the larger dataset is analyzed.

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. This poses a challenge for the law, which often conceptualizes the harm of privacy intrusions in terms of the sensitivity or highly personal nature of information collected or disclosed. This article explores this dilemma by examining three examples of how U.S. legal protection of employee privacy rests on the assumption that privacy entails protecting sensitive or critical information. More specifically, it examines antidiscrimination law's protection of medical and genetic information, the common law privacy tort's protection of embarrassing or humiliating intrusions or disclosures, and the Fair Credit Reporting Act's protection against erroneous data. These strategies rest on the assumption that particular information can be identified as problematic and protected; however, this narrow focus limits the usefulness of these laws in responding to the privacy threats posed by data mining. This article concludes with a brief glance at the differing approach taken by the European Union's General Data Protection Regulation (GDPR),[11] which suggests some steps that may help to overcome the limitations of U.S. employee privacy law.

---

9. Michal Kosinski, David Stillwell & Thore Graepel, *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NATL. ACAD. SCI. U.S.A. 5802, 5805 (2013) (showing that records of an individual's Facebook "likes" can be used to accurately predict personal characteristics such as race, gender, sexual orientation, religious and political views, and intelligence).

10. *See* Jay Hancock, *Workplace Wellness Programs Put Employee Privacy at Risk*, CNN (Oct. 2, 2015, 12:37 PM), http://www.cnn.com/2015/09/28/health/workplace-wellness-privacy-risk-exclusive/; Valentina Zarya, *Employers Are Quietly Using Big Data to Track Employee Pregnancies*, FORTUNE (Feb. 17, 2016), http://fortune.com/2016/02/17/castlight-pregnancy-data/.

11. Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

## I. PROTECTING MEDICAL AND GENETIC INFORMATION—THE ADA AND THE GINA

U.S. law seeks to protect employees from discrimination because of a disability or their genetic traits. In doing so, the law not only forbids employers from taking adverse actions based on those protected characteristics, it also limits employers from acquiring or disclosing medical or genetic information. Although these limits are found in antidiscrimination laws, they act as privacy laws, recognizing certain types of information as warranting special protection and regulating their collection and use.

The Americans with Disabilities Act (ADA) was passed in 1990 "to provide a clear and comprehensive national mandate for the elimination of discrimination against individuals with disabilities,"[12] including in employment.[13] In seeking to achieve that goal, Congress also limited employer access to medical information,[14] recognizing that medical information could reveal the presence of a disability. Because not all disabilities are immediately visible, restricting medical exams and inquiries could prevent discrimination from occurring at all, or isolate when an applicant's disability might have influenced the hiring decision.[15] The disability community had also advocated for restrictions on medical inquiries in order to prevent disclosure of disabilities, such as HIV infection, which can carry a social stigma.[16] Thus, in seeking to prevent discrimination on the basis of disability, the ADA treats medical information as particularly sensitive and restricts the circumstances under which employers can make medical inquiries or require medical exams of applicants or employees.[17]

The ADA does not wholly prohibit employers from accessing employee medical information. Employers may require new hires to undergo a medical exam after they have received an offer of employment.[18] Additionally,

12. 42 U.S.C. § 12101(b)(1) (2012).

13. Title I of the ADA forbids discrimination against qualified individuals on the basis of disability and requires employers to reasonably accommodate the needs of workers with disabilities. § 12112 (prohibition on discrimination); § 12112(b)(5)(A)-(B) (requirement of reasonable accommodation).

14. § 12112(d) (restriction on medical examinations and inquiries).

15. *See* Chai Feldblum, *Medical Examinations and Inquiries Under the Americans with Disabilities Act: A View from the Inside*, 64 TEMP. L. REV. 521, 545 (1991) (arguing that individuals with "hidden disabilities" are "best protected by an absolute bar on pre-offer inquiries or exams" to prevent inappropriate consideration of their medical condition); *see also id.* at 533 (explaining that restricting pre-offer medical inquiries but allowing post-offer examinations may result in applicants with disabilities "to isolate, if and when, their disability unjustifiably influenced a hiring practice").

16. *Id.* at 536, 539.

17. Prior to making an offer, employers are prohibited from requiring applicants to undergo a medical exam and from asking whether the applicant has a disability or about the nature or severity of a disability. § 12112(d)(2)(A). Once an offer has been made, the employer may condition employment on the results of a medical examination, so long as the requirement is imposed on all new hires, not just those with a disability, § 12112(d)(3). Finally, after employment has begun, an employer is not permitted to require medical examinations or to make medical inquiries unless the exam or inquiry is "job-related and consistent with business necessity," § 12112(d)(4)(A).

18. § 12112(d)(3).

employers may learn about an employee's medical condition as part of the interactive process of determining how to reasonably accommodate a worker's disability. When an employer lawfully obtains employee medical information, the ADA imposes restrictions on its storage and subsequent use, requiring employers to treat the information as a "confidential medical record" and to prevent access by supervisors or managers except to the extent necessary to reasonably accommodate a disability.[19] Medical information can reveal highly personal facts and employees may fear embarrassment, harm to their reputation, stigma or shunning if sensitive information is revealed to those with whom they work. Thus, the statute protects employees' privacy interest not just by restricting the collection of medical information, but also by limiting its subsequent disclosure.

The Genetic Information Nondiscrimination Act (GINA), passed in 2008, also seeks to prevent discrimination—in this case, against individuals based on their genetic characteristics.[20] In addition to prohibiting the use of genetic information in hiring, firing and other personnel decisions, it protects the privacy of individuals' genetic information.[21] Employers may not lawfully "request, require, or purchase genetic information with respect to an employee or a family member of the employee."[22] Even if a medical examination is permissible under the ADA, an employer may not seek genetic information as part of that examination.[23] There are a handful of exceptions under which an employer might lawfully acquire genetic information. For example, no violation occurs when genetic testing is part of a program monitoring for the health effects of toxic substances in the workplace or if family medical history—a form of genetic information—is learned from publicly available sources.[24] If such information is lawfully acquired, however, the GINA, like the ADA, requires the employer to treat it

19. § 12112(d)(3)(B)-(B)(i). The statute also provides exceptions for disclosure if emergency treatment is required or in case of a government investigation, § 12112(d)(3)(B)(ii)-(iii).

20. 42 U.S.C. § 2000ff-1(a) (2012).

21. Pauline T. Kim, *Regulating the Use of Genetic Information: Perspectives from the U.S. Experience*, 31 COMP. LAB. L. & POL'Y J. 693, 697-701 (2010); Similar to the ADA's restrictions on medical inquiries and tests, protecting the privacy of genetic information helps to prevent genetic discrimination by employers. *See id.* at 700; Pauline T. Kim, *Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for a Brave New Workplace*, 96 NW. U. L. REV. 1497 (2002).

22. § 2000ff-1(b).

23. There is an exception for "inadvertent" disclosures; however, the receipt of genetic information is not considered inadvertent unless the employer specifically directs the health care provider *not* to provide such information. 29 C.F.R. § 1635.8(b)(1)(i)(A) (2018). Thus, the regulations advise employers to make clear that they do not want genetic information when making otherwise lawful requests for medical information, § 1635.8(b)(1)(i)(B).

24. § 2000ff-1(b). Other examples where no violation occurs include instances when health or genetic services are offered by the employer, including when they are offered as part of a wellness program, and when "the employee provides prior, knowing, voluntary, and written authorization." § 2000ff-1(b)(2)(B).

as "a confidential medical record," and may not disclose it except under a handful of enumerated circumstances.[25]

Under both the ADA and the GINA, privacy protections are limited to certain types of personal information that are deemed sensitive or susceptible to misuse for improper purposes. In the case of the ADA, protection extends to "medical examinations and inquiries," [26] thereby protecting all kinds of medical information—at least to the extent that it is revealed through an examination or direct inquiry. The GINA more narrowly limits its protections to genetic information, which it defines to encompass an individual's genetic tests, the genetic tests of family members and family medical history.[27] A genetic test is "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes."[28] The definition does not include medical information about "a manifested disease, disorder, or pathological condition" if it is not genetic information.[29] In other words, "ordinary," nongenetic medical information is not protected.

While the ADA and the GINA shield employees' medical and genetic information to some extent, both have been criticized as insufficiently protective of employee privacy. Some have argued that the exception in the ADA allowing post-offer medical examinations creates a gap that permits unwarranted intrusions on employees' medical privacy and creates an opening for disability discrimination to occur.[30] Scholars have also criticized the GINA's definition of protected genetic information as too narrow. As discussed above, the statutory definition excludes medical information about manifested diseases or conditions. Where a disease or condition is known to have a genetic basis, that information might indirectly reveal an individual's genetic traits. Similarly, tests that entail analysis of proteins or metabolites are permitted, so long as they "[do] not detect genotypes, mutations, or chromosomal changes,"[31] even though such tests can detect abnormalities known to result from genetic causes. Mark Rothstein and others have argued

25. § 2000ff-5. The statute identifies a handful of permitted disclosures of such information by the employer such as to an occupational or health researcher or in response to a court order. *Id.*

26. 42 U.S.C. § 12112(d) (2012).

27. § 2000ff(4)(A).

28. § 2000ff(7)(A).

29. § 2000ff-9.

30. *See* Sharona Hoffman, *Preplacement Examinations and Job-Relatedness: How to Enhance Privacy and Diminish Discrimination in the Workplace*, 49 KAN. L. REV. 517, 517-92 (2001); Mark A. Rothstein, Jessica Roberts & Tee L. Guidotti, *Limiting Occupational Medical Evaluations under the Americans with Disabilities Act and the Genetic Information Nondiscrimination Act*, 41 AM. J.L. & MED. 523, 540-43 (2015); Mark A. Rothstein, *Genetic Discrimination in Employment and the Americans with Disabilities Act*, 29 HOUS. L. REV. 23, 53-61 (1992). The statute attempts to mitigate the latter risks by requiring that the pre-employment medical exam must be required of all entering employees in a job category in order to prevent the process from becoming a subterfuge for disability discrimination. § 12112(d)(3)(A).

31. § 2000ff(7)(B).

that segregating genetic information from medical information is nearly impossible given that most diseases and medical conditions have some genetic component.[32] As a result, despite the GINA's strong prohibition on acquiring genetic information, employers may be able to learn genetic information indirectly.

This criticism—that the GINA's definition of protected genetic information is too narrow—anticipated the difficulties currently posed by data mining. The critics pointed out the possibility that an employer's access to nongenetic medical information would allow them to infer information about an individual's genetic traits. This possibility of inferring sensitive information has greatly expanded with the growing use of data mining tools in the workplace. Because of the vast amount of personal information available and the power of data analytics, it may now be possible to infer not only genetic risks, but all kinds of medical conditions from nonmedical information such as behavioral and lifestyle data. This problem extends as well to other kinds of information traditionally considered private—such as sexual and financial information—which may be revealed through analysis of large datasets containing information about purchasing habits or online activities. The power of data analytics will make it increasingly difficult to separate "sensitive" from nonsensitive personal information. As a result, the approach taken in the ADA and the GINA—defining certain categories of information as sensitive and protecting them from disclosure—is unlikely to successfully protect the privacy of that information.

## II. "HIGHLY OFFENSIVE" INTRUSIONS—THE COMMON LAW INVASION OF PRIVACY TORT

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.[33] In their view, the right to privacy rested on a principle of "inviolate personality"[34] and redressed dignitary harm by compensating for "mental pain and distress."[35] This "right to privacy" eventually came to be conceptualized as four distinct torts.[36] The two most relevant here—intrusion on seclusion and public disclosure of private facts—both turn on a showing that the defendant's actions were "highly offensive to

32. *See* Mark A. Rothstein, *Genetic Exceptionalism and Legislative Pragmatism*, J.L. MED. & ETHICS 59, 61 (2007); *see also* Rothstein, Roberts, & Guidotti, *supra* note 30, at 542.

33. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193-220 (1890).

34. *Id.* at 205.

35. *Id.* at 196.

36. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

a reasonable person."[37] The "highly offensive" requirement captures the flavor of outrage that motivated the early cases. As William Prosser explained: the "ordinary reasonable man" would not take offense at the disclosure of mundane facts about his life, and therefore, liability should attach only for actions "which the customs and ordinary views of the community will not tolerate."[38] These torts are thus aimed at the most serious social breaches, "those which threaten an individual's identity by withdrawing the deference normally afforded a member of the community."[39] As Robert Post put it, the common law privacy torts afford a remedy when a violation "potentially places the plaintiff outside of the bounds of the shared community."[40]

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. For example, in one case, the plaintiff alleged that her landlord installed a listening device in her apartment and eavesdropped on her for over six months. The court acknowledged that some intrusions are "so indecent and outrageous and calculated to cause such excruciating mental pain . . . that it would be a reproach to the law not to allow redress"[41] and permitted her claim for invasion of privacy to proceed. The privacy tort also imposes liability when a disclosure of private information becomes "a morbid and sensational prying into private lives for its own sake" rather than any legitimate public interest,[42] as when information about an individual's medical condition or sexual relations are publicized.[43]

In the workplace context, successful common law privacy claims have generally involved targeted incidents of employer prying or the disclosure of

37. The intrusion on seclusion tort 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." RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977). Liability under the public disclosure tort arises 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." *Id.* § 652D.

38. Prosser, *supra* note 36, at 397.

39. Pauline T. Kim, *Privacy Rights, Public Policy and the Employment Relationship*, 57 OHIO ST. L.J. 671, 692 (1996).

40. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 968 (1989).

41. Roach v. Harper, 105 S.E.2d 564, 566 (W. Va. 1958); *see also* Souder v. Pendleton Detectives, Inc., 88 So.2d 716, 716-19 (La. Ct. App. 1956) (ongoing shadowing, eavesdropping, and peeping into windows of plaintiffs); LeCrone v. Ohio Bell Tel. Co., 201 N.E.2d 533-41 (Ohio Ct. App. 1963) (extension placed on plaintiff's phone line without her knowledge, allowing her separated husband to eavesdrop).

42. Virgil v. Time, Inc., 527 F.2d 1122, 1129 (9th Cir. 1975).

43. *See* Horne v. Patton, 287 So.2d 824 (Ala. 1973) (physician's disclosure of medical information to employer); Barber v. Time, Inc., 159 S.W.2d 291, 292 (Mo. 1942) (magazine published the plaintiff's name and photograph along with a description of a medical condition for which she was being treated in a hospital); *see also* Michaels v. Internet Entm't Grp., Inc., 5 F.Supp.2d 823 (C.D. Cal. 1998) (dissemination of private sex tape).

particularly sensitive personal information.[44] Courts have permitted intrusion claims when employers conducted unjustified searches or surreptitious surveillance impinging on bodily privacy,[45] or traditionally private spaces such as an employee's home or hotel room,[46] or workplace bathrooms and locker rooms.[47] Employers have also been held liable for investigating employees' sex lives, health problems, or family relationships,[48] and for disclosing medical information about an employee to those with no legitimate interest in knowing.[49] In these cases, the intrusiveness of the searches or the highly sensitive nature of the information disclosed made the employer's actions sufficiently egregious to meet the "highly offensive" requirement.

The application of the common law privacy tort in the workplace is limited, however. Courts find no wrongful intrusion if they conclude that the employee lacked a "reasonable expectation of privacy," and therefore surveillance in semipublic areas like an open workspace or shared office is generally permissible.[50] When the employer has a legitimate business reason for collecting or disclosing the information, intrusions are unlikely to be considered "highly offensive."[51] For example, employers have avoided

---

44. *See* Matthew T. Bodie, Miriam A. Cherry, Marcia L. McCormick & Jintong Tang, *The Law and Policy of People Analytics*, 88 U. COLO. L. REV. 961, 988-92 (2017) (summarizing law regarding employer surveillance and information gathering practices).

45. *See* Catalano v. GWD Mgmt. Corp., No. CV 403-167, 2005 WL 5519861 at *1, *6 (S.D. Ga. Mar. 30, 2005) (strip search).

46. *See* Wal-Mart Stores, Inc. v. Lee, 74 S.W.3d 634, 634-63 (Ark. 2002) (home); Sowards v. Norbar, Inc., 605 N.E.2d 468, 468-75 (Ohio Ct. App. 1992) (hotel room paid for by employer).

47. Acuff v. IBP, Inc., 77 F. Supp.2d 914, 914-36 (C.D. Ill. 1999) (video surveillance of nurse's office where employees were provided medical treatment); Doe v. Dearborn Pub. Sch., No. 06-CV-12369-DT, 2008 WL 896066 at *1 (E.D. Mich. Mar. 31, 2008) (video surveillance of area that gym teachers used to change clothes); Johnson v. Allen, 613 S.E.2d 657, 657-64 (Ga. Ct. App 2005) (video surveillance of restroom); Koeppel v. Speirs, 808 N.W.2d 177, 177-86 (Iowa 2011) (hidden video camera in restroom).

48. Johnson v. K Mart Corp., 723 N.E.2d 1192, 1192-99 (Ill. App. Ct. 2000) (sexual matters, family and health problems); *see also* French v. U.S. ex rel. Dept of Human Health & Human Service, 55 F. Supp.2d 379, 379-84 (W.D.N.C. 1999) (medical information); Van Jelgerhuis v. Mercury Fin. Co., 940 F.Supp. 1344, 1344-70 (S.D. Ind. 1996) (sex lives); Busby v. Truswal Sys. Corp., 551 So.2d 322, 322-29 (Ala. 1989) (sexual propositions and comments about plaintiffs' bodies); Phillips v. Smalley Maint. Servs., Inc., 435 So.2d 705, 705-12 (Ala. 1983) (sex relations with husband); Guccione v. Paley, No. LLICV054002943S, 2006 WL 1828363 at *1, *2-3 (Conn. Super. Ct. June 14, 2006) (religious practices and sex life).

49. *E.g.*, Blackwell v. Harris Chem. N. Am., Inc., 11 F.Supp.2d 1302 (D. Kan. 1998) (medical information); Miller v. Motorola, Inc., 560 N.E.2d 900, 900-04 (Ill. App. Ct. 1990) (medical information).

50. *See, e.g.*, Schmidt v. Devino, 206 F.Supp.2d 301, 309-10 (D. Conn. 2001) (wiretap on office telephone not an intrusion where office door was kept open and secretary just outside could listen); Marrs v. Marriott Corp., 830 F.Supp. 274, 274-84 (D. Md. 1992) (video surveillance of desk in open office permissible); Sacramento Cty. Deputy Sheriffs' Ass'n. v. County of Sacramento, 59 Cal. Rptr. 2d 834, 834-47 (Cal. Ct. App. 1996) (no expectation of privacy in booking area of county jail). *See generally* Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174, 174-84 (1st Cir. 1997) (holding that constant video surveillance of employees in an open work area did not violate the Fourth Amendment because they had no reasonable expectation of privacy).

51. *See, e.g.*, Eddy v. Brown, 715 P.2d 74, 74-78 (Okla. 1986) (no invasion of privacy where information re: psychiatric visits were of legitimate concern to supervisor); Shattuck-Owen v. Snowbird Corp., 16 P.3d 555, 559 (Utah 2000) (holding employer showing video of employee's sexual assault to a dozen people justified as part of investigation).

liability for intrusions that were incidental to work-related investigations or that occurred while trying to secure confidential business information.[52] Similarly, accessing or disclosing medical or mental health information does not trigger liability when the employer has a legitimate interest in doing so.[53] And finally, protection does not extend where the information sought or disclosed is not considered private in nature.[54]

By targeting "highly offensive" forms of information gathering, the common law torts miss the real threats to privacy posed by data mining. Although data mining requires lots of data about workers, the information utilized may not be the type typically considered private or sensitive in nature or may be information in which employers have a legitimate business interest. For example, employers routinely ask for information about applicants' background, education and experience. These materials, as well as publicly available information from social media sites or other online sources, are unlikely to be considered so private that requesting or collecting them constitutes a "highly offensive" intrusion, and yet, when combined with other available data, they can be parsed and analyzed to draw new inferences about workers.

An employer can also harvest metadata about a worker's online activities, beginning with her initial contacts with the firm. A web-based application form might record when an application was completed, how long it took to complete, what browser was used to access the site, etc. Once workers are employed, additional detailed information can be collected about their activities using geolocation devices, computer monitoring tools, smart badges and the like.[55] Each individual datum collected appears quite

52. *See, e.g.*, Sunbelt Rentals, Inc. v. Victor, 43 F.Supp.3d 1026, 1036 (N.D. Cal. 2014) (not highly offensive to review former employee's personal Apple account messages synced to work-issued iPhone during post-employment conduct investigation); Hilderman v. Enea TekSci, Inc., 551 F.Supp.2d 1183, 1204 (S.D. Cal. 2008) (intrusion into former employee's personal matters stored on work computer while trying to protect confidential information was not highly offensive "as a matter of law."); Garrity v. John Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676 at *1, *2 (D. Mass. May 7, 2002) (employer's legitimate interest in investigating possible sexual harassment "would likely trump plaintiffs' privacy interests."); Sitton v. Print Direction, Inc., 718 S.E.2d 532, 537 (Ga. Ct. App. 2011) (reviewing email as part of investigation of improper employee behavior was not an offensive intrusion).

53. *See, e.g.*, Fletcher v. Price Chopper Foods of Trumann, Inc., 220 F.3d 871, 879 (8th Cir. 2000) (holding employer's need to know in order to protect public health trumped an employee's right to privacy of medical information); Davis v. Monsanto Co., 627 F.Supp. 418, 418-23 (S.D.W. Va. 1986) (holding employer had legitimate interest in sharing employee's mental health assessment and that the disclosures were privileged).

54. *See, e.g.*, Rogers v. International Business Machines Corp., 500 F.Supp. 867, 867-70 (W.D. Pa. 1980) (investigation into plaintiff's at-work conduct following complaints not an invasion of privacy); Baker v. Burlington Northern, Inc., 587 P.2d 829, 82-35 (Idaho 1978) (disclosure of employee's criminal history to union and unemployment office is not an invasion of privacy because it is a matter of public record).

55. *See* Bodie et al., *supra* note 43, at 971 (describing badges equipped with microphones, infrared devices, and a motion detector that collects data on employee movements, interactions with coworkers or clients, and even tone of voice); Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 981-82 (2011) (explaining use of GPS, RFID chips, keystroke monitoring, webcam monitoring, and

mundane, even trivial, making it difficult to meet the "highly offensive" element necessary for tort liability. For example, one court found no intrusion upon seclusion where the employer monitored the addresses (but not the contents) of websites visited by an employee.[56] As broad-based monitoring and information gathering practices become normalized, their very ubiquity and ordinariness mean that they are less likely to arouse the concerns about the "outrageous and unjustifiable infliction of mental distress" that initially motivated the privacy torts.[57]

One might argue that it is the *cumulative* effect of all this data aggregation that constitutes an invasion of privacy. The potential for harm does not arise because any particular piece of information collected or disclosed will cause embarrassment or humiliation. Instead, the threat lies in the *uses* to which vast amounts of data can be put, and the possibility that data mining can lay bare aspects of an individual's life or psyche that she neither intended to share, nor understood could be inferred indirectly. This argument resonates with Warren and Brandeis' original theory that the common law recognizes a fundamental principle of "an inviolate personality,"[58] yet, it is not without difficulty. As a practical matter, the common law right to privacy, as interpreted by courts in the United States since Warren and Brandeis wrote, has focused on particular invasions or disclosures—those where the manner of intrusion or the highly sensitive type of information involved rendered them "highly offensive." Wholly absent from the case law is the suggestion that using data to draw inferences about individuals implicates their privacy interests. Even if the common law doctrine were to expand in this way, conceptual challenges would remain. It would not be practicable to prohibit the drawing of any inferences from data, nor would it be easy to define unacceptable or unlawful uses of data. Whenever someone acts on information, they are implicitly making inferences based on that data. For example, even when an employer relies on traditional hiring criteria like work experience or education, it is using the information to extrapolate information about the individual's skills and abilities.

The common law torts are simply not geared toward addressing the privacy risks posed by data mining techniques. By focusing on highly offensive intrusions or the collection of sensitive information, the doctrine

email scanning in the workplace); Kaplan, *supra* note 3; Don Peck, *They're Watching You at Work*, ATLANTIC (Dec. 2013), http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/.

56. Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746, at *22 (D. Or. Sept. 15, 2004); *cf.* Schibursky v. International Business Machines Corp., 820 F.Supp. 1169, 1183 (D. Minn. 1993) (finding employer surveillance of plaintiff's computer logins to audit her hours worked was not "utterly intolerable" and rejecting intentional infliction of emotional distress claim).

57. *See* Prosser, *supra* note 36, at 384.

58. Warren & Brandeis, *supra* note 33, at 205; *see also id.* at 211 (citing "the right to an inviolate personality").

does not address how data mining can threaten privacy by inferring highly personal information rather than collecting it directly. Because the data gathering and analytic process is routine, bureaucratic, and not highly visible, it is unlikely to arouse concerns about "public indignity" or "humiliation" that originally motivated the privacy torts. Thus, while the common law torts provide an important backstop by protecting against egregious, visible intrusions, they offer little protection against the privacy threats that arise when routinized data collection is combined with data mining technologies in the workplace.

## III. PROCEDURAL PROTECTIONS—THE FAIR CREDIT REPORTING ACT

Although not primarily focused on the employment relationship, the Fair Credit Reporting Act (FCRA)[59] also protects employee privacy by placing restrictions on employers' information gathering practices. Recognizing that credit reports were playing an increasingly important role in economic life, Congress passed the FCRA in 1970 "to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[60] The FCRA tries to achieve these objectives by regulating how consumer data is handled when it is used to make credit, insurance and employment decisions.[61]

When consumer reports are used for employment purposes, both the employer and the consumer reporting agency must follow procedures specified in the statute. The employer is required to give clear notice and obtain written authorization from the applicant or employee before accessing a consumer report.[62] If it intends to take an adverse action based on the report, it must provide separate notice before doing so, including a copy of the consumer report and information about the consumers' rights under the statute.[63] The credit reporting agencies that sell these reports must also meet certain requirements, such as permitting consumers to review information in their files without charge and investigating alleged inaccuracies.[64] Thus, the basic provisions of the FCRA emphasize procedural protections—requiring

59. 15 U.S.C. § 1681 (2012).

60. § 1681(a)(4).

61. § 1681b limits consumer reporting agencies to providing reports only for a list of specified purposes. These include circumstances in which the person seeking the report "intends to use the information for employment purposes." § 1681b(a)(3)(B).

62. § 1681b(b)(2). The disclosure must be "clear and conspicuous" and "in a document that consists solely of the disclosure." 1681b(b)(2)(A)(i). The employer must also certify to the consumer reporting agency its compliance with the requirements of the statute before receiving any consumer report. 1681b(b)(1).

63. § 1681b(b)(3)(A). After taking an adverse action, the employer must provide additional information pursuant to § 1681m(a).

64. § 1681g (requiring disclosure of the information in a consumer file to the consumer upon request); § 1681i (requiring consumer reporting agencies to reinvestigate disputed information).

notice and consent before using personal information to make employment decisions, and providing data subjects with the opportunity to review their records and to challenge any erroneous information.

These types of procedural protections are unlikely to be effective in addressing the privacy concerns raised by data mining. First, the FCRA has had little practical impact in restricting employers' access to workers' personal information. Workers generally give consent in order to be considered for or to keep a job, and thus, employers can freely access consumer reports, so long as they follow all the procedural requirements.[65] And the statute does not apply at all if employers receive information from entities falling outside the definition of a "consumer reporting agency,"[66] or gather data directly from their employees on the job. Apart from a handful of narrow restrictions prohibiting obsolete information in a consumer report,[67] the FCRA does not meaningfully limit collection of workers' personal information.

A second limitation is that the FCRA assumes that the risk of harm lies in discrete pieces of information about the worker, rather than the total body of data that can be amassed and the inferences that can be drawn from mining that data. By requiring employers to give notice of an adverse employment action, workers are alerted when something in a consumer report has been the basis for their rejection. The worker then has the right to contest the accuracy of the record, prompting the reporting agency to reinvestigate and, if warranted, correct the record.[68] These rights can be quite helpful when an individual has been stigmatized by a particular piece of erroneous information, such as a false report of a bankruptcy or criminal record.

---

65. As Lea Shepard explains, when passing the FCRA, Congress left intact the common employer practices of accessing credit reports and addressed only "the procedures governing the industry." Lea Shepard, *Toward a Stronger Financial History Antidiscrimination Norm*, 53 B.C.L. REV. 1695, 1749 (2012).

66. The FCRA defines "consumer reporting agency" as

> [A]ny person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

§ 1681a(f). Thus, whether an entity is a consumer reporting agency turns on whether it furnishes "consumer reports to third parties." The FCRA defines a "consumer report" as

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for . . . employment purposes.

§ 1681a(d)(1). There is currently uncertainty regarding how this definition applies to companies that use datamining software to assess workers for employers.

67. § 1681c(a) (prohibiting consumer reports from containing information such as bankruptcy cases over ten years old or civil suits, civil judgments, and arrest records over seven years old).

68. § 1681i(a)(1).

However, where the worker is harmed because of inferences or predictions made based on a data profile, the FCRA offers no way to challenge the conclusions drawn through the data mining process.

More generally, the FCRA is unconcerned with how employers use data that they receive from a consumer reporting agency, so long as they follow all of the procedural requirements by providing the required notices at the proper time and in the proper format.[69] In one case, an employee was fired because of a false consumer report that he had a felony cocaine conviction, but he was unsuccessful in challenging his employer's decision to discharge him.[70] In rejecting his FCRA claim, the court held that employers "are under no duty to reinvestigate the facts provided in a consumer report."[71] Thus, the FCRA does not prohibit employers from relying on inaccurate information, and similarly, it leaves them free to use accurate information in any way they see fit. As a result, the statute's procedural requirements will do nothing to restrict or regulate employers when they use data mining techniques to uncover new information about individual workers, through inference or prediction.

## IV. CONCLUSION

As seen from the examples discussed in this article, employee privacy protections in U.S. law generally focus on shielding discrete types of information or aspects of personal life. This approach is ill-suited to address current privacy threats in a world in which employers can amass large amounts of personal data and use sophisticated data mining tools to analyze it. These tools allow employers to draw inferences or make predictions that go far beyond the individual pieces of data collected and may reveal highly sensitive information that the worker has not consented to disclose or produce mistaken judgments that result in lost opportunities. The traditional model, which focuses on protecting certain sensitive types of information or allowing data subjects to challenge errors in their records, will do little to protect against these potential harms.

Although U.S. privacy law is often criticized for its narrow sectoral approach, even omnibus data protection regimes, such as the European Union's, struggle to provide robust protections in the current data-rich business environment. The GDPR, newly effective last year, strengthens data

69. The statute does require that an employer requesting a consumer report must certify to the reporting agency that the information "will not be used in violation of any applicable Federal or State equal employment opportunity law or regulation." § 1681b(b)(1)(A)(ii). This provision refers to existing antidiscrimination laws, but the FCRA does not appear to impose an independent duty of nondiscrimination, nor does it provide any mechanism for enforcing the employer's obligation to abide by equal employment laws when using workers' consumer records, and there appears to be little or no litigation enforcing this provision.

70. Wiggins v. District Cablevision, Inc., 853. F.Supp. 484, 484-500 (D.D.C. 1994).

71. *Id.* at 492.

privacy protections in the EU in many ways, and yet, it too has been criticized as inadequate. The same technological developments that have outpaced U.S. law are also challenging the fundamental principles underlying the EU's legal frame for data protection.[72] While the extent to which the GDPR will meaningfully increase transparency and accountability of automated decision systems is currently strongly debated,[73] the Regulation nevertheless takes important steps which are essential if the law is to address threats to privacy and fairness posed by data mining techniques in the workplace. Specifically, the GDPR explicitly recognizes the significance of profiling—the automated processing of personal data—which encompasses data mining (Art. 4). In addition, it gives the data subject certain rights relating to profiling, such as the right to "meaningful information about the logic involved" in these systems (Art. 13(2)(f), Art. 14(2)(g), and Art. 15(1)(h) and a right to object to profiling (Art. 21). It remains to be seen how these provisions in the GDPR will be implemented and what impact they will have; nevertheless, this legal recognition of the significance of profiling, distinct from the mere collection and disclosure of information, is a crucial step that U.S. law will need to take if it is to address current threats to employee privacy.

72. Bart Custers & Helena Ursic, *Worker Privacy in a Digitalized World Under European Law*, 39 COMP. LAB. L. & POL'Y J. 323, 326 (2018) (arguing that the increased use of data and technologies "challenge some key data protection principles").

73. *See, e.g.*, Bryan Casey, Ashkon Farhangi & Roland Vogl, *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Dabate and the Rise of Algorithmic Audits in Enterprise*, BERKELEY TECH. L.J. (forthcoming), available at https://ssrn.com/abstract=3143325; Bryce Goodman & Seth Flaxman, *European Union Regulations on Algorithmic Decision-making and a 'Right to Explanation'*, 38 AI MAGAZINE 50, 50-57 (2017); Andrew D. Selbst & Julia Powles, *Meaningful information and the right to explanation*, 7 INT'L DATA PRIVACY L. 233, 233-42 (2017); Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIVACY L. 76, 76-99 (2017).