Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy

Kim, Pauline T [1] ; Bodie, Matthew T [2] [1] Washington University School of Law, St. Louis, Missouri [2] Wefel Center for Employment Law, Saint Louis University School of Law

ABSTRACT (ENGLISH)

AI systems have the ability to generate insights that are not accessible based on ordinary human observation, and the more complex systems may generate results that are not fully explainable or understandable, even by their human creators.4 Early efforts at artificial intelligence endeavored to make machines into the equivalent of humans, with the ability to exercise judgment in a variety of contexts.5 These efforts to create a "general" AI have largely failed.6 However, there have been great successes in narrow AI-namely, the application of artificial intelligence to a particular problem or context.7 Familiar examples of AI breakthroughs include programs that play games such as chess and Go; speech-recognition programs that translate speech to text; and spam filters for email accounts.8 Increasingly, AI systems are being used in social domains as well-for example, to make decisions regarding policing, bail, credit, and employment.9 As these AI tools are deployed in arenas with significant human and societal impacts, concerns have been raised about the fairness, accountability, and transparency of these systems.10 Fairness centers on the risk of "discriminatory or unjust impacts when comparing across different demographics or affected communities and individuals. [...]the introduction of AI may bring employees into a vortex of massive information collection, data vulnerability, and seemingly whimsical decision-making. Employees report a feeling of powerlessness when AI is given significant power over their jobs, as they lose the ability to interact with their "supervisor" in a meaningful way.22 The voracious maw of data collection paired with the inexplicability of decisions made can create the feeling that the employee is trapped in a matrix of computer-controlled reality from which there is no escape.23 In the next two sections we explain these concerns and examine the extent to which existing law addresses them. [...]certain patterns of consumption could be correlated with health conditions, causing an algorithm to implicitly discriminate against individuals with disabilities, even if the employer neither knows nor intends to screen on that basis.30 AI can also produce biased results if it is trained using biased data.31 An algorithm trained using the subjective evaluations of a biased supervisor will make systematically biased predictions of future job performance.

FULL TEXT

Introduction

The term artificial intelligence (AI) was coined in the 1950s, but the concept has piqued humanitys interest both before and since.1 Initially relegated to science fiction and futuristic fantasies, recent technological leaps have made AI commonplace. We rely on these systems every day when we check the weather, read the news, navigate voice mail, or get directions. These systems also increasingly guide or replace human decision-making in important domains like medical care, criminal law enforcement, finance, and employment. These developments raise a number of societal challenges, and numerous scholars have begun to tackle concerns over the appropriate role of algorithmic decision-making in our society.2

In the workplace setting, employers are increasingly relying on artificially intelligent systems to recruit, select, and manage their workforces. These developments have raised fears that these systems may subject workers to discriminatory, invasive, or otherwise unfair treatment. In this article, we review those concerns and provide an overview of how current laws may apply, focusing on two particular problems: discrimination on the basis of

protected characteristics like race, sex, or disability, and the invasion of workers' privacy engendered by workplace AI systems. Part I provides a brief background on the nature of AI and its growing role in the workplace. Part II discusses the ways in which relying on AI to make personnel decisions can produce discriminatory outcomes and how current law might apply. Part III explores how these data-driven systems may threaten workers' interests in privacy and autonomy, and considers the extent to which existing legal frameworks address these concerns. It also describes the European Union's much more restrictive regime as a useful comparator. This article argues that the growing use of AI at work raises significant policy concerns about discrimination, privacy, and autonomy that are not adequately addressed by current law.

I.AI and the Workplace

The term artificial intelligence is difficult to define crisply and is often used interchangeably with other terms such as machine learning, algorithmic decision-making, and automated decision-making.3 Although these terms have somewhat different technical meanings, in this article we use the term AI loosely to refer to systems that leverage data-rich inputs and computational techniques to make predictions that either aid or replace human decision-making. These tools are built by analyzing large amounts of data to extract patterns and then using those patterns to predict outcomes in new cases or situations. Some forms of AI use machine learning techniques, which allow a program to learn from incoming data over time without humans actively structuring the process. AI systems have the ability to generate insights that are not accessible based on ordinary human observation, and the more complex systems may generate results that are not fully explainable or understandable, even by their human creators.4

Early efforts at artificial intelligence endeavored to make machines into the equivalent of humans, with the ability to exercise judgment in a variety of contexts.5 These efforts to create a "general" AI have largely failed.6 However, there have been great successes in narrow AI-namely, the application of artificial intelligence to a particular problem or context.7 Familiar examples of AI breakthroughs include programs that play games such as chess and Go; speech-recognition programs that translate speech to text; and spam filters for email accounts.8 Increasingly, AI systems are being used in social domains as well-for example, to make decisions regarding policing, bail, credit, and employment.9 As these AI tools are deployed in arenas with significant human and societal impacts, concerns have been raised about the fairness, accountability, and transparency of these systems.10 Fairness centers on the risk of "discriminatory or unjust impacts when comparing across different demographics or affected communities and individuals."11 Accountability refers to the need to take responsibility for the use of AI and the effects of that use, including the need to mitigate negative impacts on society.12 Transparency concerns relate to failures to disclose when AI is used to make decisions and to explain how it reaches those decisions.13

The use of AI in the workplace raises specific apprehensions. Much recent attention has focused on whether workers will be replaced by AI or other new forms of technology, such as automation and robotics.14 Worry about technology replacing human labor is not new, but there is a lively ongoing debate about whether advances in AI will cause disruptions on a greater scale than in the past.15 Although this question is clearly important, this article focuses instead on the policy concerns that arise when employers use AI tools to manage workers, rather than replace them.

Employers have adopted artificial intelligence systems to assist in a variety of personnel and management functions.16 AI tools are used to screen employment applicants and evaluate potential candidates for positions.17 Employers have also used AI to determine which employees might be more likely to leave the company. Data analytics have found correlations between a higher risk of flight and such factors as time interacting with colleagues, meeting attendance, and waiver of benefits coverage.18 Employers can then use these predictions to make a stronger effort at retention or to steer likely-to-depart employees away from sensitive projects. Across the board, employers are using AI to help manage their workforce-in some cases, even doing the work of management.19 This includes turning to AI applications in response to the COVID-19 pandemic. For example, security cameras outfitted with AI scanners have monitored employees for mask use and social distancing.20

Objections to the use of AI within the employment relationship have largely fallen into two categories. First, there has been significant concern that the AI may reflect, reinforce, or worsen discriminatory biases when making

employment decisions. Algorithms can produce predictions that systematically disadvantage workers along the lines of race, sex, or other protected characteristics.21 The risk is that these discriminatory outcomes will be overlooked or ignored because of the mistaken belief that AI processes are "objective" and "neutral." Second, the introduction of AI may bring employees into a vortex of massive information collection, data vulnerability, and seemingly whimsical decision-making. Employees report a feeling of powerlessness when AI is given significant power over their jobs, as they lose the ability to interact with their "supervisor" in a meaningful way.22 The voracious maw of data collection paired with the inexplicability of decisions made can create the feeling that the employee is trapped in a matrix of computer-controlled reality from which there is no escape.23 In the next two sections we explain these concerns and examine the extent to which existing law addresses them.

II.AI and Employment Discrimination

When an employer uses AI tools to make or to aid decisions about recruitment, hiring, and promotion, they can have a significant impact on access to employment opportunities. The promise of these technologies is that they will make these HR processes fairer and less discriminatory.24 Human decision-makers often harbor explicit or implicit biases, which can unfairly disadvantage racial minorities, women, and other disadvantaged groups,25 and technology might help to avoid those human biases.

Despite their aura of neutrality and objectivity, however, AI tools can also reproduce human biases or introduce new forms of bias, depending upon how such tools are built and trained. Studies have documented a number of examples of algorithmic bias. For example, Internet searches for black-identified names are more likely to be accompanied by ads suggesting an arrest record (e.g., "Latanya Sweeney, arrested?"),26 than searches for white-identified names, even when no arrest record exists.27 In another well-known example, Amazon tried to create an algorithm to screen potential candidates for software developer jobs, but abandoned the effort after finding that it systematically downgraded qualified female applicants.28

Importantly, these types of discriminatory outcomes cannot be prevented simply by removing protected attributes like race or gender from the algorithms.29 When AI tools are built using data-rich profiles, they can end up relying on proxies for a protected characteristic. For example, because place of residence is closely correlated with race in many cities, an algorithm that sorts candidates based on zip code could disadvantage racial minorities. This might occur intentionally when a proxy is used to screen out a disfavored group, but the effect could be unintentional as well because attributes can be correlated with protected characteristics in unexpected ways. For example, certain patterns of consumption could be correlated with health conditions, causing an algorithm to implicitly discriminate against individuals with disabilities, even if the employer neither knows nor intends to screen on that basis.30

AI can also produce biased results if it is trained using biased data.31 An algorithm trained using the subjective evaluations of a biased supervisor will make systematically biased predictions of future job performance. Similarly, a hiring algorithm that selects candidates by comparing them with an employer's current employees may discriminate if the employer's past practices excluded certain groups. If, for example, the employer has very few women working as computer programmers, the algorithm will likely reproduce that pattern when trying to predict the most promising hires. Similarly, an algorithm that tried to maximize "cultural fit" by recommending applicants who are similar to current employees could operate to exclude racial or ethnic minorities.32

Other data problems can also produce biased outcomes. If the data used to train the AI is less complete or less accurate for some groups, the algorithm will be less accurate in identifying the most promising candidates from that group or may systematically underestimate their likelihood of success. Similarly, if the training data are unrepresentative of the population to which that the algorithm will be applied, it could systematically disadvantage protected groups, even if neither the creator of the algorithm nor the employer using it intends to discriminate.

The risks of biased AI can even affect the diversity of the applicant pool before the employer has a chance to evaluate job candidates.33 Today, employers rely heavily on online platforms to advertise job openings and recruit strong applicants. Those platforms, however, do not simply disseminate job postings widely.34 Instead, they rely on AI to predict who is most likely to respond to a particular opportunity, and those predictions will often reflect past patterns of occupational seg- regation.35 Studies have documented that ads delivered on Facebook for

stereotypically male jobs (e.g., lumberjack, AI researcher, truck driver) are overwhelmingly targeted at male users, even though the advertising was intended to reach a gender-balanced audience.36 Other types of ads were served to race- or age-biased audiences-again, in ways that appear to reflect stereotypes about the kinds of people who fill those jobs.37

These risks of discriminatory effects arise because AI learns to make predictions by analyzing data about past patterns of behavior. In the employment sphere, those patterns may reflect prior discrimination, as, for example, when women are paid less to do the same job38 or are discouraged from pursuing certain occupations by on-thejob harassment. The American labor market has long been characterized by patterns of occupational segregation along race and gender lines.39 As a result, relying on the past to make predictions about the future runs the risk of reproducing past discrimination if care is not taken when building AI tools.40 To avoid inadvertently encoding past biases, the designers who build AI systems and the employers who use them may want to take actions to counter discriminatory effects that might otherwise occur. For example, it will often be important to audit algorithmic systems for unintended discriminatory effects and make adjustments, if necessary, to avoid unfairness.41

Given the risks of discriminatory outcomes, the growing use of AI tools in the workplace raises a number of legal questions. Federal laws prohibit discrimination on the basis of race, color, and other protected characteristics.42 These laws are relevant when algorithms are used to make employment decisions, and in some circumstances their application is clear. In other cases, however, it may be quite uncertain how existing laws apply to AI tools.

Consider first employers that use online platforms to advertise job openings. Title VII, in addition to prohibiting discrimination, also makes it unlawful for employers to publish advertisements that "indicate a preference, limitation, specification or discrimination" based on a forbidden characteristic.43 A similar provision in the Age Discrimination in Employment Act (ADEA) prohibits ads indicating a preference based on age.44 These provisions would likely apply if an employer deliberately tried to target its ads using attributes that either directly or by proxy excluded members of a protected group.45

However, as discussed above, even neutrally targeted job postings can be delivered in biased ways because of the operation of algorithms deployed by online platforms. If an employer intends to reach a broad audience, but the platform's algorithm distributes the opportunity in a biased way, is the platform responsible? Title VII's prohibitions apply to employment agencies in addition to employers and labor organizations, but few cases have interpreted that provision. If a tech platform actively intervenes to suggest or promote certain candidates or opportunities, or to facilitate certain matches, we argue that it should be treated as an "employment agency" under Title VII.46 Other platforms may not have enough direct control over access to employment opportunities to be covered by the statute.

What about hiring algorithms that sort or score job applicants? Does an algorithm that systematically disadvantages members of a protected group violate the law? Title VII encompasses two wellrecognized theories of discrimination: disparate treatment and disparate impact. Disparate treatment theory forbids adverse decisions taken "because of" race, sex, or any other protected class.47 If an employer is using a biased algorithm because it wants to screen out members of a protected group, that is clearly a form of intentional discrimination prohibited under disparate treatment theory. Proving the employer's intent may be difficult, but that type of discrimination fits quite well conceptually with the disparate treatment theory.

Disparate impact cases involve facially neutral employment practices that have discriminatory effects.48 Under current Title VII doctrine, disparate impact cases proceed through several steps.49 First, the plaintiff must identify an employer practice that has a disparate impact on a protected group.50 Then, the employer can defend the practice by showing that it is "job related" and "consistent with business necessity."51 If the employer succeeds in this defense, the plaintiff can still prevail by showing that a less discriminatory alternative exists and that the employer failed to adopt it.52

When AI selection tools disproportionately screen out women or racial minorities from an applicant pool, disparate impact theory would seem to apply. This means employers should closely monitor how AI tools operate in practice and should not use them, or should discontinue using them, if they have a disparate impact unless they are clearly job-related and consistent with business necessity. Applying these standards, however, raises a number of

questions. In the past, employers defending selection procedures by validating that they actually measured job-relevant skills or attributes.53 AI tools, however, often rely on unexplained correlations with observable attributes to make predictions about an individual's future behavior or job performance. The variable relied on by the algorithm may have no intuitive connection with performance, and, in some cases, the relationship may be purely correlational and obviously lack any causal connection to the relevant skills or abilities. As examples, it was documented in one dataset that computer programmers who frequented a particular Japanese manga site had superior coding skills, while another study found that users in the United Kingdom who "like" curly fries on Facebook had higher intelligence.54 Some types of AI use machine learning techniques where the AI tools "learn" by extracting patterns from the data, rather than the programmer deciding what factors are relevant and what weights to give them. The resulting algorithms are often exceedingly complex and completely opaque, such that it is difficult for humans to interpret. As a consequence, employers that rely on these types of algorithms may not be able to clearly articulate or explain the reasons for their personnel decisions. Applying existing employment discrimination law to AI tools will require addressing these challenges.

When Congress codified the disparate impact doctrine in in section 703(k) of Title VII, it retained the language in section 703(a)(2), which makes it an unlawful employment practice for an employer "to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive" them of opportunities because of one of the listed protected characteristics.55 This statutory language arguably continues to have independent force and could serve as a basis for scrutinizing AI systems that sort or screen-i.e., "classify"-employees or applicants in biased ways, and for ensuring that disparate impact theory meets the novel challenges that they pose.56

For discrimination law to remain effective, it must recognize the specific ways in which biased AI can unfairly discriminate.57 For example, the mere existence of a statistical correlation should not be sufficient to justify a model with discriminatory effects. In other words, an unexplained correlation should not satisfy the requirement that an employer show that a practice is "job related."58 In addition, when an algorithm systematically disadvantages protected groups, the employer should bear the burden of demonstrating that the model is statistically valid and substantively meaningful, as opposed to merely "job related." The employer, or the vendor who created the algorithm, should have to demonstrate that it avoids common sources of statistical bias-for example, by showing that it was built using data that is accurate, unbiased, and representative. In addition, the employer should have to provide some explanation of the decision process and explain its relevance to the job-something more than a mere statistical relationship. Only then can we bring to bear societal values and judgments to determine whether an algorithm's use is justified despite its effects.

Under the Americans with Disabilities Act (ADA), employers are prohibited from using tests or selection criteria "that screen out or tend to screen out" individuals with disabilities unless the test or criterion is job-related and consistent with business necessity.59 The statute also forbids the use of tests that work as obstacles to applicants or employees with sensory, manual, or speaking impairments, such that they "reflect the impaired sensory, manual, or speaking skills," rather than the actual skills or aptitude necessary to perform the job.60 In other words, employers must be careful when adopting AI screening tools, especially ones that collect data about applicants through interactive online tests or games, that the tools are not preventing or disadvantaging applicants with disabilities that may make it more difficult for them to interact online. If that is the case, employers may need to make reasonable accommodations for those applicants.

Employers who make use of AI tools in their HR processes should be aware of the potential risks of bias and take proactive steps to avoid them. Doing so requires careful scrutiny of the manner in which these tools are designed and built, and how they will be deployed in a particular workplace. A number of checklists or principles now offer guidance to employers on avoiding bias when using AI tools. For example, the Leadership Conference on Civil and Human Rights has promulgated Principles for Hiring Assessment Technologies.61 In addition, because algorithms that appear to be unbiased under testing conditions may behave differently "in the wild," employers should engage in regular auditing of the performance of these tools once they have been implemented.62 If a screening or hiring

tool has an unexpected disparate impact on disadvantaged groups, it should be scrutinized and adjusted to avoid any unfairness.

Such an approach is consistent with the Supreme Court's repeated admonition that voluntary compliance by employers is "the preferred means of achieving the objectives of Title VII."63 Although a few commenters have suggested that the Court's decision in Ricci v. DeStefano64 somehow bars employers from revising algorithmic processes after the fact to correct for discrimination,65 this belief stems from a misreading of Ricci.66 The Supreme Court in that case disapproved of a city's decision to discard the results of a promotion exam when it turned out to have a racially disparate impact. Numerous firefighters had expended significant time and resources studying for the exam, and its decision to discard the results adversely affected them because they had relied on the city's announced plan to use it for promotions.67 In contrast, the Court made clear that Title VII does not prohibit an employer from prospectively designing its employment practices "in order to provide a fair opportunity for all individuals, regardless of their race."68 Thus, it is clearly lawful for an employer to implement a new testing protocol or selection procedure in the future to create a more fair process.69

III.AI and Employee Privacy and Autonomy

In addition to assisting with traditional HR functions, AI tools are also increasingly integrated into work tasks. These tools can offer enormous benefits by helping workers perform their jobs more productively.70 At the same time, widespread integration of AI into the workplace typically entails the collection and analysis of large amounts of data, much of it harvested from employees. This massive data collection in turn creates new power that employers can use to manage and control workers.71 As a result, the increasing use of AI at the workplace raises concerns about privacy and autonomy. AI threatens employee privacy by requiring the collection and processing of huge amounts of employee data. And when AI systems make decisions with important employment ramifications in the absence of transparency or accountability, workers can be left feeling powerless and alienated. Although these issues are not new, the growing use of AI tools vastly expands the challenges they pose, and, to this point, the law provides very few mechanisms for directly addressing them.

A. Collection and Use of Employee Data

Data obtained through employee surveillance fuels AI.72 The development of artificial intelligence builds on systems that cull and process massive amounts of data. AI tools require these large datasets in order to learn patterns that allow them to make artificially intelligent decisions. For example, natural language processing systems require exposure to enormous samples of human communications to analyze and learn to imitate those communications.73 As AI is increasingly incorporated into the workplace, it must rely on data produced by humans-employees-for the raw material needed to build tools that will be useful in that setting. At the same time, new technologies have made monitoring employees and collecting data from them much more inexpensive, unobtrusive, and comprehensive. Employers can track employee movements,74 follow their activities on the web,75 and even monitor employees' heart rate and blood pressure76 with everyday technology integrated with ordinary consumer devices.77 Artificial intelligence can then crunch this data in a variety of ways, producing insights that are unique or unexpected. Below we discuss the ways in which the United States and the European Union regulate workplace data collection and processing.

1. Employee Privacy Protections Under Current U.S. Law Commentators have bemoaned the relatively weak constraints that U.S. law places on employer collection and use of workers' data.78 A patchwork of variegated protections creates only a loose set of restrictions.79 In this part we briefly survey existing legal regulations that touch on employee privacy concerns.

General Protections for Employee Privacy. Only a handful of sources of law offer broad privacy rights, and they provide quite limited protections to employees. The Fourth Amendment of the U.S. Constitution protects public-sector employees against unreasonable searches and seizures,80 but these federal rights only constrain government employers.81 In addition, because the methods of massive data collection often do not involve a search or seizure, it is unclear the extent to which constitutional provisions apply in this context.82

The privacy tort of intrusion upon seclusion83 also provides a type of generalized privacy protection, and it is

recognized by courts in over forty states.84 The intrusion tort has provided redress from a variety of privacy invasions by employers, such as spying on an employee who filed a workers' compensation claim;85 deploying informants to collect private information about fellow workers;86 searching a locker and personal belongings without consent;87 and installing cameras in bathrooms or private offices.88 To be actionable, the employer's conduct must be intentional, must intrude upon the employee's reasonable expectation of privacy, and must be considered "highly offensive to the reasonable person."89

Although the intrusion tort has successfully protected workers against egregious employer practices in the past, it is less likely to be effective in protecting employee privacy when large amounts of data are scooped up to feed AI systems.90 The type of data collected is often not the kind of information that is considered private or sensitive in nature, such that its collection would be considered highly offensive. Instead, it is often relatively mundane bits of data that employees produce as they go about their work or daily lives that get its invasive power only when aggregated with other data. In addition, employers will often be able to argue that this data is the type of information that businesses routinely collect, and courts have been fairly deferential when the employer asserts a business interest justifying the intrusion.91 If the data collection and use ultimately improve the employees' performance or the employer's underlying business, the employer's actions are likely to be adjudged prudent rather than nefarious. The intrusion tort is also unlikely to provide employees with much protection because most employees are employed at will, such that their continued employment can be conditioned on consent to data collection and use. Employee consent will not always defeat claims of privacy intrusion,92 but consent is generally regarded as a defense to intentional tort claims.93 Even if consent does not waive the employees' rights completely, it still undercuts the "highly offensive" aspect of the claim, as the employee agreed to the intrusion. The expanding ubiquity of employer monitoring also erodes the privacy expectation of employees, making it less likely to be considered an intrusion in the first place.94

In terms of worker surveillance, the employer is generally allowed to monitor its employees.95 Even continual electronic observation is permitted in many areas of the workplace.96 The states of California, Connecticut, and Delaware require employers to give notice when they engage in electronic monitoring.97 And, as discussed above, surveillance in traditionally private places like bathrooms or employees' homes can give rise to tort liability. The National Labor Relations Act prohibits employer surveillance that would chill or otherwise interfere with its employees' protected concerted activity.98 However, apart from these laws, employers are generally unrestricted in their ability to monitor or surveil their employees, including using electronic tools to collect data about their activities. The common law has determined that surveillance can be tortious when conducted at personal locations away from work when done without the employee's consent.99 However, observation of an employee in public is permitted.100 Federal law forbids an employer from intercepting an employee's telephone or other electronic communications, even from the employer's phone, without specific consent.101 Surveillance can be legally problematic under the common law if undisclosed, but secrecy is generally permissible when employed for significant and legitimate business reasons, such as to catch a thief.102 Once again, data collection is generally permitted if disclosed to employees, and they consent.

Protections for Specific Types of Data. Beyond these general vacy are variegated statutory and regulatory provisions that protect specific types of data. However, because these provisions focus on particular kinds of information that are deemed sensitive in some way, they provide only very patchy protections against comprehensive data collection.

No law broadly regulates the privacy of employees' health information, although the ADA limits employers' ability to conduct medical exams or make medical inquiries, and the Genetic Information Nondisclosure Act (GINA) prohibits employers from requesting or acquiring employees' genetic information.103 Although many assume that the federal Health Information Portability and Accountability Act (HIPAA)104 protects employee medical information, HIPAA only applies to health plans, health care providers, and health care clearinghouses.105 Employers are not covered entities unless they fall into one of these categories.106 And, even if they are covered, employers need not comply with HIPAA when it comes to records held in their role as employer.107 If the information does fall under HIPAA,

patient authorization generally provides permission to collect and use the protected health information.108
Illinois provides a private right of action for improper collection, retention, or use of biometric data such as fingerprints or facial scans in the Biometric Information Privacy Act (BIPA).109 Although the BIPA allows employers to collect biometric information with employee consent, the statutory scheme also provides a number of protections and limitations on the use of the data. Employers have been sued for failing to notify employees about the purpose and length of the data's use; neglecting to establish a timeline for destruction of the data; and failing to obtain employee consent for disclosure or dissemination of the biometric data to a third party.110 Other states have also begun to enact limitations on the collection and use of biometric data, although it is not always clear if these state statutes apply to employment, and many do not provide private rights of action.111 Like the BIPA, these statutes are narrowly limited in the types of information that are protected and apply only within the state's borders.
The federal Fair Credit Reporting Act (FCRA) regulates employers' access to applicants' or employees' credit reports. The statute requires employers to get written authorization to obtain employee credit reports; employers must also notify employees if the credit report is used to take adverse action against them.112 The FCRA applies only when employers receive or use consumer reports from consumer reporting agencies, but the term consumer report is construed broadly to include any information that goes to "character, general reputation, personal characteristics, or mode of living."113 Because the FCRA largely focuses on procedural requirements of notice and consent, employers can generally avoid liability under the Act if they comply with the details of the statutory scheme.114
Although relatively narrow in scope, state statutes also regulate the use of specific types of information within the employment relationship. Twenty-six states have laws prohibiting employers from requesting access to applicants' or employees' private social-media accounts.115 And a number of states and municipalities have passed "ban the box" laws that prohibit employers from requesting information about prior arrests or convictions at certain early points in the hiring process.116
Artificial intelligence that relies on employee data also raises concerns about the security of the data that has been collected. The ADA and GINA require employers to keep any medical or genetic information they lawfully acquired in a secure and confidential manner.117 All fifty states have data breach notification laws that would apply to employers when a data breach involves employee personal data.118 Statutory schemes such as HIPAA and Illinois BIPA impose security requirements on certain types of information.119 Tort claims against employers for faulty or negligent data security systems have met with mixed success.120
2. Protecting Workplace Privacy under a Data Protection Framework
American law has tended to follow a privacy rights approach that focuses on prohibiting particular types of intrusions or shielding certain kinds of information, but this framework has created only limited restrictions on employers' ability to collect data about applicants and workers. In Europe, however, the focus has been on data protection more broadly, relying on principles that apply across sectors and types of information. The data protection model of the European Union (EU) aims to restrict the collection, use, and disclosure of personal information except where justified, and does so by creating rights in individual data subjects to enforce those restrictions. The EU's General Data Protection Regulation (GDPR) is a paradigmatic example of a comprehensive data protection regime.121 Its scope, requirements for processing data, and muscular enforcement regime empower individuals with important rights over the use of their data.122
The GDPR applies to all processing of personal data,123 including by employers. The broad definition of personal data124 means that all information collected by an employer about applicants and employees is covered as long as it is connected to an identifiable person. Any processing-including collection, use, or disclosure-of personal data must have a legal justification.125 Although data processing can be justified by the consent of the data subject in certain circumstances, consent is not considered valid "where there is a clear imbalance between the data subject and the controller."126 The employment relationship is understood to be one example of such a "clear imbalance."127 Employer collection and use of employee data must therefore be justified by basic requirements of the work relationship or the legitimate needs of the employer, rather than by relying on consent.

Where the processing of employee data is necessary, the GDPR asks employers to take steps to mitigate the effects on employees-for example, by monitoring only in specific places and not sensitive areas, or collecting data by sampling rather than continuous monitoring.128 The EU privacy agency's guidance on the workplace provides examples of illegitimate employer uses of employee data: when monitoring designed to protect employee safety is used for job-evaluation purposes; when a CCTV system is used to regularly monitor employee behavior; or when geolocation data is used to continuously track an employee's movements and actions.129

The GDPR also gives data subjects two sets of rights: rights to know about the processing, and rights to affect the processing. Data processors, including employers, are required to disclose information about the processing in clear and accessible language.130 This information includes the categories of data collected, the purpose of and legal basis for the processing, how the data will be used and/or disclosed, and the procedures for challenging these processes.131 Rights affecting data processing include the right to correct inaccurate data, the right to supplement incomplete data,132 and the right to request deletion of data under some circumstances.133

The GDPR thus represents a very different model for the regulation of employee data collection and use. It is comprehensive in scope, requires specific justifications for data collection, limits data use beyond the original purpose, and provides individuals with specific rights regarding the collection and use of their personal data.

Although the GDPR applies to data about individuals located in the EU, it is having significant impact worldwide. In part, its influence arises from the fact that data flows often are not limited by political boundaries, but the GDPR also sets an example that influences lawmaking elsewhere. In the United States, it has been suggested as a blueprint for federal privacy legislation and has already influenced state law. The California Consumer Privacy Act (CCPA), which went into effect in 2020, provides important notification requirements on the collection and processing of personal data, as well as the right to delete certain data and opt out of third party transfers.134 Voters passed the California Privacy Rights Act (CPRA) in fall 2020; the CPRA will enhance consumers' ability to correct inaccurate information, limit the use of sensitive data, expand the private right of action, and create an independent state agency for privacy regulation.135 Both of these Acts, however, have limited impact on employment; the CCPA currently has a specific exception that excludes employee data from coverage.136

Following the EU's data protection model would be a dramatic departure from the current U.S. approach to employee privacy. Only a patchwork of laws currently restrict employers' ability to collect data from and about their employees. Employers in the United States face only limited prohibitions on the collection of employee data, and paratively restrictions on how they use data once it has been collected. They may not use information about individual workers to discriminate on the basis of protected characteristics or to retaliate against them for exercising statutory rights, but, beyond that, employers are generally free to use the information they have about employees however they wish. They may aggregate and analyze worker data to infer new information about their employees.137 And U.S. law generally neither limits employers to only using data for the purpose for which it was collected nor requires that they ensure the accuracy of the data.138

B. AI Accountability and Transparency in the Workplace

Distinct from employees' interests in limiting collection and use of their personal information is the growing push for greater transparency, accountability, and explainability in algorithmic processes.139 Although not part of traditional "privacy" concerns, these values are partially addressed through broader approaches to data regulation.140 Moreover, these values resonate with employee concerns about the increasing use of AI within the workplace. It is not just that data is constantly vacuumed from employees; it is that the data is then put to use to make decisions about them that can appear arbitrary or severe, with no opportunity for employee recourse.141 Their vulnerability to observation and scrutiny thus heightens their vulnerability to capricious and sudden managerial discretion. Workers can feel that they are cogs within a massive and impersonal machine.

U.S. law currently does little to ensure the accountability and transparency of artificial intelligence.142 If anything, it reinforces the hidden nature of AI processes through trade secret protections.143 Some reformers have proposed that AI processes be accountable and made transparent through mandates requiring entities that use these systems to conduct algorithmic impact assessments (AIA).144 Others have argued that incentivizing the use of more

appropriate and less error-ridden algorithmic tools may be preferable to creating new individual rights to challenge machine decisions.145 But, although proposed legislation has included transparency and accountability requirements, currently no American laws comprehensively regulate the use of AI in decision-making.

Once again, the GDPR suggests an alternative model. It specifically addresses AI decision-making by requiring disclosure of automated decision-systems and restricting their use, even allowing data subjects to opt out of fully automated profiling. Article 22 states, "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."146 Profiling is described as

any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.147

The restriction does have two significant exceptions: one if the processing is necessary to performance of a contract, and another if the individual gives "explicit consent."148 While these exceptions seem to relieve employers of the requirements of Article 22, they are not as broad in the employment context as they may appear. "Necessary" to contractual performance means that the performance must be impossible without the automated processing, and, as discussed earlier, the consent exception is generally unavailable to employers.149 Given the newness of the GDPR, and in particular the protections in Article 22,150 it remains to be seen how potent this right will be in restricting the use of predictive AI. It is possible that entities that use machine learning (ML) tools will simply put a human nominally in charge at the end of the process to rubber-stamp the decision in order to argue that the decision is not "based solely on automated processing" and therefore falls outside the regulation.151

Employees arguably have a stronger interest in challenging automated processing than consumers, because they are more likely to feel its effects keenly when it is used to manage and discipline them. However, current U.S. law offers no clear vehicles for raising such challenges. So far, legal reform and enforcement efforts have largely focused on consumer interests, as seen in recent consumer-focused state privacy statutes and the Federal Trade Commission's consumeroriented enforcement against unfair trade practices. Even if the law were to create stronger data protection rights for workers, they may not be able to effectively assert those rights in the absence of effective vehicles for them to exercise voice and power in the workplace. Thus, meaningful protections of employees' privacy and autonomy interests around predictive AI tools will likely require not only legal change, but enhanced worker power through collective activity as well.

Conclusion

Current U.S. law is ill-equipped to manage the challenges posed by the increasing use of artificial intelligence within the workplace. While some existing legal rules shield workers from discrimination and protect employee privacy and autonomy, the law lacks a comprehensive framework for addressing the particular risks of harm posed when machine learning tools are applied to manage workers. As AI becomes more integrated and essential to business, the law will need to adapt in order to effectively prevent discrimination, protect privacy, and redress concerns about worker alienation and loss of personal security.

Footnote

1. Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 U.C. Davis L. Rev. 399, 401 (2017).

2. See Deborah Hellman, Measuring Algorithmic Fairness, 106 Va. L. Rev. 811, 813-14 (2020) (The use of algorithms, and in particular their connection with machine learning and artificial intelligence, has attracted significant attention in the legal literature as well.). For a small sampling of the literature, see Frank Pasquale, The Black Box Society (2015); Hannah Bloch-Wehba, Access to Algorithms, 88 Fordham L. Rev. 1265 (2020); Danielle Keats Citron &Frank Pasquale, The Scored Society: Due Process for Automated Predictions, 89 Wash. L. Rev. 1 (2014); Aziz Z. Huq, A Right to a Human Decision, 106 Va. L. Rev. 611, 613 (2020); Sonia K. Katyal, Private Accountability in the Age of Artificial Intelligence, 66 UCLA L. Rev. 54 (2019); David Lehr &Paul Ohm, Playing with the Data: What Legal Scholars Should Learn About Machine Learning, 51 U.C. Davis L. Rev. 653, 655 (2017).

3. Calo, supra note 1, at 404 (defining AI as "a set of techniques aimed at approximating some aspect of human or animal cognition using machines" and explaining that "[t]here is no straightforward, consensus definition of artificial intelligence"); Ashley Deeks, The Judicial Demand for Explainable Artificial Intelligence, 119 Colum. L. Rev. 1829, 1832 (2019) ("Artificial intelligence is a notoriously capacious and slippery term."); see Commission White Paper onArtificial Intelligence-A European Approach to Excellence and Trust, COM (2020) 65 final (Feb. 19, 2020),<https://ec.europa.eu/info/sites/info/files /commission-white-paper-artificial-intelligence-feb2020_en.pdf> [https://perma.cc/P3KG -UFEV] ("Simply put, AI is a collection of technologies that combine data, algorithms and computing power.").
4. Calo, supra note 1, at 402 (noting that "a vast increase in computational power and access to training data has led to practical breakthroughs in machine learning, a singularly important branch of AI"); Deeks, supra note 3, at 1829 ("A recurrent concern about machine learning algorithms is that they operate as 'black boxes.'").
5. Future of Privacy Forum, The Privacy Expert's Guide to Artificial Intelligence and Machine Learning 5 (2018), https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial -Intelligence_Digital.pdf [https://perma.cc/949W-QHL4] [hereinafter FPF Expert's Guide].
6. See id. at 5-6.
7. Id. at 6; Calo, supra note 1, at 405 ("An important consequence of the shift was that researchers began to try to solve specific problems or master particular 'domains,' such as converting speech to text or playing chess, instead of pursuing a holistic intelligence capable of performing every cognitive task within one system.").
8. FPF Expert's Guide, supra note 5, at 6; Alison DeNisco Rayome, Why IBM's Speech Recognition Breakthrough Matters for AI and IoT, TechRepublic (Mar. 13, 2017, 9:39 AM), https://www.techrepublic.com/article/why-ibms-speech-recognition-breakthrough-matters-for-ai-and-iot [https://perma.cc/F9SH-HSQF]. The speed of advancement just in the last five years has taken some observers by surprise. See Cynthia Estlund, What Should We Do After Work? Automation and Employment Law, 128 Yale L.J. 254, 265-66 (2018) (discussing the leap forward in natural language translation in 2016).
9. See, e.g., Elizabeth E. Joh, Artificial Intelligence and Policing: Hints in the Carpenter Decision, 16 Ohio St. J. Crim. L. 281, 283-84 (2018); Tom C.W. Lin, Artificial Intelligence, Finance, and the Law, 88 Fordham L. Rev. 531, 532 (2019); William Magnuson, Artificial Financial Intelligence, 10 Harv. Bus. L. Rev. 337, 340-41 (2020); Andrew D. Selbst, Disparate Impact in Big Data Policing, 52 Ga. L. Rev. 109, 113-14 (2017); Crystal S.Yang &Will Dobbie, Equal Protection Under Algorithms: A New Statistical and Legal Framework, 119 Mich. L. Rev. 291 (2020).
10. Pasquale, supra note 2, at 3-11; Citron &Pasquale, supra note 2.
11. FPF Expert's Guide, supra note 5, at 22.
12. Id.
13. Id.
14. See Erik Brynjolfsson &Andrew McAfee, The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies 126-28 (2014); Frank Pasquale, Data-Informed Duties in AI Development, 119 Colum. L. Rev. 1917, 1917 (2019) ("Corporations will increasingly attempt to substitute artificial intelligence (AI) and robotics for human labor."); Kevin J. Delaney, The Robot That Takes Your Job Should Pay Taxes, Says Bill Gates, Quartz.com (Feb. 17, 2017), https://qz.com/911968/bill-gates-therobot-that-takes-your-job-should-pay-taxes [https://perma.cc/D3SD-3JXK].
15. Compare Estlund, supra note 8, at 264 ("[B]ecause emerging technologies are able to replicate or surpass a wider swath of human capabilities, there is more reason this time around to expect job destruction to outpace job creation."), with H. James Wilson &Paul R. Daugherty, Collaborative Intelligence: Humans and AI Are Joining Forces, Harv. Bus. Rev. (July- Aug. 2018), https://hbr.org/2018/07/collaborative-intelligence -humans-and-ai-are-joining-forces [https://perma.cc/Z8AK-WJDH] ("While AI will radically alter how work gets done and who does it, the technology's larger impact will be in complementing and augmenting human capabilities, not replacing them.").
16. Miranda Bogen &Aaron Rieke, Upturn, Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias 3 (2018),<https://www.upturn.org/static/reports/2018/hiring -algorithms/files/Upturn%20-%20Help%20Wanted%20-

%20An%20Exploration%20> of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.
17. See, e.g., Ifeoma Ajunwa, Beware of Automated Hiring, N.Y. Times (Oct. 8, 2019), https://www.nytimes.com/2019/10/08/opinion/ai-hiring-discrimination.html [https://perma .cc/4YKD-9A4E]; Chris Opfer, AI Hiring Could Mean Robot Discrimination Will Head to Courts, Daily Lab. Rep. (BL) (Nov. 12, 2019, 5:01 AM), https://news.bloomberglaw .com/daily-labor-report/ai-hiring-could-mean-robot-discrimination-will-head-to-courts [https://perma.cc/WCP2-H2E2].
18. Rachel Emma Silverman &Nikki Waller, The Algorithm That Tells the Boss Who Might Quit, Wall St. J. (Mar. 13, 2015, 7:05 PM), https://www.wsj.com/articles/the -algorithm-that-tells-the-boss-who-might-quit-1426287935 [https://perma.cc/4EE3-4NB4].
19. Vegard Kolbjørnsrud, Richard Amico &Robert J. Thomas, How Artificial Intelligence Will Redefine Management, Harv. Bus. Rev. (Nov. 2, 2016),<https://hbr.org/2016/11 /how-artificial-intelligence-will-redefine-management> [https://perma.cc/NK42-J46J] ("The fact is, artificial intelligence will soon be able to do the administrative tasks that consume much of managers' time faster, better, and at a lower cost.").
20. Rani Molla, 10 Ways Office Work Will Never Be the Same, Recode, (Mar. 23, 2021, 8:20 AM), https://www.vox.com/recode/22331447/10-ways-office-work-pandemic-futureremote-work [https://perma.cc/P72F-N8TS]; Matthew Wille, Employers Are Turning to AI to Enforce Social Distancing for COVID-19, Input (Apr. 28, 2020, 11:01 AM), https:// www.inputmag.com/tech/employers-are-turning-to-ai-to-enforce-social-distancing-covid -19-coronavirus[https://perma.cc/CU4Q-YSHA].
21. See Dave Gershgorn, Companies Are on the Hook If Their Hiring Algorithms Are Biased, Quartz (Oct. 22, 2018), https://qz.com/1427621/companies-are-on-the-hook -if-their-hiring-algorithms-are-biased [https://perma.cc/WM4W-NNBM] (discussing Amazon test program that consistently chose men over women for positions).
22. Ifeoma Ajunwa, Kate Crawford &Jason Schultz, Limitless Worker Surveillance, 105 Calif. L. Rev. 735, 737 (2017) ("Employees' suspicion that OccupEye's true purpose was mass surveillance of worker performance quickly led to public outrage, union pressure, and, ultimately, its ejection from the Telegraph building.").
23. Deeks, supra note 3, at 1829 ("Because these algorithms repeatedly adjust the way that they weigh inputs to improve the accuracy of their predictions, it can be difficult to identify how and why the algorithms reach the outcomes they do."); Andrew D. Selbst &Solon Barocas, The Intuitive Appeal of Explainable Machines, 87 Fordham L. Rev. 1085, 1087 (2018) ("The results of these algorithms can be unnerving, unfair, unsafe, unpredictable, and unaccountable.").
24. See, e.g., Claire Cain Miller, Can an Algorithm Hire Better Than a Human?, N.Y. Times: The Upshot (June 25, 2015), http://www.nytimes.com/2015/06/26/upshot/can -an-algorithm-hire-better-than-a-human.html [https://perma.cc/PKM6-4JY4]; Matt Richtel, How Big Data Is Playing Recruiter for Specialized Workers, N.Y. Times (Apr. 27, 2013), http://www.nytimes.com/2013/04/28/technology/how-big-data-is-playing-recruiter forspecialized-workers.html [https://perma.cc/XAF6-SKXC]; Dustin Volz, Silicon Valley Thinks It Has the Answer to Its Diversity Problem, Atlantic (Sept. 26, 2014), http://www .theatlantic.com/politics/archive/2014/09/silicon-valley-thinks-it-has-the-answer-to-its -diversity-problem/431334 [https://perma.cc/VA6N-6W53].
25. For a few of the many articles documenting human bias in the employment process, see Jerry Kang &Kristine Lane, Seeing Through Colorblindness: Implicit Bias and the Law, 58 UCLA L. Rev. 465, 468-89 (2010); Linda Krieger, The Content of Our Categories: A Cognitive Bias Approach to Discrimination and Equal Employment Opportunity, 47 Stan. L. Rev. 1161, 1186-88 (1995); Anthony G. Greenwald &Linda Hamilton Krieger, Implicit Bias: Scientific Foundations, 94 Calif. L. Rev. 945, 946 (2006); R. Richard Banks, Jennifer L. Eberhardt &Lee Ross, Discrimination and Implicit Bias in a Racially Unequal Society, 94 Calif. L. Rev. 1169, 1170 (2006).
26. Latanya Sweeney is a prominent computer scientist and professor at Harvard University. She conducted the study documenting this effect after a colleague notified her that such an ad had appeared when he had Googled her name.
27. Latanya Sweeney, Discrimination in Online Ad Delivery, Commc'ns ACM, May 2013, at 44, 46-47.
28. Jeffrey Dastin, Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women, Reuters (Oct. 10,

2018, 6:04 PM),<https://www.reuters.com/article /us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that> -showed-bias-against-women-idUSKCN1MK08G [https://perma.cc/T6NZ-T4ZW].
29. See Solon Barocas &Andrew D. Selbst, Big Data's Disparate Impact, 104 Calif. L. Rev. 671, 674 (2016).
30. See Alex Engler, For Some Employment Algorithms, Disability Discrimination by Default, Brookings (Oct. 31, 2019),<https://www.brookings.edu/blog/techtank/2019/10/31 /for-some-employment-algorithms-disability-discrimination-by-default> [https://perma.cc /M7RS-MW5C].
31. For systematic discussions of how algorithms can produce biased results, see Barocas &Selbst, supra note 29, at 674; Pauline T. Kim, Data-Driven Discrimination at Work, 58 Wm. &Mary L. Rev. 857, 874, 887, 891 (2017) [hereinafter Kim, Data-Driven Discrimination]; David Lehr &Paul Ohm, Playing with the Data: What Legal Scholars Should Learn About Machine Learning, 51 U.C. Davis L. Rev. 653, 703-04 (2017).
32. Ifeoma Ajunwa, The Paradox of Automation as Anti-Bias Intervention, 41 Cardozo L. Rev. 1671, 1713 (2020).
33. Bogen &Rieke, supra note 16, at 5-6.
34. Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove &Aaron Rieke, Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes, 3 Proc. ACM on Hum.-Comput. Interaction 1 (2019).
35. Pauline T. Kim, Manipulating Opportunity, 106 Va. L. Rev. 867, 881 (2020).
36. Piotr Sapiezynski, Avijit Ghosh, Levi Kaplan, Alan Mislove &Aaron Rieke, Algorithms That "Don't See Color": Comparing Biases in Lookalike and Special Ad Audiences, arXiv (Dec. 17, 2019), https://arxiv.org/pdf/-1912.07579.pdf [https://perma .cc/HG3E-NLCY]; Ava Kofman &Ariana Tobin, Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement, ProPublica (Dec. 13, 2019, 5:00 AM), https://www.propublica.org/article/facebook-ads-can-still-discriminate -against-women-and-older-workers-despite-a-civil-rights-settlement [https://perma.cc /F3YU-HCTQ].
37. Ali et al., supra note 34, at 8; Kofman &Tobin, supra note 36.
38. Ledbetter v. Goodyear Tire &Rubber Co., 550 U.S. 618, 622 (2007).
39. Kevin Stainback &Donald Tomaskovic-Devey, Documenting Desegregation: Racial and Gender Segregation in Private-Sector Employment Since the Civil Rights Act 7 (2012).
40. Kim, Manipulating Opportunity, supra note 35, at 892.
41. Pauline T. Kim, Auditing Algorithms for Discrimination, 166 Univ. Pa. L. Rev. Online 189, 190 (2017), https://scholarship.law.upenn.edu/cgi/viewcontent .cgi?article=1212&context=penn_law_review_online.
42. Title VII of the Civil Rights Act of 1964 expressly forbids discrimination based on race, color, religion, national origin and sex, Civil Rights Act of 1964 703-716, 42 U.S.C. 2000e to 2000e-15, and the Supreme Court recently interpreted its prohibitions to extend to sexual orientation and gender identity discrimination as well, Bostock v. Clayton Cty., Georgia, 140 S. Ct. 1731, 1743 (2020). The Age Discrimination in Employment Act, 29 U.S.C. 621-634, the Americans with Disabilities Act, 42 U.S.C. 12101-12117, and the Genetic Information Nondiscrimination Act, 42 U.S.C. 2000ff, protect against discrimination on the basis of age, disability, and genetic information, respectively.
43. 42 U.S.C. 2000e-3(b).
44. 29 U.S.C. 623(e).
45. Pauline T. Kim &Sharion Scott, Discrimination in Online Employment Recruiting, 63 St. Louis Univ. L. J. 93, 94 (2018). The settlement in 2019 of a lawsuit against Facebook makes it more difficult for employers to deliberately target its ads on that platform in a way that excludes protected groups. Galen Sherwin &Esha Bhandari, Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform, ACLU (Mar. 19, 2019, 2:00 PM),<https://www.aclu.org/blog/womens-rights/womens-rights-work place/facebook-settles-civil-rights-cases-making-sweeping> [https://perma.cc/H6D6-UMJ4]. Pursuant to the settlement, Facebook agreed to require employment, housing, and credit advertisements to be placed through a special portal that restricts the options for targeting these types of ads. Although the restrictions will make it more difficult to deliberately exclude an audience based on a protected characteristic, doing so is still possible. Kim, Manipulating Opportunity, supra note 35, at 890-

91; see also Miriam A. Cherry, Age Discrimination in the On-Demand Economy and Crowdwork, 40 Berkeley J. Emp. &Lab. L. 29, 56-57 (2019).
46. See, Kim, Manipulating Opportunity, supra note 35, at 913.
47. See 42 U.S.C. 2000e-2(a)(1).
48. See Griggs v. Duke Power Co., 401 U.S. 424, 429-30 (1971); see also 42 U.S.C. 2000e-2(k).
49. 42 U.S.C. 2000e-2(k).
50. Id. 2000e-2(k)(1)(A).
51. Id. 2000e-2(k)(1)(A)(i).
52. Id. 2000e-2(k)(1)(A)(ii). The ADEA and the ADA do not have provisions comparable to 703(k), which sets out these shifting burdens, but they do contain language authorizing disparate impact claims based on age and disability. 29 U.S.C. 623(a)(2); 42 U.S.C. 12112(b)(3). Some courts, however, have held that disparate impact claims by applicants, as opposed to current employees, are not available under the ADEA. Kleber v. CareFusion Corp., 914 F.3d 480, 480 (7th Cir. 2019); Villarreal v. R.J. Reynolds Tobacco Co., 839 F.3d 958, 970 (11th Cir. 2016).
53. Uniform Guidelines on Employee Selection Procedures, 29 C.F.R. 1607.15 (2020).
54. Don Peck, They're Watching You at Work, Atlantic (Dec. 2013), https://www.the atlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681 [perma.cc /MAG2-UFAQ]; Michal Kosinski, David Stillwell &Thore Graepel, Private Traits and Attributes Are Predictable from Digital Records of Human Behavior, 110 Proc. Nat'l Acad. Sci. U.S. 5802, 5805 (2013).
55. 42 U.S.C. 2000e-2(a)(2), Parallel language appears in the ADEA, 29 U.S.C. 623(a)(2), although it omits "applicants." The ADA defines discrimination to include use of criteria that "have the effect of discrimination," 42 U.S.C. 12112(b)(3)(a), which authorizes disparate impact cases. Raytheon Co. v. Hernandez, 540 U.S. 44, 53 (2003).
56. Kim, Data-Driven Discrimination, supra note 31, at 857, 916-17.
57. Id. at 886-87.
58. The problem with relying on pure correlations is that the relationship between two variables may not be stable over time. A correlation in the past may not hold true in the future, which means that applicants could be denied an opportunity on what turns out to be an arbitrary, irrelevant basis.
59. 42 U.S.C. 12112(b)(6).
60. Id. 12112(b)(7).
61. Leadership Conf. Educ. Fund et al., Civil Rights Principles for Hiring Assessment Technologies (2020), http://civilrightsdocs.info/pdf/policy/letters/2020/Hiring _Principles_FINAL_7.29.20.pdf.
62. See generally Kim, supra note 41.
63. Ricci v. DeStefano, 557 U.S. 557, 581 (2009) (quoting Local No. 93, Int'l Ass'n of Firefighters v. City of Cleveland, 478 U.S. 510, 515 (1986)).
64. 557 U.S. 557 (2009).
65. See, e.g., Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson &Harlan Yu, Accountable Algorithms, 165 U. Pa. L. Rev. 633, 692 (2017).
66. See Kim, supra note 41, at 197-202 (explaining why Ricci does not prohibit employers from correcting algorithms that cause biased outcomes).
67. Ricci, 557 U.S. at 583-84.
68. Id. at 585.
69. See, e.g., Maraschiello v. City of Buffalo Police Dep't, 709 F.3d 87 (2d Cir. 2013); Carroll v. City of Mount Vernon, 707 F. Supp. 2d 449 (S.D.N.Y. 2010), aff'd, 453 F. App'x 99 (2d Cir. 2011).
70. See Wilson &Daugherty, supra note 15 (discussing collaborations between workers and AI).
71. Ellyn Shook, Eva Sage-Gavin &Susan Cantrell, How Companies Can Use Employee Data Responsibly, Harv. Bus. Rev. (Feb. 15, 2019), https://hbr.org/2019/02/how -companies-can-use-employee-data-responsibly

[perma.cc/SP5N-DKQU].
72. Calo, supra note 1, at 405 ("The recent explosion of [AI] efficacy comes from a combination of much faster computers and much more data."); Jeffrey M. Hirsch, Future Work, 2020 Univ. Ill. L. Rev. 889, 897 ("To learn in a sufficiently accurate manner, AI programs not only require massive amounts of data, but data that is organized in precise ways.").
73. For example, the pool of emails taken from Enron by the federal government and released to the public, known as the Enron Corpus, has been critical in developing speechand language-related AI. See Jessica Leber, The Immortal Life of the Enron E-Mails, MIT Tech. Rev. (July 2, 2013), https://www.technologyreview.com/2013/07/02/177506/the -immortal-life-of-the-enron-e-mails [perma.cc/GTC7-5JR6].
74. See, e.g., David Kravets, Worker Fired for Disabling GPS App That Tracked Her 24 Hours a Day, Ars Technica (May 11, 2015, 9:41 AM),<http://arstechnica.com/tech -policy/2015/05/worker-fired-for-disabling-gps-app-that-tracked-her-24-hours-a-day> [https://perma.cc/476P-L94B].
75. Frank Pasquale, The Other Big Brother, Atlantic (Sept. 21, 2015), https:// www.theatlantic.com/business/archive/2015/09/corporate-surveillance-activists/406201 [perma.cc/8QMW-2VYX] ("Employers are monitoring keystrokes, tones of voice, and faces, all in the name of predictive analytics.").
76. Christopher Rowland, With Fitness Trackers in the Workplace, Bosses Can Monitor Your Every Step-and Possibly More, Wash. Post (Feb. 16, 2019, 6:13 PM), https:// www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace -bosses-can-monitor-your-every-step-and-possibly-more/2019/02/15/75ee0848-2a45 -11e9-b011-d8500644dc98_story.html [perma.cc/JAJ6-S2DP].
77. Stephen Baker, Managing by the Numbers, Businessweek, Sept. 8, 2008, at 32, 34.
78. See, e.g., Ajunwa, Crawford &Schultz, supra note 22, at 772; Leora Eisenstadt, Data Analytics and the Erosion of the Work/Nonwork Divide, 56 Am. Bus. L.J. 445, 447 (2019); J.S. Nelson, Management Culture and Surveillance, 43 Seattle Univ. L. Rev. 631, 634 (2020).
79. Alan F. Westin, Privacy in the Workplace: How Well Does American Law Reflect American Values?, 72 Chi.-Kent L. Rev. 271, 282-83 (1996) ("[T]he U.S. approach to privacy remains a more eclectic blend of constitutional interpretation, pin-pointed and sector-specific legislation, sector-based administrative agency rules, common-law judicial interpretation, labor-management bargaining (where employees are unionrepresented), voluntary organizational policies, and market-based dynamics.").
80. See, e.g., O'Connor v. Ortega, 480 U.S. 709, 725-26 (1987); City of Ontario v. Quon, 560 U.S. 746, 756-57 (2010).
81. Cf Pauline T. Kim, Privacy Rights, Public Policy, and the Employment Relationship, 57 Ohio St. L.J. 671, 674 n.17 (1996) ("In rare cases, where a private employer is acting as an instrument or agent of the government, constitutional privacy protections may extend to workers in the private sector."). Only a handful of states have constitutional or statutory provisions that provide general privacy protections for private sector employees. For example, California's constitutional privacy provision applies to private actors. Cal. Const. art. I, 1 (providing for "inalienable rights" including "pursuing and obtaining safety, happiness, and privacy"); Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 642-44 (Cal. 1994) (holding that the state's constitutional right of privacy extends to private actors, including private-sector employers); see also Mass. Gen. Laws ch. 214, 1B (2018); Neb. Rev. Stat. 20-203 (2019); R.I. Gen. Laws 9-1-28.1(a)(1) (2019); Wise. Stat. Ann. 995.50(2)(a) (2019).
82. The Constitution has also been thought to protect informational privacy, although the existence of such a right has not been authoritatively confirmed. See Nat'l Aeronautics &Space Admin. v. Nelson, 562 U.S. 134, 138 (2011) (assuming, without deciding, that employees had a right to informational privacy).
83. Intrusion on seclusion is one of four privacy torts recognized in the Restatement (Second) of Torts 652B (Am. L. Inst. 1977). The other three privacy torts are public disclosure of private fact, id. 652D; appropriation of another's name or likeness, id. 652C; and publicity that unreasonably places another in a false light, id. 652E.
84. Restatement of Emp. L. 7.01 Reporters' Notes cmt. b, at 296-98 (Am. L. Inst. 2015) (discussing states that have

adopted the privacy torts).
85. See, e.g., York v. Gen. Elec. Co., 759 N.E.2d 865 (Ohio Ct. App. 2001).
86. See, e.g., Johnson v. K-Mart Corp., 723 N.E.2d 1192 (Ill. App. Ct. 2000).
87. See, e.g., K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 640-41 (Tex. App. 1984).
88. See, e.g., Elmore v. Atl. Zayre, Inc., 341 S.E.2d 905, 906-907 (Ga. Ct. App. 1986) (bathroom); Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073 (Cal. 2009) (office).
89. Restatement (Second) of Torts 652B (Am. L. Inst. 1977).
90. Pauline T. Kim, Data Mining and the Challenges of Protecting Employee Privacy Under U.S. Law, 40 Comp. Lab. L. &Pol'y J. 405, 416 (2019) (explaining that the common law tort doctrine "does not address how data mining can threaten privacy by inferring highly personal information rather than collecting it directly").
91. See Feminist Women's Health Ctr. v. Super. Ct. of Sacramento Cnty., 61 Cal. Rptr. 2d 187, 195 (Ct. App. 3d 1997) (finding that a requirement that employees demonstrate self-cervical exams to clients of the Center was not a privacy intrusion because of the employer's "fundamental goal of educating women about the function and health of their reproductive systems").
92. Restatement of Emp. L., 7.06 cmt. h (Am. L. Inst. 2015) ("In the employment context, employee consent obtained as a condition of obtaining or retaining employment is not effective consent to an employer intrusion and does not in itself provide a defense . . . .").
93. Restatement (Second) of Torts 892A(1); see Steven L. Willborn, Consenting Employees: Workplace Privacy and the Role of Consent, 66 La. L. Rev. 975, 1008 (2006) (arguing for the importance of the concept of consent within workplace privacy protections).
94. Restatement of Emp. L. 7.03(b) (describing the conditions for finding a reasonable expectation of privacy).
95. See Ajunwa, Crawford &Schultz, supra note 22, at 747 ("There are no federal laws that expressly address employer surveillance or limit the intrusiveness of such surveillance.").
96. See, e.g., Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174, 184 (1st Cir. 1997) (permitting the use of cameras to continually surveil the employees' work space).
97. California makes it a misdemeanor to use an electronic tracking device to follow the location or movement of a person without her consent. Cal. Penal Code 637.7 (West 2019); see also Kendra Rosenberg, Location Surveillance by GPS: Balancing an Employer's Business Interest with Employee Privacy, 6 Wash. J.L. Tech. &Arts 143, 149 (2010). Connecticut requires employers to provide prior written notice of the monitoring, Conn. Gen. Stat. 31-48d(b)(1) (2020); Gerardi v. City of Bridgeport, 985 A.2d 328, 335 (Conn. 2010) (prohibiting an employer from electronically monitoring an employee's activities without prior notice). Delaware requires advance written notice that the employee must then acknowledge. Del. Code Ann. tit. 19, 705 (2020).
98. 29 U.S.C. 158(a)(1); see Charlotte Garden, Labor Organizing in the Age of Surveillance, 63 St. Louis Univ. L.J. 55, 60 (2018) (noting that "certain surveillance activities by employers have been illegal since the earliest days of the NLRA").
99. See Ass'n Servs., Inc. v. Smith, 549 S.E.2d 454, 463 (Ga. Ct. App. 2001) (employer trespassed onto employee property); Saldana v. Kelsey-Hayes Co., 443 N.W.2d 382, 384 (Mich. Ct. App. 1989) (finding intrusion (but no liability) when investigator took pictures inside employee's home using a telephoto lens); see also Pemberton v. Bethlehem Steel Corp., 502 A.2d 1101, 1117 (Md. Ct. Spec. App. 1986) (holding that the use of a listening device within personal areas is generally actionable); Burns v. Masterbrand Cabinets, Inc., 874 N.E.2d 72, 77 (Ill. App. 2007) (remanding for further proceedings on intrusion claim when the employer's investigator secretly videotaped an employee in his home after gaining entry on false pretenses).
100. See, e.g., ICU Investigations, Inc. v. Jones, 780 So. 2d 685, 693 (Ala. 2000) (no intrusion when videotaped in front yard); York v. Gen. Elec. Co., 759 N.E.2d 865, 866 (Ohio Ct. App. 2001) (no intrusion when employer representative observed the employee arriving at work, going into his chiropractor's office, visiting a lawnmower repair shop, mowing his lawn, and riding a motorcycle).
101. See 18 U.S.C. 2511 (criminalizing the actions of a person who "intentionally intercepts, endeavors to intercept,

or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication"). The intercept is not illegal if one of the parties (namely, the employee) consents to it. Id. 2511(2)(c). However, courts have not been disposed to find implied consent. Watkins v. L.M. Berry, 704 F.2d 577, 581 (11th Cir. 1983) (notice as to employer policy of interception did not establish consent). Furthermore, a "business extension" exception allows for monitoring "in the ordinary course of business." 18 U.S.C. 2510(5)(a)(i). However, listening in to personal calls is not generally within the ordinary course of business. See Watkins, 704 F.2d at 583. Wiretapping is also problematic under state common law. See Narducci v. Village of Bellwood, 444 F. Supp. 2d 924, 938 (N.D. Ill. 2006) ("Eavesdropping via wiretapping has been conspicuously singled out on several occasions as precisely the kind of conduct that gives rise to an intrusion-on-seclusion claim.").

102. See Marrs v. Marriott Corp., 830 F. Supp. 274, 283 (D. Md. 1992) (permitting secret videotaping after hours to uncover thief); Sacramento Cty. Deputy Sheriffs' Assoc. v. County of Sacramento, 59 Cal. Rptr. 2d 834, 847 (Ct. App. 1997) (theft of inmates' property justified secret surveillance). But see Acuff v. IBP, Inc., 77 F. Supp. 2d 914, 927 (C.D. Ill. 1999) (videotaping nurse's office during medical exams not justified by concerns about theft).

103. 42 U.S.C. 12112(d) (ADA limitation on examinations); 42 U.S.C. 2000ff-1(b) (making it "an unlawful employment practice for an employer to request, require, or purchase genetic information with respect to an employee").

104. Health Information Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26, 29, and 42 U.S.C.). 105. 45 C.F.R. 160.103 (2020) (defining covered entity as a health plan, a health care clearinghouse, or a health care provider).

106. See id. 164.103, 164.105; Sharona Hoffman, Employing E-Health: The Impact of Electronic Health Records on the Workplace, 19 Kan. J.L. &Pub. Pol'y 409, 419 (2010) ("Employers who are self-insured can receive medical information from providers for payment purposes without their employees' authorization. Such employers are considered 'hybrid' entities whose business activities include both covered (insurance) and non-covered (employment) functions.").

107. See 45 C.F.R. 160.103. In addition, covered entities may provide employee health information to employers in order "[t]o evaluate whether the individual has a work-related illness or injury." Id. 164.512(b)(v)(A)(2); see also id. 164.504(f) (noting that as a condition of providing the information, the covered entity must require the employer to protect the information and not use it for employment-related actions).

108. What Is the Difference Between "Consent" and "Authorization" Under the HIPAA Privacy Rule?, U.S. Dep't Health &Hum. Servs. (2013),<https://www.hhs.gov/hipaa /for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization /index.html> [https://perma.cc/B64H-APE5].

109. Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1-/99 (2018).

110. Corrado Rizzi, Illinois Wendy's Operator Hit with BIPA Class Action over Employee Fingerprint Scans, ClassAction.org (Oct. 11, 2019), https://www.classaction .org/news/illinois-wendys-operator-hit-with-bipa-class-action-over-employee-fingerprint-scans [https://perma.cc/PSQ9-BCG6] (describing O'Sullivan v. All-Star, Inc., No. 2019CH11575, filed in the Circuit Court of Cook County, Illinois, on Oct. 7, 2019). Thirdparty vendors may also be liable to employees for failing to obtain consent. Figueroa v. Kronos, Inc., 454 F. Supp. 3d 772, 782 (N.D. Ill. 2020).

111. See, e.g., Tex. Bus. &Com. Code Ann. 503.001 (West 2019) (requiring consent for the capture of a biometric identifier and sale of biometric data, as well as reasonable care in storage and disposal, but without a private right of action); Wash. Rev. Code 19.375.020 (2019) (regulating use of biometric data in commercial databases and foregoing a private right of action).

112. See Fair Credit Reporting Act of 1970, 15 U.S.C. 1681b(b)(1)-(3), 1681m; see also N.Y. Fair Credit Reporting Act, N.Y. Gen. Bus. L. 380-b (2020) (regulating the use of credit reports).

113. 15 U.S.C. 1681a(d)(1).

114. See Pauline T. Kim &Erika Hanson, People Analytics and the Regulation of Information Under the Fair Credit Reporting Act, 61 St. Louis Univ. L.J. 17, 20 (2016) ("[A]lthough employers face significant liability risks if they disregard the statute's requirements, the FCRA in fact does little to curb invasive data collection practices or to

address the risks of discriminatory algorithms.").
115. See, e.g., Ark. Code Ann. 11-2-124 (2019); Cal. Labor Code 980 (2019); Colo. Rev. Stat. 8-2-127 (2019); 820 Ill. Comp. Stat. 55/10 (2018); La. Rev. Stat. Ann. 51:1953 (2018); Md. Code Ann., Lab. &Emp. 3-712 (2019); Mich. Comp. Laws 37.273 (2018); Nev. Rev. Stat. 613.135 (2019); N.H. Rev. Stat. Ann. 275:74 (2018); N.J. Stat. Ann. 34:6B-5 (2019); N.M. Stat. Ann. 50-4-34 (2019); Okla. Stat. tit. 40, 173.2 (2018); Or. Rev. Stat. 659A.330 (2019); 28 R.I. Gen. Laws 28-56-3 (2018); Tenn. Code Ann. 50-1-1003 (West 2019); Utah Code Ann. 34-48-201 (West 2019); Wash. Rev. Code 49.44.200 (2019); Wis. Stat. 995.55 (2019). Roughly half of the states had such legislation under consideration. See Access to Social Media Usernames and Passwords, Nat'l Conf. of State Legislatures (July 1, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013. aspx [https://perma.cc/6X5P-KVFA].
116. See, e.g., Mass. Gen. Laws ch. 151B, 4(9), (9A) (2018); see also Dallan F. Flake, Do Ban-the-Box Laws Really Work?, 104 Iowa L. Rev. 1079, 1079 (2019) (providing empirical examination of ban-the-box laws).
117. 42 U.S.C. 12112(d)(3)(B); 42 U.S.C. 2000-ff(a).
118. Security Breach Notification Laws, Nat'l Conf. of State Legislatures (July 17, 2020),<https://www.ncsl.org/research/telecommunications-and-information-technology /security-breach-notification-laws.aspx> [https://perma.cc/8PX7-DFTS].
119. HIPAA regulations require that covered entities "protect against any reasonably anticipated threats or hazards to the security or integrity" of protected health information. 45 C.F.R. 164.306(a)(2) (2020); 740 Ill. Comp. Stat. 14/5 (2008).
120. See Corona v. Sony Pictures Entm't, Inc., No. 14-CV-09600 RGK EX, 2015 WL 3916744, at ·1 (C.D. Cal. June 15, 2015) (class-action lawsuit filed against Sony Pictures for failing to prevent hack of 100 terabytes of employee data). The suit was settled. Assoc. Press, Sony Pictures Settles with Former Workers in Data Breach Lawsuit, Wall St. J. (Sept. 2, 2015, 8:49 PM ET), http://www.wsj.com/articles/sony-pictures-settles-with -former-workers-in-data-breach-lawsuit-1441241363 [https://perma.cc/VC32-W5TX]. But see Bodah v. Lakeville Motor Express, Inc., 663 N.W.2d 550, 558 (Minn. 2003) (finding no liability when social security numbers were faxed out to sixteen different business locations); Allison v. Aetna, Inc., No. 09-2560, 2010 WL 3719243 (E.D. Pa. Mar. 9, 2010) (dismissing complaint for lack of standing due to the absence of any injury in fact to employees after data breach).
121. Regulation 2016/679, of the European Parliament and of 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) (EU) [hereinafter GDPR]. An easily accessible version of the GDPR can be found at Intersoft Consulting, GDPR, https://gdpr-info.eu/. The GDPR is intended to protect "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data." Id. art. 1(2).
122. See, e.g., Anupam Chander, Margot E. Kaminski &William McGeveran, Catalyzing Privacy Law, 105 Minn. L. Rev. 1733, 1734 (2021) (noting that the GDPR "positioned the European Union as the world's privacy champion").
123. GDPR, supra note 121, art. 3(1) (applying to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not"); id. art. 4(2) (definingprocessing to mean "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction").
124. Id. art. 4(1) (defining personal data to mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person").
125. Id. art. 6. The GDPR lists a number of specified criteria for lawful processing of personal data. Id.

126. Id. Recital 43(1). Recitals are nonbinding but offer important guidance. See Margot E. Kaminski, The Right to Explanation, Explained, 34 Berkeley Tech. L.J. 189, 193-94 (2019) ("The GDPR consists of both text (Articles) and an extensive explanatory preamble. The preambular provisions, known as Recitals, do not have the direct force of law in the EU. . . . [T]hey are not binding law, but they are often cited as authoritative interpretations where the GDPR is vague.").
127. In its interpretive guidance of the GDPR as applied to the workplace, the Article 29 Working Party-the earlier title for the European Union agency responsible for data protection-stated that "for the majority of such data processing at work, the legal basis cannot and should not be the consent of the employees (Art [6](a)) due to the nature of the relationship between employer and employee." Article 29 Data Protection Working Party, Opinion 2/2017 on Data Processing at Work, 17/EN WP 249 (June 8, 2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=45631 [hereinafter WP Work Opinion]. The Article 29 Working Party is now known as the European Data Protection Board. GDPR, supra note 121, art. 68.
128. WP Work Opinion, supra note 127, at 7-8.
129. Id. at 10.
130. GDPR, supra note 121, art. 12.
131. Id. art. 13, 15.
132. Id. art. 16.
133. Id. art. 17(1). Exceptions apply for information that involves freedom of expression, public health, or research/archiving. Id. art. 17(3). The controller must also provide data subjects with the right to a portable version of the data, in a commonly-used and machine-readable format, when the processing is automated and conducted pursuant to the data subject's consent or contract. Id. art. 20.
134. Cal. Civ. Code 1798.140(o) (West 2020).
135. The California Privacy Rights Act of 2020, Proposition 24 (Cal. 2020). In March 2021 Virginia passed a consumer privacy statute similar to but less restrictive than the CCPA. Virginia Consumer Data Protection Act, H.B. 2307, S.B. 1392 (Va. Mar. 2, 2021), https://lis.virginia.gov/cgi-bin/legp604.exe?212+sum+HB2307; Cat Zakrzewski, Virginia Governor Signs Nation's Second State Consumer Privacy Bill, Wash. Post (Mar. 2, 2021 7:17 PM), https://www.washingtonpost.com/technology/2021/03/02/privacy -tech-data-virgina.
136. Cal. Civ. Code 1798.145(m)(1) (excluding personal information collected "by a business about a natural person in the course of the natural person acting as . . . an employee of . . . that business"). This exclusion is set to expire on January 1, 2023. Id. 1798.145(m)(4). The CCPA still requires the employer to provide notice of data collection to its employees; this notice must include the type of personal information collected and its intended use. See id. 1798.145(m)(3); 1798.100(b). And employers must adequately protect data they collect, as employees may bring suit in the event of a data breach. See id. 1798.145(m)(3); 1798.150(a)(1).
137. For example, relatively trivial information can reveal sensitive information such as whether an individual is pregnant or trying to conceive. In one example, Target used a wide variety of personal data-both generated by the store and purchased from external vendors-to develop consumer profiles including particular needs such as a pregnancy. Charles Duhigg, How Your Shopping Habits Reveal Even the Most Personal Information, N.Y. Times, Feb. 19, 2012, (Mag.), at 1. Employers have successfully developed similar profiles. Valentina Zarya, Employers Are Quietly Using Big Data to Track Employee Pregnancies, Forbes (Feb. 17, 2016), http://fortune.com/2016/02/17/cast light-pregnancy-data [https://perma.cc/TK37-YF3U].
138. Matthew T. Bodie, Miriam A. Cherry, Marcia L. McCormick &Jintong Tang, The Law &Policy of People Analytics, 88 Univ. Colo. L. Rev. 961, 1001-02 (2017). The U.S. government is restricted as to secondary uses of data. See, e.g., Privacy Act of 1974, 5 U.S.C. 552a(e)(3)(B). The FCRA does regulate use but its requirements are largely procedural. See Kim &Hanson, supra note 114, at 33 (arguing that the FCRA is "ill equipped to . . . curb the use of unfair or discriminatory algorithms").
139. FPF Expert's Guide, supra note 5, at 22.
140. See Calo, supra note 1, at 424 ("Why label the question of asymmetric access to data a 'privacy' question? I do

so because privacy ultimately governs the set of responsible policy outcomes that arise in response to the data parity problem.").
141. See id. at 423 ("Again, the privacy conversation has evolved to focus not on the capacity of the individual to protect their data, but on the power over an individual or group that comes from knowing so much about them.").
142. See Kaminski, supra note 126, at 191-92 (noting that the literature on AI in the United States "has been largely speculative, operating in a policy vacuum").
143. See, e.g., Pasquale, supra note 2, at 12-15; Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan. L. Rev. 1343, 1353 (2018) (arguing against companies invoking trade secret law to avoid scrutiny of their AI by criminal defendants).
144. Dillon Reisman, Jason Schultz, Kate Crawford &Meredith Whittaker, AI Now, Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability 16 (2018), https://ainowinstitute.org/aiareport2018.pdf [https://perma.cc /Y7V4-FWE2].
145. See, e.g., Huq, supra note 2, at 687 (arguing that a "well-calibrated machine decision maker may have underappreciated advantages that sound in dignity and autonomy terms").
146. GDPR, supra note 121, art. 12(1).
147. Id. Recital 71.
148. Id. art. 12(2).
149. Lee A. Bygrave, Article 22 Automated Individual Decision-Making, Including Profiling, in The EU General Data Protection Regulation (GDPR): A Commentary C.4.3, at 522, 537 (Christopher Kuner, Lee A. Bygrave &Christopher Docksey eds., 2020) (noting that Article 22's consent derogation "must otherwise be applied in light of the definition of consent in Article 4(11)").
150. Id. A, at 526 ("The travauxpréparatoires to the GDPR provide scant explanation of the rationale and policy underpinnings for Article 22.").
151. See, e.g., What Does the GDPR Say About Automated Decision-Making and Profiling?, U.K. Info. Comm'r's Off.,<https://ico.org.uk/for-organisations/guide-to-data -protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision -making-and-profiling/what-does-the-gdpr-say-about-automated-decision-making-and> -profiling [https://perma.cc/P5KP-JEJ8] ("Solely means a decision-making process that is totally automated and excludes any human influence on the outcome. . . . A process won't be considered solely automated if someone weighs up and interprets the result of an automated decision before applying it to the individual.").
For a discussion of "human in the loop" systems, see Ge Wang, Humans in the Loop: The Design of Interactive AI Systems, Stanford HAI (Oct. 20, 2019), https://hai.stanford .edu/blog/humans-loop-design-interactive-ai-systems [https://perma.cc/5VJC-TMTE] (discussing systems that incorporate human judgment within the process).

DETAILS

Subject:	Employers; Employees; Employment; Decision making; Artificial intelligence
Business indexing term:	Subject: Employers Employees Employment Artificial intelligence
Publication title:	ABA Journal of Labor &Employment Law; Chicago
Volume:	35
Issue:	2
Pages:	289-315

Publication year:	2021
Publication date:	2021
Publisher:	American Bar Association
Place of publication:	Chicago
Country of publication:	United States, Chicago
Publication subject:	Law
ISSN:	21564809
e-ISSN:	23294604
Source type:	Scholarly Journal
Language of publication:	English
Document type:	Journal Article
ProQuest document ID:	2583140249
Document URL:	http://eproxy.lib.hku.hk/login?url=https://www.proq uest.com/scholarly-journals/artificial-intelligence-challenges-workplace/docview/2583140249/se-2?accountid=14548
Copyright:	Copyright American Bar Association 2021
Last updated:	2022-10-16
Database:	ABI/INFORM Global,Research Library

LINKS