UC BERKELEY
LABOR CENTER

Center for Labor Research and Education
University of California, Berkeley

WORKING PAPER, TECHNOLOGY AND WORK PROGRAM | 11.17.20

Data and Algorithms in the Workplace: An Overview of Current Public Policy Strategies

Emlyn Bottomley

Contents

Introduction

This working paper provides an overview of existing and proposed public policy strategies designed to mitigate the risks and maximize the benefits of data processing systems[1] and algorithms at work.[2] Employers may use a multitude of technologies and techniques to monitor or otherwise collect data on their workforce. Through these methods they can collect a wide array of information on workers, including their location and movements,[3] computer activity,[4] health and wellness status,[5] co-worker interactions, biometric identifiers,[6] and social media activity.

The troves of data collected in the workplace – along with advances in the capacity of computers to store and process that data – have fueled innovations in the development of algorithmic technologies. These systems are often used to analyze worker data, make predictions or decisions about workers, influence or shape worker behaviors, plan and direct workplace tasks, train or assist workers in their job, or automate tasks entirely. In other words, algorithmic systems are used throughout a variety of operational areas to assist, augment, or automate work. For example, a Human Resources (HR) department may use predictive analytics to anticipate future staffing needs, screen or prioritize applicants with the assistance of an algorithmic system,[7] and score candidates' video interviews using emotion recognition technology. Algorithmic systems are fueled by data; as they become more widely adopted in the workplace, the imperative to collect granular, real-time, and continuous data similarly increases.

In some cases, employers implement algorithms that make or facilitate consequential employment-related decisions without any human oversight. These decisions may have significant impacts on workers' wages, benefits, hours, work schedules, hiring decisions, disciplinary actions, promotions, terminations, job content, and productivity requirements. While proponents maintain that algorithmic technologies are efficient and can mitigate human prejudices, critics argue that they are often unaccountable, dehumanizing, and can introduce new sources of bias. It is often difficult or impossible to determine how an algorithm arrived at its determinations, which is especially problematic when employers use these systems to make important decisions affecting hiring, work scheduling, promotions, or even discipling workers. Policy makers, academics, and advocates who are concerned about these issues are considering a variety of approaches to regulate the information systems and algorithmic technologies that employers use to collect and process worker data.

Policy makers at the federal, state and local levels have begun to respond to specific issues raised by data processing systems and algorithmic technologies.[8] Think tanks, academics, and advocacy groups have also advanced numerous policy proposals. These responses reflect varying approaches towards addressing the novel issues raised by data processing systems and algorithms. Some recommend technology-specific policies, such as moratoriums or bans on facial recognition technologies, while

others have proposed laws targeting particular issue areas, such as laws regulating the use of algorithmic systems in the criminal justice system. Another strategy focuses on addressing specific harms, such as erratic work schedules that are generated by algorithms. Although the majority of policies currently target government use of algorithms or focus on consumer privacy issues, many of these regulations could be adapted or applied to the workplace. In some cases, such as algorithmic bias, the workplace is one of the primary areas of concern.

This working paper provides an inventory of existing public policy strategies that have been developed to address the challenges of data processing systems and algorithms in the workplace. The policy elements presented here are organized into the following five groups:[9]

1. Notice and Transparency

Employers may collect data and implement algorithms without disclosing these practices to affected workers. For example, unbeknownst to its employees, Amazon used an algorithm to programmatically fire warehouse fulfillment center workers who failed to meet productivity targets.[10] When employers are not transparent about the systems they use, workers and their representatives are left with little recourse or ability to demand accountability. Notice and transparency policies aim to remedy this situation by requiring employers to provide workers with substantive information about their use of data processing systems and algorithmic technologies or periodically disclose such information to third-party auditors or government agencies.

2. Accountability

Although transparency is a necessary condition of accountability, it is insufficient to ensure that employers use data processing systems and algorithms responsibly. Unfortunately, employers may experience data breaches that reveal sensitive information about their workforce, including biometric identifiers, social security numbers, or bank account numbers.[11] These breaches may put workers at risk and cause harm to their personal lives.[12] Beyond the threat of data exposure, data processing systems and algorithms may hurt workers by invading their privacy, threatening their personal autonomy and dignity, and jeopardizing their health and safety. Policies that promote accountability require organizations to adequately safeguard workers' personal information and employ a risk-based approach to collecting data and using algorithmic systems.

3. Individual Data Rights

Providing workers with privacy rights over their own data is another approach to safeguard workers from emerging harms. Privacy rights allow individual workers to express agency over how their data are collected and used and establish limitations based on their personal preferences. Specifically, they may allow workers to consent or object to the collection, processing, or use of personal data; delete or correct inaccurate or misleading data; or access and transport data generated throughout the duration of their employment.

4. Workplace Rights

Data processing systems and algorithmic technologies used in the workplace may further harm workers by undermining established employment and labor laws. Algorithmic systems can produce outcomes that are biased against workers in protected classes, such as when Bon-Ton Stores, Inc. implemented a hiring algorithm that evaluated factors that are highly correlated with race.[13] Unfortunately, existing laws may be unable to provide redress for workers who are discriminated against by algorithmic systems.[14] Furthermore, the chilling effects of electronic monitoring technologies may inhibit workers from exercising their workplace rights, including engaging in protected concerted activity. For example, Walmart employs both traditional surveillance techniques and novel methods such as monitoring employees' social media activity, which serves to discourage workers from organizing or forming a union.[15] Policies promoting workplace rights attempt to bolster discrimination, employment, and labor laws to address the emerging or heightened challenges posed by data processing systems and algorithmic technologies.

5. Government Oversight and Regulation

Although notice and transparency, accountability measures, individual data rights, and workplace protections are important, they may be insufficient to address the collective harms created by data processing systems and algorithmic technologies. Individual workers may lack the time and expertise to exercise their rights or may fear retaliation. Furthermore, due to rapid developments in computing power, monitoring techniques, and artificial intelligence, protections that target specific technologies or practices may quickly become obsolete. Recognizing these challenges, some have advocated for expanding the powers of existing regulatory agencies or establishing new governance institutions to address the impacts of data-fueled technologies at work. These institutions may be given broad regulatory authority similar to the Food and Drug Administration (FDA), or vested with more limited powers, ranging from standards setting to apportioning liability.

Before proceeding, it should be noted that the purpose of this working paper is to provide a general overview of existing public policy strategies and proposals responding to data processing systems and algorithms in the workplace. This working paper does not address the role of worker voice in governing data and algorithms at work. Worker voice is a significant topic that deserves to be discussed in greater detail than can be afforded in this working paper. This working paper also does not attempt to analyze the efficacy of specific policies, nor does it advocate or recommend any particular strategy. In certain instances, along with a brief explanation, arguments for and against specific policies may be presented as they appear in the literature. This is solely for the purpose of familiarizing the reader with the debates surrounding certain issues.

1. Notice and Transparency

Policies that require notice and transparency regarding the collection and use of data are essential to individual informed decision-making, civic mobilization, and effective legislation. Without robust transparency measures and sufficient notice, it is difficult or impossible for workers, citizens, and policy makers to assess the risks and benefits of algorithms and data processing systems.

While transparency policies alone may be insufficient to adequately address the harms of emerging workplace technologies, they lay a foundation for more substantive policies. Information measures can be divided into two main groups: notice and transparency policies.

1.a Notice

Individuals and workers are often unaware of the presence, degree, and nature of employers' data processing and algorithmic systems. Furthermore, employers often do not provide an explanation of the intended purpose of these technologies. Notice policies are intended to provide individuals with information on how their personal data are collected, processed, and used.

Generally, these provisions compel organizations to notify individuals of the existence, purpose, scope, and likely outcomes of their data processing practices and their use of algorithmic systems. Some of these policies protect consumers and may or may not apply to workers, while other provisions are specifically intended to provide notice in the employment context. All of the general notice policies listed below have been enacted, while none of the employment-specific policies have been instituted.

Examples of enacted notice provisions that are not specific to the employment context include:

- Notice of data collection: Some countries and states require organizations that collect or process personal data to notify individuals when their personal data are either collected directly or obtained from a third party. The European Union's General Data Protection Regulation (GDPR)[16] creates obligations for organizations that collect, process, or use personal data to provide affected individuals with: (a) the identity of the entity that obtained the data, (b) the purpose and legal basis of processing the data, and (c) the types of individuals that may have access to the information.[17] The California Consumer Privacy Act (CCPA) compels organizations to inform individuals of the categories of information collected and the purposes for which they are used.[18] Washington and New Mexico have proposed legislation with similar notice provisions.[19]
- Notice of decisions made or assisted by algorithms: Some privacy regimes compel organizations to notify individuals when they are the subject of a decision that was made by or assisted by an algorithm. The GDPR instructs organizations that use decision-making algorithms to notify impacted individuals as to the existence and likely effects of the system.

Notice may only be required when these algorithms are used in specific contexts. For example, in Illinois, employers must provide notice and receive consent from job applicants prior to using "artificial intelligence" to evaluate video-recorded interviews.[20]

- Breach notifications: Breach notification policies compel organizations that process personal information to notify users when the security of their data has been compromised. Organizations may need to provide additional information to affected individuals, including: (a) how the data was exfiltrated, or exported;(b) what information was exposed; (c) the steps that the organization is taking to remedy the situation; (d) the steps the individual can take to better protect themselves; and (e) how to obtain further information. All 50 U.S. states have enacted some form of breach notification law.[21]

- Biometric notice requirements: Some states have enacted notice policies specific to biometric identifiers. Illinois, Texas, and Washington require organizations that collect or process the biometric identifiers of consumers or workers to provide prior notice and explain how the information is to be used.[22]

Some proposed employment-related notice provisions include:

- Notice of electronic monitoring or data collection: Electronic monitoring (EM) refers to the technologies and practices used by employers to observe the activities or communications of their workforce by any means other than direct observation. This may include through video cameras, keystroke or computer activity tracking software, email monitoring, or even GPS location trackers. Notice policies often require employers to inform employees of the: existence of EM practices; types of monitoring technologies used; types of information gathered; intended uses of information collected; and types of infractions that, if revealed through EM, will result in discipline.[23] The Center for Privacy and Technology at Georgetown has drafted model privacy legislation specific to the workplace that would require employers to provide notice of how and why they collect workers data, as well as how they plan to use it.[24]

- Indication of monitoring: Some advocates argue that employers should provide observed workers with a visual or aural cue signaling that surveillance is taking place. These indicators must be readily apparent during the time of active monitoring. Appropriate signals may include a visible light on a surveillance camera, a recorded message, or a pop-up on a computer screen.[25]

- Expansion of the "Fair Credit Reporting Act" to cover data brokers: The Fair Credit Reporting Act (FCRA) requires employers to obtain consent from job applicants prior to accessing their credit history or any "consumer report."[26] Furthermore, the employer must provide notice if an adverse employment action is taken based on the report. While the FCRA was originally intended to regulate credit agencies, some have argued that data brokers,[27] which similarly provide information on job applicants and employees, qualify as "Consumer Reporting

Agencies" and thus are covered under the Act. Advocates who take this position suggest that the Federal Trade Commission or Consumer Financial Protection Bureau should update its guidance to explicitly state that data brokers are considered consumer reporting agencies.[28]

- Disclosure of "software rules": Employers may use software to "algorithmically" manage employees. For example, software may assign shifts to workers, rate their performance, or set pay rates. The rules that guide algorithmic management tools may significantly affect the conditions of employment in ways that are similar to formal employment policies. Some advocates have argued that employers should provide workers with an easily understandable description of the logic used by software that makes or influences employment-related decisions.[29] For example, employers may need to include a description of how their timekeeping software works (including information on automatic break deductions and how the program rounds shift times) in an employee handbook.[30] While this may make sense for "by-hand" software that follows prescribed rules, it may be difficult for employers to document the logic used by machine learning algorithms.[31]

1.b Transparency

Transparency policies require organizations to disclose relevant information regarding their data processing systems and algorithmic technologies to third parties, government agencies, or the public. Employers may need to provide high-level qualitative information or even technical details, such as an algorithm's source code or training data. Transparency measures may also require disclosing employment-related information such as hours worked or sales data.

Advocates of algorithmic accountability argue that transparency is crucial to ensure that individual rights are not violated and verify that algorithms are functioning as intended. On the other hand, firms and some courts have maintained that algorithmic transparency may inhibit innovation by jeopardizing trade secrets and intellectual property.[32] Some have sought to strike a balance through "qualified transparency" measures that limit disclosures in order to balance the need for information with property rights and trade secrets concerns. In such a regime, transparency would mean disclosing only that information which is appropriate and proportionate to the risk level of the data processing or algorithmic system and the context in which it is used.[33] Although transparency measures may promote accountability and therefore overlap with other policies that require disclosures, such as impact assessments, the primary function of these transparency provisions is to inform stakeholders.[34]

All of the policies listed below have been proposed, but none have been enacted.

Examples of proposed transparency policies include:

- Disclosures to third parties: Organizations could be required to periodically submit qualitative and technical information related to their algorithmic systems to certified third-party auditors. These auditors would then inspect the algorithm's source code and training data in order to determine the likelihood it will produce biased or discriminatory outcomes.[35] These auditors may also provide certifications for algorithms that meet specified criteria. Scholars believe that disclosures to third parties would provide some limited transparency while preserving trade secrets and protecting intellectual property.[36]

- Qualitative public disclosures: Organizations that use or produce risky or highly impactful data processing or algorithmic systems could be required to provide qualitative information to the public, similar to disclosures required by the Securities and Exchange Commission (SEC). These disclosures may include substantive information about how the algorithm functions, its efficacy, and the errors it is likely to make. They would not include training data, code, or other technical details that could jeopardize trade secrecy.[37]

- Public disclosure of technical details: In cases where algorithmic systems are likely to produce significant risks to individuals, advocates believe that regulators should demand more substantial public disclosures.[38] In these cases, organizations would need to publicly disclose technical details such as an algorithm's source code and training data. These requirements would preempt trade secret protections.[39]

- Disclose employment data for online labor platform workers: In order to orchestrate and coordinate distributed workforces,[40] online labor platform or gig companies – such as Uber and TaskRabbit – collect extensive information on workers. This may include data on shift times, work history, employment dates, wages, hours, and workers' locations. Some have argued that labor platform companies should be required to share this information with the Internal Revenue Service or the Department of Labor. Researchers and worker organizations would be permitted to access and analyze the data, while regulators could use it to identify labor violations. However, since many platform workers are currently classified as contractors, they are not protected by wage and hour, collective bargaining, and anti-discrimination laws. Several municipalities and states, including California, New York City, Seattle, Washington, DC, and Chicago have instituted some form of information-sharing requirements for Transportation Network Companies such as Lyft and Uber.[41]

- Preempting trade secrets protections in litigation: Trade secrets protections may shield employers and software vendors from disclosing information relating to how an algorithmic system works during legal proceedings. This is especially problematic when employers use algorithms to make or assist in making decisions that have significant impacts on individuals' legal rights, financial circumstances, or employment prospects.[42] Without information on how an algorithm functions or the factors that it evaluates, workers may be unable to receive redress for employment and labor law violations resulting from its use. In the

criminal justice context, some lawmakers have proposed legislation that would preempt trade secrets protections when they prevent defendants from obtaining evidence to which they would otherwise be entitled. Courts may instead allow plaintiffs to discover crucial algorithmic evidence relevant to their case under a protective order. Similar protections could be enacted in the employment context to prohibit employers and software vendors from invoking trade secrets protections during litigation.[43]

2. Accountability

Algorithms and data processing systems are powerful tools that can substantially impact the lives and legal rights of workers. They often make, or assist companies with making, consequential employment-related decisions that impact wages, benefits, hours, work schedules, hiring decisions, disciplinary actions, promotions, terminations, job content, and quotas. Due to the potential for harm, advocates assert that organizations that collect, process, or use individuals' personal data have a special duty to protect the interests of those individuals.[44] In other words, these organizations should adhere to reasonable standards of accountability, responsible use, and security. These duties may include creating processes and safeguards to minimize risk and ensure responsible data stewardship.

Accountability measures expand upon transparency by requiring organizations to accept responsibility for their actions and take active measures to mitigate harms.[45] These policies outline the institutional arrangements, processes, and mechanisms necessary to ensure responsible data collection and use. Measures that foster accountability can both improve the ability of organizations to comply with regulations and increase the capacity of regulators to enforce them.

There are several categories of policy proposals focused on accountability: general principles and duties of responsible data stewardship, restrictions on the collection and use of sensitive data, data protection impact assessments (DPIAs), algorithmic impact assessments (AIAs), data protection officers (DPOs), and information fiduciary relationships. While most of these policies were envisioned as consumer data protections, they are often relevant to the workplace and could be expanded to regulate employer use of data processing systems and algorithms.

2.a General Principles and Duties of Responsible Data Stewardship

Policy makers in the European Union (EU) have recognized the duty of organizations that process or control personal information to abide by principles that promote the responsible use and stewardship of data. This duty may be even more necessary when there is an employment relationship that requires workers to disclose sensitive information. These principles are not prescriptive, and instead seek to embody the "spirit" of data protection laws.[46] While this ambiguity may weaken protections, it may also provide the flexibility necessary to address the challenges of

rapid technological change. Laws that are narrowly targeted on specific practices or technologies can quickly become obsolete as alternative techniques are developed, while broad principles may apply equally well to emergent technologies as methods that are currently in use.[47]

Although principles do not provide hard and fast rules, they can be legally enforceable. For example, organizations operating in the EU that fail to comply with the principles of the GDPR (listed below) may be fined up to the higher amount of €20 million ($22.5 million in USD) or 4% of their worldwide revenue.[48]

Examples of general responsible stewardship principles include:

- Purpose limitation: Purpose limitation principles prohibit organizations from collecting data unless it is for specific, legitimate, and clear purposes. Furthermore, data may only be processed to accomplish the specific purpose it was collected for and may not be further processed to accomplish another, incompatible goal.[49]

- Data minimization: Data minimization provides that organizations should only collect and process personal data that is relevant and limited to accomplishing a specific and legitimate purpose.[50]

- Data quality: Data quality requires organizations to take reasonable measures to ensure that the personal information that they collect and store is accurate and up to date. This may also entail promptly erasing or changing inaccurate data and implementing procedures for complying with individuals' requests to correct their personal information.[51]

- Storage limitation: Storage limitation refers to the principle that organizations should only keep data in a state that permits the identification of an individual for as long as is necessary to accomplish the purpose for which the data was originally collected.[52]

- Integrity and confidentiality: Integrity and confidentiality principles require organizations to implement and maintain appropriate technical and institutional safeguards to ensure the security of the personal information they collect and process. This may include protecting that data against unauthorized access and use, accidental loss, and destruction.[53]

- Appropriate safeguards for decision-making algorithms: Legislators can require organizations that use algorithms to make or assist in making decisions that affect an individual's legal status or rights, health, financial circumstances, reputation, employment opportunities, behavior, or choices to enact appropriate safeguards.[54] These may include periodically auditing the algorithm to ensure it is unbiased, using anonymization techniques, restricting data retention, and enacting data minimization policies.[55]

2.b Restrictions on the Collection and Use of Sensitive Data

Certain categories of personal data, such as biometric identifiers, health and medical information, and wellness data, are particularly sensitive and may require additional protective measures. Unauthorized or improper use or access to data in these categories poses substantial risks to the rights and wellbeing of workers.

Biometric identifiers are unique measurements of an individual's physical traits that can be used to identify them, such as fingerprints, facial geometry, gait, heartbeat, and retina scans. In the workplace, biometric devices (e.g., fingerprint scanners) are used for time tracking, security, or identity authentication. Unlike passwords, credit cards, or even social security numbers, biometric identifiers cannot be changed if they are stolen or otherwise compromised. Several states have enacted specific laws to regulate the collection, storage, sale, or use of biometric identifiers.[56] Other privacy legislation, such as the California Consumer Privacy Act (CCPA), includes stronger regulations on biometric identifiers in addition to broader data protections.

Health information refers to individually identifiable medical information such as past diagnoses, medical test results, and drug prescriptions. While health data are broadly protected under the Health Insurance Portability and Accountability Act (HIPAA), the Act generally does not apply to such information when it is held by employers.[57] Employers similarly have few limitations on how they can collect and use wellness data, which refers to information regarding the characteristics of an individual's lifestyle that may influence their health or wellbeing.[58] Wellness data includes but is not limited to information about daily activities, sleep patterns, time spent meditating, heart rate, and mood. This data can be used to infer a worker's sensitive and private health information or risk of developing a medical condition. Some employers even monitor workers menstrual cycles, raising fears that the collection of this data may result in discrimination.[59]

All of the biometric policies listed below have been enacted by a government entity. None of the wellness-related policies have been enacted.

Examples of enacted policies regulating the use of biometric data include:

- Consent: Consent policies require covered organizations to obtain consent prior to collecting, capturing, receiving, or disseminating biometric identifiers or other similarly sensitive data. In the workplace, employers may require workers to provide consent as a condition of employment.[60]

- Limitations on the use or sale of biometric data: Legislators can prescribe a limited set of acceptable or unacceptable uses for biometric identifiers. For example, the Illinois Biometric Information Privacy Act (BIPA) prohibits organizations from selling or otherwise profiting from an individual's biometric identifiers.[61]

- Standards of care for biometric data: Some legal regimes require organizations that store, transmit, or otherwise use biometric identifiers to exercise "reasonable care" with the data.[62] These organizations may also be obligated to treat biometric information as confidential and take certain precautions to protect this information.[63] Conversely, organizations could be held to a more stringent, "best efforts" standard, which requires them to take all reasonable steps, including everything that is necessary and proper, to ensure the integrity of biometric information.[64]

- Limitations on the retention of biometric identifiers: Some biometric laws require organizations that collect or process biometric data to establish and publish a biometric retention policy. In the policy, the organization must specify how long biometric identifiers will be stored and guidelines for destroying the biometric data after the initial purpose of collecting is accomplished. Organizations may also be required to delete biometric identifiers after a specified amount of time has elapsed.[65]

- Facial recognition bans and moratoriums: Some municipal governments have considered or enacted moratoriums or bans on the use of facial recognition technology by government agencies. Critics of the technology have focused on the potential for abuse by law enforcement agencies. In a San Francisco ordinance, city supervisors argued that the risks of facial recognition technologies to civil rights and liberties outweighed the benefits. Critics of facial recognition technology have argued that the technology is overly invasive, deeply flawed, and biased. Similar arguments could be applied to the use of facial recognition technology in the workplace.[66]

Examples of proposed policies that would regulate the use of health and wellness data:

- Expansion of HIPAA: HIPAA requires organizations that collect, process, or transmit health data to enact appropriate safeguards. HIPAA also holds organizations accountable for medical privacy violations. However, HIPAA only applies to health care entities and may not protect health information possessed by employers.[67] Some advocates argue that HIPAA should be amended to cover employers that collect, process, or otherwise use worker health data. Some of these advocates further suggest that HIPAA should be expanded to cover wellness information as well as health data.[68]

- Disclosure of wellness plan information: Workers who enroll in wellness plans may not receive adequate information about how their data will be collected, processed, and used. In some cases, data gathered through wellness programs can affect the insurance premiums paid by workers.[69] Some have suggested that employers, health care service plans, and insurers be required to provide workers with information concerning the scope of wellness data collection, how the data will be used, and their rights related to wellness programs under state and local law.[70]

- Restrictions on transmission of wellness data: Under current law, employers, wellness programs, and insurers can sell, share, or transmit wellness data without notifying affected workers or receiving their permission. Some have suggested barring organizations from sharing or transmitting wellness data unless they receive consent.[71] Alternatively, organizations that collect, process, or use wellness data could be restricted from sharing this information altogether.[72]

- Access, rectification, and deletion rights: Some have proposed requiring employers and wellness companies to delete wellness data upon the termination of an employment relationship or once a worker ceases to participate in a wellness plan. Furthermore, workers may be granted the right to access wellness data, challenge the veracity of the information, request a correction, or demand its destruction.[73]

- Prohibit adverse actions on the basis of wellness data: Due to the potential for discrimination, some have proposed that employers, health care service plans, and insurers be prohibited from taking adverse actions against workers based on wellness data or data gathered through a wellness plan. This would include information concerning an individual's decision to participate or stop participating in wellness programming. Adverse actions may include but would not be limited to increasing a premium on a policy, termination, demotion, fines, or suspension.[74]

- Wellness data minimization: Similar to general principles of data minimization, employers, health care service plans, and insurers could be required to limit the collection, transmission, retention, and use of wellness data to the minimum level necessary to operate the program.[75]

2.c Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a formal, evidence-based procedure used to assess the economic and social impacts of collecting and processing data.[76] Some jurisdictions require government agencies and private entities that control or process data to complete a DPIA prior to engaging in data processes that produce significant risks. In the European Union, organizations may even be required to conduct DPIAs when an information system impacts their workers.[77]

The primary function of a DPIA is to evaluate and analyze an information system's projected impact on an individual's rights or a community's wellbeing, assess alternatives to the system, and identify appropriate mitigation measures for anticipated harms. DPIAs may also assess whether or not safeguards adequately protect an individual's privacy. Advocates contend that impact assessments deter harmful projects and transform institutional decision-making as organizations accumulate knowledge and information sharing occurs between regulators and companies. Critics argue that

impact assessments are often ineffectual and create needless hurdles while failing to drive accountability.[78]

A DPIA may be released publicly, reviewed by a certified third party, or remain confidential. DPIAs required by the GDPR must include the components listed below.

Common components of Data Protection Impact Assessments (DPIAs) include:

- Systemic description: DPIA policies often require organizations conducting DPIAs to provide a detailed description of how they collect, store, and use personal information. As part of this description, organizations must specify the intended purpose of processing the data and justify their legitimate business interest in doing so.. In other words, this description should include details such as the nature, scope, context, and duration of data collection and processing activities.[79]

- Risk assessment: In order to complete a DPIA, organizations may be required to analyze the nature and severity of harms that could result from their use of data processing systems. Potential risks associated with data may include threats of unauthorized access, modification, or deletion of data. Certain practices may be associated with heightened risks, such as those that involve systematic monitoring, collection of sensitive data, integration of multiple data sets, collection of data on vulnerable subjects, novel data collection technologies, and transmission of data across national borders.[80]

- Proportionality assessment: DPIAs may require organizations that use highly risky data processing systems to formally assess the necessity of processing personal data relative to its purpose. In other words, they must weigh the societal benefits of a data processing system against its potential harms. In situations where organizations are unable to adequately mitigate the risks associated with their data processing systems, they may need to consult with, and receive approval from, the appropriate government oversight body before proceeding.[81]

- Risk mitigation measures: Where a risk assessment identifies potential risks, businesses may be required to specify and implement appropriate mitigation measures to minimize risks and protect the privacy rights of individuals. These may include internal processes,[82] technical safeguards, and post hoc remedies.

2.d Algorithmic Impact Assessments (AIAs)

Algorithmic Impact Assessments (AIAs) are similar to Data Protection Impact Assessments but focus on evaluating the economic and social impacts of algorithmic systems. In particular, AIA's are often discussed in the context of algorithms that make or assist in making consequential decisions that affect individuals. Advocates of AIAs argue that these systems are inherently risky, often biased, and

highly likely to infringe on individual rights. To address these risks, policymakers have proposed legislation requiring companies to conduct impact assessments on the algorithmic technologies they use.[83]

Advocates assert that AIAs serve important functions, such as informing workers about the potential impacts of algorithmic systems on their lives, increasing businesses' capacity to evaluate and procure algorithmic systems, ensuring greater accountability among firms that design and deploy these systems, and empowering affected individuals with meaningful opportunities to respond to and dispute the use of algorithmic systems.[84]

The policies listed below have been proposed in the US, but not enacted. Some of the components have been enacted in the EU as part of the GDPR.

Proposed components of the Algorithmic Impact Assessment (AIA) process include:

- Systemic description: Organizations that use algorithms to make or assist in making decisions may be required to provide a systemic description of the system. The description may include the following information:
    - Purpose: Organizations using algorithmic systems to make or assist in making decisions must provide information about the purpose of the system, including the specific problems it is attempting to address.[85]
    - Technical documentation: Organizations may be required to archive the data used to train the algorithm, document its technical architecture, and maintain a record of its past decisions. Organizations may also be required to document the algorithm's source code.[86]
    - Risk Level: Organizations may be required to identify the "high-risk" algorithms that they use. If the outputs of an algorithm significantly impact an individual's employment, financial, or legal circumstances, it may be considered a high-risk system. Depending on the risk level of the system, it may be subject to more or less oversight and regulation.[87] Some policies only require AIAs for high-risk algorithms.
    - Risk mitigation: When an impact assessment identifies a significant risk, the responsible organization may be required to document and implement appropriate safeguards to mitigate potential harms. These may include data minimization strategies, recourse processes,[88] limitations on data storage, internal controls,[89] and training programs for individuals who interpret the outputs of algorithms.[90]
- Assessment of impact: Advocates argue that AIAs help organizations evaluate whether the anticipated benefits of an algorithm that makes or assists in making decisions outweighs their societal costs or risks. AIA's often require an analysis of the following characteristics of the algorithmic system:

- Stakeholders: Organizations may be required to identify the communities, individuals, or social groups that will be impacted by the decisions that are made or assisted by the algorithm. In the workplace, this would mean identifying the workers, roles, or units that could be affected.[91]

- Proportionality: Organizations may also be required to assess the benefits and risks associated with an algorithmic system relative to its intended purpose. The evaluation should explicitly identify potential privacy and security harms as well as risks of inaccurate, unfair, biased, or discriminatory decisions that the algorithmic system could produce or enable.[92] The proportionality analysis may include a justification for why, in light of these risks, the algorithm will have a net positive impact. Additionally, the organization may need to evaluate alternatives to implementing an algorithmic system.[93]

- Human involvement: As part of the risk assessment, the organization may need to evaluate the degree of human involvement in the decision-making process and at what stages it takes place. For human oversight to be meaningful, it must be carried out by someone who has the authority and competency to understand and challenge the decision made or assisted by the algorithm.[94]

- Public comment period: Government entities that plan on using algorithms that make or assist in making consequential decisions could be legally required to hold a public comment period prior to procuring or implementing the system. This process would include publishing an AIA and holding public hearings to gather community feedback.[95] In the workplace, employers could be similarly required to establish a forum wherein workers can review an impact assessment and provide feedback.

- Challenge and judicial review: Some critics have pointed out that impact assessments often lack real force and merely establish a set of procedural "check boxes." Some experts have argued that individuals who are adversely affected by an organization's use of an algorithm should be granted the right to challenge the sufficiency of the relevant AIA.[96] Under this framework, courts would review the AIA and prohibit an organization from using an algorithmic system when appropriate.[97] This could be similar to the process established under the National Environmental Policy Act (NEPA), which requires federal agencies to conduct an Environmental Impact Assessment for actions that will have significant environmental consequences. Individuals who may be adversely impacted by the environmental consequences of an action are able to challenge either: (a) the agency's decision not to conduct an impact assessment;[98] (b) the adequacy of the impact assessment;[99] or, (c) the substantive merits of the agency's decision.[100] If the plaintiff's challenge is considered meritorious the court can issue an injunction blocking the action.[101] In the employment context, workers could similarly be given the right to challenge the implementation of problematic algorithmic systems that may adversely affect them.

- Meaningful access: While the prior elements of AIAs are designed to minimize the risks of algorithmic systems prior to implementation, it will often be impossible to fully anticipate and prevent all possible harms. In order to hold organizations accountable for unintended consequences, researchers or auditors could be allowed to access and study algorithms during an initial trial period and at regular intervals thereafter. The degree of access would depend on whether the organization is public or private and the anticipated risk associated with the algorithmic system. Auditors could either be allowed to publicize their report in order to promote transparency or be required to keep their findings confidential to protect trade secrets.[102]

2.e Data Protection Officers (DPOs)

Some argue that Data Protection Officers (DPOs) are necessary in order to drive accountability. A DPO is a senior level position at an organization that reports directly to the highest level of management regarding issues related to the collection, processing, or use of personal data. The primary function of a DPO is to assist organizations in complying with relevant data protection laws and safeguard the rights and interests of data subjects. DPOs should have extensive knowledge of data protection laws and the underlying technologies. Furthermore, they must have sufficient resources to adequately perform their job functions. They also must exhibit a high level of independence from the organization they are working for.[103]

The European Union requires companies, organizations, and governments to appoint a designated DPO. In the United States, many government agencies and corporations staff similar positions, especially if they operate within the EU.

Specific tasks that are required of DPO's:

- Monitor compliance: A DPO is required to identify the specific data processing activities that the organization engages in and monitor compliance with relevant laws. They also offer guidance and recommendations on best practices relating to data use and collection.[104]

- Advise and conduct DPIAs and AIAs: Entities that collect or process personal data are instructed to seek the advice of their DPO when considering whether or not to conduct a Data Privacy Impact Assessment (DPIA). DPOs advise the entity on the correct methodology for the impact assessment, whether or not to outsource the DPIA, appropriate safeguards to mitigate anticipated risks, and whether or not the organization's use of data is compliant with relevant regulations. DPOs may also be responsible for performing a DPIA or AIA and ensuring its adequacy.[105]

- Cooperate with relevant government entities: A DPO is responsible for collaborating with government entities regarding issues related to the collection, processing, or use of personal data. DPOs need to consult with relevant government entities[106] and receive

approval prior to the implementation of any "high risk" data processing or algorithmic system.[107]

- Record maintenance: DPOS must create and maintain a register of proposed and implemented data collection and processing activities. They are also required to disclose the registry upon request by an authorized government entity.[108]

2.f Information Fiduciaries

A fiduciary relationship is often established where a business arrangement necessitates trust and confidence, such as when a patient divulges sensitive health information to a doctor. Similarly, employers and other organizations that collect and process sensitive data may require similar levels of trust as commonly found in a fiduciary relationship.[109] Lawmakers have proposed legislation establishing "information fiduciary" duties for online service providers. The concept may also apply to employers that collect similar types of personal information from workers.[110] Some critics argue that these provisions will be inadequate to protect the rights of individuals because pre-existing fiduciary relationships between companies and their shareholders will take primacy over companies' fiduciary duties to consumers and workers.[111]

Some proposed obligations of information fiduciaries include:

- Duty of care: When individuals or entities have fiduciary responsibilities, they must act with competence and diligence so as not to harm the interests of the client. In the context of an information fiduciary, the duty of care could include protecting a consumer's or worker's privacy and facilitating their control over their personal data.[112]

- Duty of loyalty: Fiduciaries must act on behalf of their clients and refrain from creating conflicts of interest. This would prevent information fiduciaries from using a worker's or consumer's personal data in a manner that may result in a reasonably foreseeable harm or may be unexpected and highly offensive.[113]

- Duty of confidentiality: Information fiduciaries would also be barred from selling or disclosing identifying information when doing so would be in conflict with either the duty of care or the duty of loyalty. Furthermore, any third party to which the fiduciary transmits identifying information would be required to abide by the same duties of care, loyalty, and confidentiality.[114]

3. Individual Data Rights

Individual data rights grant workers autonomy over how their data are collected and used. These rights are widely believed to be foundational in ensuring that governments and private organizations respect and safeguard an individual's privacy. Although privacy is often thought of as the "right to be left alone," it can also entail an individual's right to control the use, sale, and collection of their personal information.[115]

Advocates have argued that privacy rights should extend to the workplace. Control over one's privacy requires an individual, in their role as a worker, to have the right to provide or withhold consent from the collection and processing of their personal information. It may also entail providing workers with the right to access and rectify personal data possessed by their employers. This may even extend to customer reviews, or "reputation data," which can have significant consequences for workers. Finally, general protections, such as anti-retaliation provisions, may be necessary to ensure that workers are able to adequately exercise their individual data rights.

3.a Consent

Consent policies give workers agency over whether their data are collected, processed, used, or disseminated. Under certain legal jurisdictions companies are required to receive workers' consent prior to using their personal data, and workers are able to revoke consent at any time.

Different policies require varying levels of consent. For example, Europe's General Data Protection Regulation (GDPR) require consent to be freely given, specific, informed, and unambiguous. Under the GDPR, a worker's consent alone may not provide sufficient justification for processing personal information due to the potential for coercion within an employment relationship.[116] Advocates argue that prohibitions on coercion or retaliation by employers are necessary in order to ensure that consent policies adequately safeguard individual data rights. For example, workers that are required to provide consent as a condition of employment are likely to acquiesce to extreme intrusions on their privacy.[117] All of the policies listed below have been enacted by a state or foreign government.

Some examples of consent policies include:

- General consent requirements: In Europe, companies are only permitted to process personal data when a worker or consumer provides consent for one or more specific purposes. Consent is only considered valid only if it is specific, informed, unambiguous, and given freely.[118] Individuals are allowed to withdraw their consent at any time. Under certain exceptional circumstances, however, business entities or governments are be allowed to process personal data without individual consent.[119]

- Right to restrict data processing: Under the GDPR, workers and consumers have the right to prohibit organizations that collect, store, or maintain their data from processing or otherwise using it. This right does not apply when the organization has an overriding reason for processing the data, such as complying with relevant laws.[120]

- Right to restrict data sales: Some privacy experts have advocated that companies be prohibited from selling personal data unless they receive consent from the worker or consumer. Under the California Consumer Privacy Act (CCPA), individuals have the right to direct companies to refrain from selling their data, or to "opt-out" of the sale. Furthermore, the CCPA requires companies to make opt-out mechanisms readily accessible.[121] In Europe, individuals are allowed to restrict the sale of personal information when it is used for specific purposes, such as marketing.[122] Others have proposed restraining employers from selling worker data altogether.[123]

3.b Access

Access policies allow workers and consumers to acquire information regarding the categories and contents of their personal data that an organization collects or processes. These policies may also include provisions specifying how often the data must be made available, and the format in which it is to be presented.

Access is a foundational component of other data rights, such as rectification and erasure, which cannot be exercised unless workers know the categories and contents of the personal information that an organization collects, maintains, or processes.[124]

Some examples of access policies include:

- Right to access: In some countries and states, workers and consumers have the right to access personal information that is under the control of an organization. Depending on the jurisdiction, the organization may need to provide the data itself, the categories of data, the organizations' purpose for processing the data, and any recipients of the data (when it is disclosed or transmitted to third parties).[125]

- Right to access and review employment data: Some have advocated that workers should have the right to access and review personal data that is collected, maintained, or processed by employers. This would cover data that is used for employment decisions, although certain categories of information may be exempted.[126] The employer would be required to provide personal data in a format that is understandable.[127]

3.c Rectification

Using inaccurate data for employment decisions produces significant risks to workers or job applicants. For example, a job applicant can be denied employment opportunities due to inaccurate information returned in a background check.[128] Advocates of rectification policies maintain that they are necessary to ensure data quality. Several data laws, including the GDPR and the CCPA,[129] recognize the importance of rectification and have established rights for individuals to correct or delete inaccurate information.[130]

Rectification policies often include provisions that allow workers to correct or delete personal information. In instances where algorithms are used to make or assist in making decisions, employers are required to provide an explanation for why a specific action was taken and establish procedures for workers to contest the decision.

Some examples of rectification policies include:

- Right to correct: In some jurisdictions, such as the European Union, workers may have the right to correct or complete inaccurate or misleading data.[131] The right to rectification does not apply when the data relates to subjective information or an opinion, such as a performance evaluation.[132] Under the GDPR, an organization makes an initial determination regarding whether a correction is warranted. If the data subject disagrees with the decision, they have the opportunity to appeal the decision to a neutral authority such as a court or administrative body. Some have argued that employers should be required to establish a grievance process whereby workers are able to contest the validity of, or add context to, personal data collected by their employer. If mutually agreed upon, the data would be amended or deleted. If the employer decides not to correct the data, they would be required to keep a record of the worker's request.[133]

- Right to erasure or deletion: Under the GDPR and CCPA individuals have the right to instruct an organization that stores or processes personal data to delete their information once the purposes for which it was originally collected have been fulfilled. Similarly, individuals may instruct a covered organization to delete data after they withdraw their consent. The organization may be exempted from these obligations if it has a legal duty to maintain or preserve the data or in certain exceptional circumstances.[134] The Center for Privacy and Technology at Georgetown has drafted model legislation explicitly guaranteeing the right to deletion for workers.[135]

- Right to explanation: In the European Union, individuals who are subject to decisions made or assisted by algorithmic systems have a right to explanation. This may include: (a) the purpose(s) of the algorithmic system, (b) the criteria or data used, (c) the source and relevance of the information, and (d) the likely consequences of the decision. The information must be provided in a form that is easily understandable to a lay person while detailed enough to allow impacted individuals to contest the automated decision.[136]

- Right to obtain human intervention: The GDPR provides consumers and workers the right to human intervention in highly impactful decisions. In other words, an algorithmic system may not be solely responsible for decisions that are likely to produce significant effects on workers. Significant effects include decisions that affect workers' financial circumstances, employment, or access to health services or education. Workers are also provided the right to challenge decision made with the assistance of an algorithmic system. When organizations communicate the results of a decision that was made or assisted by an algorithmic system, they are required to inform workers of these rights and refer them to an appeal process. Human involvement must be meaningful and undertaken by someone who has sufficient authority, discretion, and resources to review, change, or overrule the algorithmic system. Furthermore, the individual reviewing the algorithmic decision should have adequate expertise to understand the outputs of the algorithm.[137]

3.d Reputation Ownership

Reputation systems are often used by labor platform companies, such as Uber and Handy, to establish consumer trust. On certain platforms, they may have significant consequences for workers' livelihoods; a high rating can make the difference between a worker being banned from a platform and receiving additional work or better assignments. Furthermore, reputation systems may lock workers into one platform, limiting their mobility and reducing their employment options.[138]

Reputation data are often produced by customer reviews, which may include appraisals that are capricious, mistaken, or discriminatory.[139] Advocates have suggested a set of principles that could be used to regulate reputational systems.[140] None of these principles has been implemented.

Some proposed principles of reputation ownership include:

- Portability: A reputation system must be able to incorporate inputs from multiple labor platforms and should be accepted by any similar platform company.[141]

- Worker-controlled: The reputation system must be owned and maintained by worker-based organizations, such as a union or worker data cooperative,[142] rather than a private company. Workers themselves should have a say on important decisions related to how the reputation system functions.

- Transparent: Reputations must be transparent. Workers should be able to see their ratings and user comments in order to better understand their "reputation."[143]

- Reparable: Workers must be able to take certain steps, attend trainings, or be given the opportunity to accumulate positive reviews in order to repair their reputations.

- Resistant to bias and prejudice: Reputation systems must take steps to protect workers against bias and prejudice. This would include auditing ratings for discriminatory intent and expunging reviews when appropriate.

- Grievance procedure: Employers who use reputation systems must establish an appropriate grievance processes for workers who feel that reviews are inaccurate or unfair. Workers should be able to contest reviews and correct or delete them when appropriate.

3.e General Data Rights

General data rights safeguard and strengthen the protections listed above. For example, advocates believe freedom from retaliation is necessary to prevent companies from punishing workers for invoking their data rights. All of the policies listed below have been enacted by some state or national government.

Examples of general policies that promote data rights include:

- Freedom from retaliation: Under the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR), organizations are prohibited from retaliating against an individual or worker for exercising their data rights. Depending on the law, denying service, charging different rates, or reducing the quality of service can qualify as retaliation. In the employment context, retaliation could include employment-related decisions, such as consideration for promotion, work schedules, task assignment, and hiring and firing decisions.[144]

- Data portability: Individuals and workers protected by the CCPA and GDPR have the right to request and receive all of their personal information from an organization in a "structured, commonly used, and machine-readable format." They can also instruct the organization to transmit their personal data to another entity.[145]

- Authorized agents: Advocates believe that consumers and workers should be able to authorize a third party, such as a labor union or a non-profit, to act as their agent in exercising their privacy or data rights. They are concerned that individuals may lack the necessary resources to hold organizations accountable unless third parties may act as their agents for purposes of enforcing their rights. Authorized agents may be better suited than individual consumers or workers, to demand access to personal data, verify its accuracy, and request rectification. Critics of these proposals point out that such arrangements could create additional privacy concerns.[146] Although the GDPR does not provide an explicit right for individuals to delegate rights to a third party, some supervisory authorities expect organizations to comply with requests from an authorized agent.[147] The CCPA provides an explicit right for individuals to authorize a third party to act on their behalf.[148]

4. Workplace Rights

Policies that promote accountability, provide transparency, or grant individuals rights over their data can protect workers, mitigate potential harms, and ensure compliance with relevant laws. However, these measures may be insufficient to respond to the novel and heightened issues posed by new "algorithmic management" technologies. Just as labor practices that emerged out of the Industrial Revolution necessitated new workplace rights to safeguard the dignity, autonomy, and safety of workers, the proliferation of algorithmic technologies and data processing systems in the workplace may warrant the establishment of additional protections.

Some scholars contend that existing labor and employment laws are ill-suited to address the challenges posed by modern workplace technologies. Some legal protections, such as those afforded by Title VII of the Civil Rights Act[149] and the National Labor Relations Act (NLRA),[150] may need to be modernized to keep pace with technological developments. In addition, data processing systems and algorithmic technologies may necessitate new and innovative protections; for example, the rapid proliferation of inexpensive and invasive electronic monitoring technologies facilitates a previously unimaginable level of workforce monitoring.

Policies establishing workplace rights related to data processing systems and algorithms are often intended to address bias and discrimination, protect the right to organize, strengthen labor standards, and limit workplace surveillance.

4.a Bias and Discrimination

In the employment context, algorithmic technologies can be used extensively in the HR cycle – assisting with sourcing candidates, screening applicants, assessing interviews, evaluating performance, and predicting employee churn.[151] They may also be used throughout production processes to assign tasks or facilitate workforce scheduling. In many of these applications, the use of algorithmic systems may increase the risks of discrimination.

Algorithms that make or assist in making decisions can produce discriminatory outcomes due to the use of biased data, encoded values of their developers, technical errors or limitations, constraints introduced from algorithmic objectives, or inability of humans to fairly interpret the results.[152] As learning algorithms are often "trained" on historic data,[153] they can replicate historic patterns of discrimination, reproduce the biases of past decision makers, or encode societal prejudices.[154] Algorithms may produce discriminatory outcomes even when they do not explicitly evaluate an individual's protected class status or other sensitive characteristics.[155] Although AI practitioners are attempting to develop solutions, algorithmic bias remains a persistent issue and may be impossible to remedy with a technical fix.[156]

Existing anti-discrimination law may be largely ill-equipped to address the challenges of algorithmic bias. Some scholars have maintained that many algorithmic systems that produce discriminatory outcomes would not generate employer liability under existing Title VII law.[157] Some legal scholars and advocates have suggested policies to address algorithmic discrimination, but so far none have been adopted.

Some policies proposed to address algorithmic bias and discrimination include:

- Amend disparate impact standards: Some scholars are concerned that rote applications of existing anti-discrimination doctrine may fail to address workplace discrimination that occurs due to data-driven algorithms.[158] Disparate impact doctrine allows an employer to defend against a Title VII claim by demonstrating the existence of a correlation between an individual identity characteristic and job performance. Predictive analytics identify statistical relationships between variables regardless of whether the evaluated factor is causally related to job performance. This may result in employers discriminating against protected classes when they use decision-making algorithms that evaluate variables that serve as proxies for protected class characteristics, such as zip code. Some have suggested reforming disparate impact doctrine to better address the dangers of algorithmic bias. They argue that employers should be (a) required to prove that their algorithmic systems are free of bias and (b) demonstrate the "job-relatedness" of all factors that the algorithm evaluates. Advocates suggest that this could be accomplished by either amending Title VII of the Civil Rights Act or updating the Equal Employment Opportunity Commission (EEOC) guidelines.[159]

- Prohibit the use of proxy variables: Experts have pointed out that algorithmic systems can produce discriminatory outcomes if they evaluate "proxy variables", regardless of whether they explicitly consider protected class characteristics.[160] According to these scholars, removing protected class information may actually exacerbate discrimination by making bias more difficult to detect.[161] Some lawmakers have introduced legislation prohibiting predictive algorithms that influence employment decisions from using data that correlates with race or zip code.[162]

- Algorithmic discrimination audits: Some scholars argue that auditing algorithmic systems can mitigate the risk of discrimination.[163] Companies above a certain size would be required to conduct internal or third-party audits of the training data and outputs of algorithmic systems. The results of the audit may either be publicly disclosed or reported to an oversight body, such as the EEOC. Companies that discover bias in their algorithmic systems would need to take additional steps, such as repairing training data or refraining from using the system until it no longer produces discriminatory outcomes.[164] The New York City Council recently introduced an ordinance that would prohibit the sale of algorithmic systems that assist in hiring unless they are subject to an annual bias audit.[165]

4.b Right to Organize

Under the National Labor Relations Act, employees have a right to form a union and engage in concerted activity. It is illegal for employers "to interfere with, restrain, or coerce employees in the exercise of their rights."[166] Some employers, however, use a variety of methods to subvert these protections.[167] In the modern workplace, the growing sophistication of predictive analytics and the increasing prevalence of electronic monitoring technologies could further undermine workers' rights to organize.

Employers can use sentiment analysis or personality assessments to identify workers with attitudes and beliefs that are sympathetic towards unions. Predictive algorithms could increase these risks as they may allow employers to find correlations between seemingly unrelated variables in order to infer employees' likelihood of supporting a union. This could allow employers to effectively hide their anti-union bias in hiring, promotion, and termination decisions. Furthermore, the use of electronic monitoring technologies may exert a chilling effect that deters workers from organizing for fear of retaliation.[168]

Advocates have called for additional labor protections to safeguard workers' right to organize in light of the novel challenges posed by emerging workplace technologies. None of the policies listed below have been enacted.

Some policies proposed to protect the right to organize include:

- Restrict or ban pre-hire assessments and tests: Pre-hire tests may be used to assess applicants' skills, abilities, knowledge, job aptitudes, or personality traits.[169] However, these tests have also been used to screen out workers with pro-union sympathies.[170] Sophisticated algorithms may increase this risk, as they could be used by employers to predict a worker's stance towards unions based on their answers to seemingly unrelated questions. In order to protect the right to organize, advocates have argued that employers should be required to provide a clear business necessity for each question on a pre-hire assessment. The National Labor Relations Board (NLRB) could adopt similar guidance as the EEOC, which already requires employers to demonstrate the validity of pre-hire tests to defend against discrimination claims.[171] Alternatively, pre-hire tests and assessments could be banned altogether.[172]

- Limitations on engagement surveys: Companies may be able to identify departments, units, or workers that are likely to unionize based on employee engagement surveys. These surveys solicit employees' feedback on issues such as pay and benefits as well as employees' perceptions of the fairness, quality, and integrity of management. While employers may solicit this information in order to improve the workplace, they could also analyze survey responses to predict the likelihood of a union organizing drive.[173] Some have argued that employers should be required to prove that a questionnaire is not being used to identify

unionization vulnerabilities before issuing a survey. Alternatively, employee surveys could be prohibited altogether.[174]

- Surveillance as unfair labor practice: The National Labor Relations Board (NLRB) has recognized that workplace surveillance can give employers an unfair advantage in opposing unionization drives and may exert a chilling effect on organizing efforts due to fears of retaliation.[175] Under certain circumstances, the NLRB has ruled that surveillance may constitute an unfair labor practice.[176] However, legal standards established by the board to address in-person monitoring by supervisors may be insufficient to address the novel challenges to organizing posed by modern surveillance practices.[177] The NLRB could confront the chilling effects of electronic monitoring by classifying the most intrusive surveillance technologies as unfair labor practices, unless employers can prove that they are necessary to accomplish a legitimate business purpose. Alternatively, the NLRB might only allow employers to electronically monitor workers when (a) the employer can demonstrate a legitimate purpose for the monitoring and (b) workers cannot establish that the surveillance practice was deployed to inhibit concerted activity.[178]

4.c Wages, Hours, and Scheduling

Algorithmic technologies and data processing systems can assist employers in evading or avoiding wage and hour laws and can result in erratic scheduling.[179] Time-tracking software can include features that systematically under-report hours worked, which can lead to wage theft. Furthermore, sophisticated scheduling software allows employers to adjust staffing levels based on customer demand, which shifts the risks associated with variable demand onto workers. This may result in lower pay and more unstable schedules. Finally, the ubiquity of communication technology threatens to blur the distinction between working hours and off-duty time, as workers can now be expected to be accessible at all hours of the day.[180]

Scholars, advocates, and policy makers have responded to these issues in a number of ways. State and local politicians have often led the way in enacting policies that address harms like erratic scheduling practices. Some of the policies listed below have been enacted by state, city, or foreign governments. Others are still policy proposals.

Some examples of policies establishing new workplace standards include:

- Wage theft protections for time-tracking software: Algorithmic systems may be useful tools for standardizing employment practices and preventing employment law violations such as wage theft. Conversely, they may also undermine employment protections. Some reforms that could reduce the risks of wage theft include:
    - Eliminate shift rounding: Timekeeping software often allows employers to round shift times to the nearest quarter hour increment. In some cases, employers exploit

this function to save on payroll expenses. Some have suggested that employers be required to use non-rounded shift times for purposes of hourly compensation. Alternatively, lawmakers could regulate vendors by prohibiting time tracking software from providing rounding features.[181]

- Automatic break deductions: Some employers use timekeeping software to automatically deduct unpaid rest or break times from workers' hours. These deductions may occur whether or not the employee actually takes a break, or even if they are called back to work during their break. Overriding these deductions requires managerial approval which can intimidate workers who fear retaliation. This may result in under-compensation for worked hours. Some have argued that software vendors should be prohibited from offering automatic break deduction features.[182]

- Employer liability for software-related employment law violations: When employment law violations occur as a result of an employers' use of an algorithmic system, it may be unclear whether the employer or the vendor is liable. Advocates maintain that employers shouldn't be shielded from liability for employment law violations simply because of the software they use. They argue that courts should presume that employers know the likely effects of the software they use in the workplace when assessing liability. In instances where the use of software results in wage and hour violations, discrimination, or other employment law violations, the employer should be held liable as though the technology implements an employment policy.[183]

- Regulating scheduling: Companies increasingly use algorithmic systems to manage shift times and assist in workforce scheduling. Algorithmic systems may be used to anticipate customer activity based on historical sales data, the season, and the weather (among other factors) and adjust workers' schedules in real-time to match predicted demand. While this can help managers reduce labor costs, it can also result in erratic schedules, insufficient notice prior to shift changes, or inadequate rest periods between shifts.[184] State and local governments have responded to these concerns with a variety of policies, which are often called "Fair Workweek" laws. These policies are covered extensively elsewhere, but some key elements include:[185]

    - Businesses must provide employees with advanced notice of work schedules
    - Businesses must provide additional compensation to employees for unexpected shift changes
    - Employees must be given the right to decline added or lengthened shifts without reprisal

- Employees must be allowed minimum rest periods between shifts
- Employees must be given the right to request shift changes
- Employees who are called in during non-scheduled time must be guaranteed a specified number of hours
- Employers must pay employees who are sent home during regularly scheduled time a certain percentage of scheduled pay
- Employers must pay employees for a minimum number of hours, regardless of how many hours the employee actually works

In addition to expanding protections through state laws or worker campaigns, some scholars have recommended amending the Fair Labor Standards Act or modifying the Department of Labor's interpretation of "On-Call" time so that workers are compensated for the time they are on standby and may be called in.[186]

- Right to disconnect: Right to disconnect policies attempt to establish reasonable expectations for, and limitations on, the use of digital communications outside of the workplace or normal working hours. France's El Khomri laws require employers and employee representatives to bargain over expectations of digital responsiveness outside of work hours.[187] Several other countries have proposed similar laws, including Belgium, the Netherlands, Luxembourg, India, and Canada.[188] In New York City, a councilmember proposed an ordinance that would make it unlawful for employers to force employees to access work-related electronic communications outside of work hours, except in cases of emergency.[189]

4.d Limitations on Electronic Monitoring

The emergence of inexpensive and sophisticated electronic monitoring technologies has greatly increased the capacity of employers to observe their workforce. Some survey data indicates that workplaces are extensively and intensively monitored using a variety of surveillance methods.[190] Employers may electronically monitor their workforce for a number of reasons, including to defend against legal claims, ensure policy compliance, strengthen security, protect intellectual property and trade secrets, and monitor productivity or performance. Increasingly, electronic monitoring is used to generate the granular, real-time, and continuous data that enables employers to use algorithmic management systems.[191] While electronic monitoring may protect or benefit workers – such as when it is used to investigate toxic managers or claims of discrimination – it can also violate workers' privacy, autonomy, and dignity, create power asymmetries, and inhibit workers from organizing or invoking their legal rights. [192]

Workplace monitoring is legal unless a worker has "a reasonable expectation" of privacy, which generally does not exist in the workplace or when workers use equipment supplied by employers. While some states restrict highly invasive forms of electronic monitoring – such as cameras placed in a restroom – the privacy of workers is generally unprotected in the workplace.[193]

Workplace surveillance policies restrict the use of electronic monitoring technologies in the workplace. Strict limitations impose restrictions on where, when, or why monitoring technologies can be used. Contextual limitations create more flexible policy regimes that attempt to balance the business purpose of surveillance against the level of invasiveness.

Examples of policies establishing strict limitations on surveillance include:

- Limitations on the physical scope of electronic monitoring: Some have advocated for prohibiting electronic monitoring in specific, highly sensitive areas of the workplace. Some states have enacted laws that prohibit audio-visual surveillance in areas where employees may be partially or completely undressed, such as restrooms, locker rooms, or changing rooms.[194] Others have proposed restricting electronic monitoring in recreational areas, such as break rooms, lounges, and cafeterias.[195]

- Prohibit electronic monitoring of off-duty employees: In many cases, employers are permitted to monitor workers who are off-duty. Some have advocated for prohibiting monitoring outside of the workplace and limiting observation to work-related activities.[196]

- Limiting use of electronic monitoring data: In some cases, it is not the act of monitoring that is problematic, but how the data are used. Some have argued that employers should be prevented from using data gathered through electronic monitoring for any reason other than to accomplish narrow pre-specified purposes. Others advocate that employers only be permitted to use electronic monitoring data when protecting the legitimate interests of workers, such as ensuring workplace safety or preventing harassment and discrimination. In many cases, these policies would prohibit employers from using electronic monitoring data to evaluate employee performance or as a basis for disciplinary actions.[197] In Germany, employers are prohibited from monitoring employees in situations that do not involve a "concrete suspicion of a criminal violation" or a "serious breach of duty."[198]

Some proposed policies that establish contextual limitations on workplace surveillance include:

- Proportionality requirements: Some scholars have argued that electronic monitoring should be proportional to the legitimate business purpose that it is intended to accomplish. Less invasive technologies (like timekeeping software) could be used for a variety of business purposes, including defending against legal claims or conducting investigations. The most invasive technologies (such as wearable devices, internally facing dashboard cameras, or keystroke monitoring), however, would only be permitted for conducting an investigation into worker misconduct, and only after the employer completes an impact assessment.[199]

- Permissive use permits: Others have proposed strictly limiting the use of electronic monitoring technologies but allowing employers to petition a government agency for permission to use them for additional purposes. In this framework, electronic monitoring would only be permitted where no suitable alternatives are available to accomplish a legitimate business purpose. Monitoring employee performance would not be considered a legitimate purpose, and the company would bear the burden of proving that the surveillance practice is legitimate. Employers would be able to apply for a permissive use permit from the Secretary of Labor that would exempt them from some or all of the limitations outlined above.[200]

- Strengthen the legal standard for "Reasonable Expectation of Privacy": When determining whether an individual has a reasonable expectation of privacy, courts in the United States evaluate whether they (a) have exhibited an actual expectation of privacy and (b) that expectation is reasonable. Applying this test, courts have generally found that employees do not have a reasonable expectation of privacy in the workplace.[201] Some have suggested that US courts should adopt a stronger standard, such as the four factor conjunctive test the Canadian government uses to assess the legitimacy of surveillance.[202] This test considers: (a) whether the surveillance practice targets a specific need, (b) the probability that the practice will be effective in meeting the need, (c) the proportionality of the loss of privacy in relation to the gained benefit, and (d) the availability of a less intrusive method to achieve the goal.[203]

- Prohibit performance tracking systems that restrict employee rights: Some companies have implemented performance tracking systems in order to ensure that workers meet strict production quotas. In certain cases, these exacting quotas cannot be met if workers take breaks, use the bathroom, or even comply with basic safety precautions. Employers may make decisions such as promotions or even terminations based on performance in relation to these quotas. These policies and practices could undermine OSHA protections, such as those that prohibit unreasonable restrictions on bathroom access.[204] One method of addressing this issue would be to prohibit employers from making employment decisions based on performance tracking systems that abrogate employment laws or workplace protections.[205]

5. Government Oversight and Regulation

Governance policies move beyond a precautionary approach of mitigating the improper use of data and algorithms and delineate a framework for oversight of the technologies themselves. While all the policies included in this working paper could be thought of as governance strategies, these policies are differentiated by their focus on the creation of institutions with the authority to regulate data processing and algorithmic systems.

Some of the key responsibilities of governance institutions include setting standards, promulgating regulations, providing oversight, setting liability standards, and apportioning liability. While no federal, state, or local agency currently has broad jurisdiction over algorithmic or data processing technologies, existing agencies may have the ability to regulate these systems within specific domains.

5.a Standards-Setting Organizations

Some have suggested establishing an algorithmic Standards-Setting Organizations (SSO) with responsibility for coordinating and developing algorithmic classifications and design standards. SSOs are non-regulatory bodies that develop, revise, amend, interpret, or otherwise maintain technical standards. The National Institute of Standards and Technology (NIST) is one prominent example of an SSO.

Some advocates have argued that an algorithmic SSO should also make recommendations regarding liability apportionment and best practices.

Some proposed functions of an algorithmic standards-setting organization include:

- Classification: An SSO could create algorithmic classifications based on predictability, explainability, scale, types of outcomes, and general intelligence. For example, algorithms that follow predictable and understandable rules, operate on a limited scale, and are unlikely to have significant impacts on workers may be categorized as "low-risk." Algorithms producing results that are unexplainable, produce legal or similarly significant effects, and operate at a large scale may be categorized as "high-risk." The SSO may then recommend different performance, design, or liability standards depending on the classification.[206]

- Performance standards: An SSO may provide guidance on relevant performance standards based on an algorithm's intended use and risk classification. Standards could specify acceptable levels of accuracy and identify the types of errors that are unacceptable. Standards may be more stringent for algorithms that are classified as higher risk. The SSO could also certify algorithms that are compliant with relevant performance standards.[207]

- Design standards: The agency could establish measures of "explainability" to ensure that algorithmic outputs are understandable to lay people and issue guidance on how to develop algorithms that are compliant with specified standards. As scholars and experts develop ways of auditing and repairing algorithms with discriminatory potential, the organization could publicize and recommend best practices.[208]

- Liability standards and apportionment: The agency could develop liability standards and apportion liability for algorithmic harms among developers, implementers, distributors, and

end-users. The liability standards may differ depending on the algorithm's use case, industry, classification, and whether or not it has been certified by the SSO. [209]

5.b Regulatory and Oversight Bodies

Some advocates contend that dedicated regulatory agencies must be established to address the novel challenges associated with data processing systems and algorithms. Others have argued that these technologies are merely tools that should be overseen or regulated by existing agencies with relevant jurisdiction.

Regulatory and oversight regimes may vary based on their structure, political independence, jurisdiction, scope of authority, and enforcement powers. Some agencies may be able to promulgate regulations, while others may only be able to rely on judicial remedies.[210] The proposals listed here range from less restrictive oversight models, such as an advisory agency, to more forceful regulatory bodies. While specific functions are grouped by proposal, an agency may be vested with any combination of the responsibilities listed below.

Examples of proposed types of oversight or regulatory bodies include:

- Advisory agency: Occasionally, governments may establish advisory agencies or commissions when a policy area requires deeply specialized knowledge or technical expertise.[211] Some have advocated for establishing a "Federal Robotics Commission" with expertise in the field of algorithms, AI, and robotics. [212] While this institution would not have regulatory, enforcement, or investigatory authority, it could advise and inform agencies, legislative bodies, and state and local governments on issues related to algorithmic technologies. For example, the agency could advise the Equal Employment Opportunity Commission (EEOC) on hiring algorithms, and the Department of Labor (DOL) on the impacts of automation. The agency could consult with federal, state, and local lawmakers on relevant policy initiatives. Additionally, the agency could be granted discretion over allocating funds for research initiatives. The agency could also convene stakeholders from government, civic society, industry, and academia to discuss issues and publish reports related to data processing and algorithmic technologies.

- Algorithmic safety board: Governments often establish review boards when technologies or products pose a risk to public safety or wellbeing. Some of the responsibilities of these boards may include quality and safety inspection,[213] retrospective analysis of issues and accidents,[214] and planning oversight through supervising impact assessments.[215] Some have proposed creating an "Algorithmic Safety Board" vested with similar responsibilities.[216] The board could also administer and review Algorithmic Impact Assessments, and periodically investigate algorithms' training data, source code, and outputs.[217] The board would investigate instances where algorithms produce harm, publish incident reports, and provide

recommendations to agencies with regulatory powers. The board may could also assist other agencies with conducting investigations that demand technical expertise.

- Enforcement agency: An algorithmic oversight agency may act as an administrative enforcement body with jurisdiction over violations of statues that regulate algorithms. Similar to how the EEOC enforces the Civil Rights Act, this body may investigate or arbitrate disputes related to employers use of data processing systems and algorithms. The agency would also oversee administrative legal proceedings to provide remedies to affected individuals.[218] The agency could choose to represent plaintiffs in administrative or civil actions.[219]

- "FDA for algorithms": An algorithmic oversight body could also act as a "hard-edged" regulator by requiring software developers to demonstrate the safety and effectiveness of certain algorithms prior to implementation. The approval process could be modeled on the FDA, which prohibits the sale of certain medical products unless they meet exacting safety standards. Pre-market approval may only be necessary for the highest-risk algorithms such as those that operate at a large scale and make highly consequential decisions that affect employment, housing, or criminal justice.[220]

- Expand regulatory powers of existing agencies: Some experts believe that it would be a mistake to create a centralized regulatory or oversight agency with jurisdiction over all algorithmic systems. These individuals argue that, since algorithmic systems are used to accomplish a variety of purposes in a wide range of contexts, no one agency would have adequate subject area expertise or be able to effectively navigate the relevant regulatory frameworks.[221] Instead, these advocates would prefer a model where existing federal agencies oversee and regulate algorithms operating under their jurisdiction. For example, the DOL could regulate time keeping software, while the EEOC could regulate resume screening algorithms. Critics argue that each agency will lack sufficient expertise on algorithms to effectively regulate their use under this model.

5.c Liability for Algorithmic Harms

Some scholars argue that assigning liability for algorithmic harms to companies that collect, process, or use personal data may promote accountability and reduce labor and employment law violations. Organizations that are held liable for the harms created by the algorithmic technologies they use may evaluate software vendors more rigorously. Similarly, if software developers are concerned about liability, they may invest more resources in mitigating the risks of their products. The policies listed below provide an overview of proposed liability regimes.

Some proposals concerning assignment of liability for algorithmic harms include:

- Apportion liability to developers: One way of encouraging responsible software development is to apportion liability for algorithmic harms to the algorithm's developer. In the employment context, some software vendors have argued that they are not liable for employment law violations – including violations of Title VII of the Civil Rights Act – stemming from use of their software. The EEOC and other regulatory bodies overseeing enforcement could issue rulings clarifying that software vendors are liable for employment violations related to the use of their products. Apportioning liability to software developers could result in these companies better internalizing the societal costs of risky algorithmic systems and developing safer technologies.[222]

- Joint, joint & several, and proportional liability: When two parties are jointly liable, a plaintiff can recover the full amount of their damages from either party. When there is proportional liability, each party is liable for damages that are proportional to their fault in creating the harm. If vendors and employers are jointly and severally liable, a plaintiff may seek damages from any responsible party, who may then pursue compensation for damages paid in excess of their proportionate liability from the remaining defendants. In the employment context, there is joint liability for FLSA violations where a joint employment relationship has been established. Some legal scholars have suggested assigning proportional liability where algorithmic systems, such as those used by Autonomous Vehicles (AV), are employed.[223] Similarly, joint, proportional, or joint and several liability could be applied to employment violations that occur as a result of an employer using a third-party algorithm to make or assist in making employment-related decisions.[224]

- Strict liability: Under strict liability, employers would be required to prove that the algorithmic systems they use are unbiased. In order to receive redress, a worker would merely need to show that the employer's use of an algorithmic system resulted in an adverse employment action. If the employer is unable to prove that their system is free of bias, they may be held liable for any damages it produced.[225]

About the Author

Emlyn Bottomley is a graduate of the University of California at Berkeley (UC Berkeley) where he received his Masters of Public Policy. While at UC Berkeley he studied issues at the intersection of technology and employment. From 2019 through 2020 he worked as a technology researcher at the UC Berkeley Labor Center where he focused on the impacts of algorithmic systems and data processing technologies in the workplace. Prior to his graduate studies, Emlyn had worked for four years as an analyst at an Information and Communications Technology (ICT) company.

Acknowledgements

The author would like to thank Lisa Kresge for her guidance and feedback throughout the research and writing of this working paper as well as Reem Suleiman and Annette Bernhardt for their insights and advice.

This research was supported by a grant from the Ford Foundation.

Endnotes

[1] Data processing refers to any operation or set of operations performed on data including collection, storage, manipulation, alteration, transmission, dissemination, correction, use, or erasure. Data processing systems refer to the combination of hardware, software, organizations, people, and policies that execute or otherwise influence a data processing activity.

[2] An algorithm refers to a computational process for solving a problem or accomplishing a task. A basic algorithm can be outlined in code by a human programmer, using basic if-then logic for how the computer will perform a task. Alternatively, in the case of learning algorithms (often referred to as "machine learning algorithms" or "artificial intelligence"), programmers write code enabling the computer to develop its own rules for how to perform the task by leveraging statistical, mathematical, and computer science techniques on large data sets. The data sets that these algorithms analyze to develop a model is called "training data". Due to their complexity, it may be impossible for anyone, including a machine learning algorithm's creator(s), to understand how the algorithm determined the appropriate "rules." Although algorithms are technically a component of a data processing system, they will be referred to separately because they are associated with distinct harms which are often addressed in targeted policies. For more information on algorithmic systems, how they work, and how they are used, please see Data and Algorithms in the Workplace Part I

[3] This may include GPS location, acceleration and deceleration, and speed.

[4] Computer activity data may include data such as browsing history, email contents, keystrokes, and time spent idle.

[5] Employers may offer workplace "wellness" programs in order to promote health, decrease the risk of disease, and lower insurance costs. These programs may collect information such as heart rate, exercise history, and sleep patterns. Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *Calif* 105 (2017): 735.

[6] Biometrics refers to the intrinsic physical or behavioral characteristics that can be used to verify an individual's identity. Examples of biometric identifiers include facial and palm geometry, gait, voice tone, and iris measurements. See "Biometrics." *Electronic Frontier Foundation*. accessed June 3, 2020 https://www.eff.org/issues/biometrics.

[7] Algorithmic systems include "decision-making algorithms" which are also often referred to as Automated Decision Systems (ADS). While there is universally agreed upon definition of decision-making algorithms or ADS, they generally refer to "[a]any software, system, or process that aims to automate, aid, or replace human decision-making. Automated decision systems can include both tools that analyze datasets to generate scores, predictions, classifications, or some recommended action(s) that are used by agencies [organizations] to make decisions that impact human welfare and the set of processes involved in implementing those tools." Richardson, Rashida. *Confronting Black Boxes: A Shadow*

Report of the New York City Automated Decision System Task Force, AI Now Institute. December 4, 2019. https:// ainowinstitute.org/ads-shadowreport-2019.html.

[8] While there have been several high-profile federal proposals addressing issues raised in this working paper, the majority of legislation that has actually been enacted was implemented at the state and local level.

[9] Some policies that have been proposed or enacted comprises elements in multiple categories. For this reason, specific policies may be referenced in multiple places throughout this inventory.

[10] Employees learned of the system only once it was revealed through a labor dispute. Lecher, Colin. "How Amazon Automatically Tracks and Fires Warehouse Workers for 'Productivity.'" *The Verge*, April 25, 2019. https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.

[11] Porter, Jon. "Huge Security Flaw Exposes Biometric Data of More than a Million Users." *The Verge*, August 14, 2019. https://www.theverge.com/2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data ; Whittaker, Zack. "Chegg Confirms Third Data Breach since 2018." *TechCrunch*, April 29, 2020. https://social.techcrunch.com/2020/04/29/hackers-chegg-employee-breach/ ; Stahie, Silviu. "Interserve Hit by Data Breach; 100,000 Employee Records Stolen." *Security Boulevard*, May 15, 2020. https://securityboulevard.com/2020/05/interserve-hit-by-data-breach-100000-employee-records-stolen/

[12] "Kaspersky Finds 30% of IT Security Managers Missed Important Personal Events Due to Data Breaches." accessed May 22, 2020 https://usa.kaspersky.com/about/press-releases/2020_do-you-care-about-your-companys-reputation-and-employee.

[13] Bon-Ton Stores used an algorithmic system developed by Kenexa to screen job applicants. Among the factors it considered was how far the applicant lives from work. While this may seem like a facially neutral variable, its correlation with race or ethnicity may result in it acting as a "proxy variable" for protected categories. Williams, Betsy Anne, Catherine F Brooks, and Yotam Shmargad. "How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications." *Journal of Information Policy* 8 (2018): 78–115 ; Walker, Joseph. "Meet the New Boss: Big Data." *Wall Street Journal*, September 20, 2012, sec. Management. https://www.wsj.com/articles/SB10000872396390443890304578006252019616768.

[14] Pauline T. "Data-Driven Discrimination at Work." *Wm* 58 (2016): 857.

[15] Berfield, Susan. "How Walmart Keeps an Eye on Its Massive Workforce." *Bloomberg*, November 24, 2015. http://www.bloomberg.com/features/2015-walmart-union-surveillance/.

[16] In 2018, the European Union (EU) enacted the General Data Protection Regulation (GDPR), which is considered to be among the strongest set of data protections in the world. The GDPR generally applies to personal information, or data that is capable of being used to identify a person, and organizations that collect, process, maintain, or use that data. For more information on the history of GDPR, its scope, and its key provisions, see "What Is GDPR, the EU's New Data Protection Law?" *GDPR.EU*, November 7, 2018. https://gdpr.eu/what-is-gdpr/.

[17] Regulation (EU) 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) *OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)* ELI: http://data.europa.eu/eli/reg/2016/679/oj

[18] The California Consumer Privacy Act (CCPA) establishes data protections for California consumers and imposes responsibilities on companies that buy, sell, collect, process or otherwise use personal data. The CCPA was signed into law on June 28th, 2018 and went go into effect on January 1st, 2020. California Consumer Privacy Act, Cal.Civ.Code § 1798.100 (United States California)

[19] Washington Privacy Act of 2019, W.A. Senate SSB-6281, W.A. Senate (66th Legislature Sess. 2019); Consumer Information Privacy Act of 2019, N.M. Senate SB 176 (54th Legislature Sess. 2019).

[20] Artificial Intelligence Video Interview Act of 2019, I.L. General Assembly HB 2557 (101st General Assembly Sess. 2019); Regulation (EU) 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) *OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)* ELI: http://data.europa.eu/eli/reg/2016/679/oj

[21] "Security Breach Notification Laws." *National Conference of State Legislatures*, March 8, 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[22] Biometric Identifiers, RCW 19.375 (United States Washington); Capture or Use of Biometric Identifier, V.T.C.A., Bus (United States Texas); Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/15 (United States Illinois).

[23] Privacy for Consumers and Workers Act of 1993, U.S. House of Representatives H.R.1900, U.S. House of Representatives (103rd Congress Sess. 1993); Notice of Electronic Monitoring Act of 1999, U.S. House of Representatives H.R. 4908, U.S. House of Representatives (106th Congress Sess. 1999).

[24] "The Worker Privacy Act: Discussion Draft." *Georgetown Law Center on Privacy and Technology.* 2019. https://drive.google.com/file/d/1Mi1JTezFbmTdJg2Fbp_MreFuSTWQ5QmK/view

[25] "Through the Keyhole: Privacy in the Workplace, an Endangered Right." *American Civil Liberties Union*. accessed June 30, 2020 https://www.aclu.org/other/through-keyhole-privacy-workplace-endangered-right.

[26] Under the FCRA, a consumer report means "any 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;" Fair Credit Reporting Act, 15 U.S.C.A § 1681a

[27] "Data brokers are entities that collect information about consumers, and then sell that data (or analytic scores, or classifications made based on that data) to other data brokers, companies, and/or individuals. These data brokers do not have a direct relationship with the people they're collecting data on, so most people aren't even aware that the data is even being collected." Grauer, Yael. "What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?" *Vice*. accessed July 2, 2020 https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.

[28] Kim, Pauline T, and Erik A Hanson. "People Analytics and the Regulation of Information Under the Fair Credit Reporting Act." *Louis ULJ* 61 (2016): 17. Kim

[29] This may include decisions that impact wages, benefits, hours, work schedules, performance evaluations, hiring decisions, disciplinary actions, promotions, terminations, job content, productivity requirements, workplace health and safety, and the right to organize.

[30] Alexander, Charlotte S, and Elizabeth Tippett. "The Hacking of Employment Law." *Mo* 82 (2017): 973.

[31] See note 2 for a description of the difference between "learning algorithms" and "by-hand" software and the challenges of explainability

[32] Pasquale, Frank. *The Black Box Society*. Harvard University Press. 2015.

[33] Tutt, Andrew. "An FDA for Algorithms." *Admin* 69 (2017): 83.

[34] While Impact Assessments (IAs) may require public or limited disclosures, the primary purpose of an IA is to ensure that organizations properly evaluate the risks and benefits of projects or decisions with significant effects and mitigate the harms. In the case of IAs, disclosures are ancillary to these primary goals. For more information on IAs see Data Protection Impact Assessments (DPIAs) p. 14 and Algorithmic Impact Assessments (AIAs) p. 15

[35] Source code refers to the text that makes up an executable program. Training data refers to the initial dataset used to enable a learning algorithm to understand the data and to develop its own rules for how to perform a task or accomplish a goal. For more information on how an algorithms source code or training data may produce biased outcomes see Barocas, Solon, and Andrew D Selbst. "Big Data's Disparate Impact." *Calif* 104 (2016): 671.

[36] Tutt, Andrew. "An FDA for Algorithms." *Admin* 69 (2017): 83

[37] Tutt, Andrew. "An FDA for Algorithms." *Admin* 69 (2017): 83

[38] Lawmakers in Europe have indicated that decisions which affect a person's financial status, health, reputation, access to services or other economic or social opportunities are likely to be considered significant. For example, an algorithmic system that makes or assists hiring decisions is likely to produce significant risks as it directly impacts an individual's economic opportunities.

[39] Tutt, Andrew. "An FDA for Algorithms." *Admin* 69 (2017): 83

[40] Distributed workforces refer to geographically dispersed workers that do not operate in a traditional offices

[41] Sinroja, Ratna. "Review of state and city level requirements on data sharing for Transport Network Companies (TNCs)", UC Berkeley Labor Center, unpublished; Rogers, Brishen. "Fissuring, Data-Driven Governance, and Platform Economy Labor Standards." *SSRN Journal*, 2017. https://www.ssrn.com/abstract=3057635 ; Mobility devices: personal information of 2019, C.A. Assembly AB 3116, C.A. Assembly (2019)

[42] In State v. Loomis, 2016 WI 68, 371 Wis. 2d 235, 881 N.W.2d 749 the Wisconsin Supreme Court ruled that the developers of an algorithmic risk-assessment tool (COMPAS) did not need to reveal relevant information describing how the algorithm calculated risk due to trade secrets protections. The defendant in the case, Eric Loomis, was sentenced to six years in prison.

[43] Justice in Forensic Algorithms Act of 2019, U.S. House of Representatives H.R.4368, (116th Session Sess. 2019).

[44] Balkin, Jack M. "Information Fiduciaries and the First Amendment." *UCDL Rev.* 49 (2015): 1183.

[45] Koene, Ansgar, Chris Clifton, Yohko Hatada, Helena Webb, and Rashida Richardson. *A Governance Framework for Algorithmic Accountability and Transparency*, European Parliamentary Research Service. 2019. https://www.europarl.europa.eu/stoa/en/home/highlights.

[46] "The Principles." Information Commissioner's Office. ICO. April 30, 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.

[47] For example, several municipalities have enacted, or are considering facial recognition moratoriums. These protections may be fleeting however, as technologists are rapidly developing new methods for identifying individuals at distance based on unique characteristics, such as their gait or heartbeat. Schneier, Bruce. "Opinion | We're Banning Facial Recognition. We're Missing the Point." *The New York Times*, January 20, 2020, sec. Opinion. https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html.

[48] "The Principles." Information Commissioner's Office. ICO. April 30, 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.

[49] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[50] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[51] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[52] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[53] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[54] "What Does the GDPR Say about Automated Decision-Making and Profiling?" Information Commissioner's Office. ICO. June 14, 2019. 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/.

[55] WP29 (Article 29 Data Protection Working Party). "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679," 2016; Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[56] Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/15 (United States Illinois); Biometric Identifiers, RCW 19.375 (United States Washington); Capture or Use of Biometric Identifier, V.T.C.A., Bus (United States Texas)

[57] Depending on the type of medical information, how it is collected, and how it is used, employers may be regulated under a number of statutes including HIPAA, Genetic Information Nondiscrimination Act (GINA), the Americans with Disabilities Act (ADA), the Family and Medical

Leave Act (FMLA), and relevant state and local laws. For more information on medical privacy rights in the workplace, see https://www.workplacefairness.org/medical-privacy-workplace (Riggs, 2018)

[58] Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *Calif* 105 (2017): 735.

[59] Harwell, Drew. "The Pregnancy-Tracking App Ovia Lets Women Record Their Most Sensitive Data for Themselves — and Their Boss." *The Washington Post*, April 10, 2019. https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?arc404=true.

[60] Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/15 (United States Illinois); Biometric Identifiers, RCW 19.375 (United States Washington); Capture or Use of Biometric Identifier, V.T.C.A., Bus (United States Texas)

[61] Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/15 (United States Illinois)

[62] Organizations that are subject to a reasonable standard of care may be liable for negligence if they fail to exhibit "[t]he degree of care (watchfulness, attention, caution, and prudence) that a reasonable person should exercise under the circumstances." See https://www.nolo.com/dictionary/standard-of-care-term.html

[63] Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/15 (United States Illinois); Biometric Identifiers, RCW 19.375 (United States Washington); Capture or Use of Biometric Identifier, V.T.C.A., Bus (United States Texas);

[64] In the United States, courts are inconsistent in their interpretations of the differences between the "best efforts" and "reasonable care" standards. While "best efforts" sometimes denotes a higher standard of care, "best efforts" and "reasonable care" may also be used interchangeably. Hirshberg, Brian, and Alex Speyer. "Contractual Standards: Distinctions Without A Difference?" *Mayer Brown*, 2018. https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2018/08/on-point--contractual-standards-distinctions-witho/files/on-point-contractual-standards/fileattachment/on-point-contractual-standards.pdf.

[65] Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/15 (United States Illinois); Biometric Identifiers, RCW 19.375 (United States Washington); Capture or Use of Biometric Identifier, V.T.C.A., Bus (United States Texas);

[66] Cameron, Dell. "We Don't Need to 'Pause' Police Use of Face Recognition—We Need to Ban It Forever." *Gizmodo*, May 22, 2019. https://gizmodo.com/we-dont-need-to-pause-police-use-of-face-recognition-we-1834958605. ; Acquisition of Surveillance Technology, San Francisco, Mun. Code Ch. 19B (United States California 2019); Commercial Facial Recognition Privacy Act of 2019, U.S. Senate S.847, U.S. Senate (116th Congress Sess. 2019).

[67] HIPAA only applies to healthcare plans, healthcare clearinghouses, and "healthcare providers that electronically transmit certain health information." HIPAA may apply to self-funded insurance plans operated by employers but will not apply to health data contained "in employment records held by a covered entity in its role as an employer." HIPAA will apply to data transmitted from a covered entity to an employer. Riggs, Kelly. "What All Employers Need to Know About Protecting Employee Health Information." *Ogletree Deakins*, March 20, 2018. https://ogletree.com/insights/what-all-employers-need-to-know-about-protecting-employee-health-information.

[68] Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *Calif* 105 (2017): 735.

[69] The West Virginia teacher strikes of 2018 were partially catalyzed by the mandatory enrollment of educators in an invasive wellness program, Go365. The teachers' insurance premiums were tied to how many "wellness" points they earned through the program. Go365 was cancelled after significant backlash and worker strikes. Solow, Lena. "The Scourge of Worker Wellness Programs." *The New Republic*, September 2, 2019.

[70] Lane, Megan. *Assembly Labor And Employment Re: Wellness Programs*, California Legislative Analyst. 04/15/19. https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200AB648.

[71] Wellness Program Protection Act of 2019, AB 648, C.A. Assembly (Sess. 2019).

[72] Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *Calif* 105 (2017): 735.

[73] Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *Calif* 105 (2017): 735; Wellness Program Protection Act of 2019, AB 648, C.A. Assembly (Sess. 2019).

[74] Wellness Program Protection Act of 2019, AB 648, C.A. Assembly (Sess. 2019).

[75] Wellness Program Protection Act of 2019, AB 648, C.A. Assembly (Sess. 2019).

[76] DPIAs borrow from the impact assessment framework, which is widely used for environmental impact reports (EIRs) and Policy Impact Assessments (PIAs). EIRs are often required for projects that may have significant environmental effects and PIAs may be required for highly consequential policy decisions. Petersen, Grant, Simon McMenemy, Danielle Vanderzanden, and Stephen Riga. "A GDPR Update for Employers,

Part III: Preparing Required Data Protection Impact Assessments." *Ogletree Deakins*, May 2, 2019. https://ogletree.com/insights/a-gdpr-update-for-employers-part-iii-preparing-required-data-protection-impact-assessments/.

[77] While private companies operating in the United States are not currently required to conduct DPIAs, federal agencies must conduct privacy impact assessments prior to implementing or changing technologies that collect, maintain, or disseminate personally identifiable information (E-Government Act, 2002)

[78] Pope, Jenny, Alan Bond, Angus Morrison-Saunders, and Francois Retief. "Advancing the Theory and Practice of Impact Assessment: Setting the Research Agenda." *Environmental Impact Assessment Review* 41 (2013): 1–9; Ortolano, Leonard, and Anne Shepherd. "Environmental Impact Assessment: Challenges and Opportunities." *Impact Assessment* 13, no. 1 (1995): 3–30.

[79] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[80] WP29 (Article 29 Data Protection Working Party). "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679," April 4, 2017; Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[81] "Necessity & Proportionality." *European Data Protection Supervisor*. accessed July 2, 2020 https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en; WP29 (Article 29 Data Protection Working Party). "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679," April 4, 2017; Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[82] Internal processes designed to mitigate risk may include approval processes for sensitive requests, establishing data access permission sets, conducting internal audits, and other similar procedural controls.

[83] According to the EU's guidelines on DPIAs, impact assessments are required when algorithmic systems make or assist in making decisions that impact workers. WP29 (Article 29 Data Protection Working Party). "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679," April 4, 2017; Algorithmic Accountability Act of 2019, U.S. Senate S. 1108, U.S. Senate (116th Congress Sess. 2019).

[84] Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability." *AI Now Institute*, 2018, 1–22.

[85] Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability." *AI Now Institute*, 2018, 1–22.

[86] Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability." *AI Now Institute*, 2018, 1–22.

[87] Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability." *AI Now Institute*, 2018, 1–22.; Algorithmic Accountability Act of 2019, U.S. Senate S. 1108, U.S. Senate (116th Congress Sess. 2019).

[88] For more information on recourse processes, see the section on "Individual Data Rights" p. 29

[89] See note 82

[90] Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability." *AI Now Institute*, 2018, 1–22; Algorithmic Accountability Act of 2019, U.S. Senate S. 1108, U.S. Senate (116th Congress Sess. 2019).

[91] Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability." *AI Now Institute*, 2018, 1–22.

[92] Algorithmic Accountability Act of 2019 of 2019, U.S. Senate S. 1108, U.S. Senate (116th Congress Sess. 2019).

[93] Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability." *AI Now Institute*, 2018, 1–22.

[94] WP29 (Article 29 Data Protection Working Party). "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679," 2016.

[95] Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability." *AI Now Institute*, 2018, 1–22.

[96] An organization's use of an algorithmic system may be challenged if the organization fails to conduct an AIA when legally required to do so or if the AIA is critically flawed. An AIA may be considered critically flawed if it fails to, "rigorously explore and objectively evaluate all reasonable alternatives", "devote substantial treatment to each alternative", consider the alternative of "no action", or "include appropriate mitigation measures." Furthermore, courts may evaluate whether the organization appropriately balanced the costs against the benefits and prohibit the use of the decision-making algorithm if the harms outweigh the benefits. Selbst, Andrew D. "Disparate Impact in Big Data Policing." *Ga* 52 (2017): 109.

[97] Jacobsen, Kenneth A. "Environmental Law-Judicial Review Under NEPA," 1978; Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability." *AI Now Institute*, 2018, 1–22.

[98] If an agency determines that a proposed action does not merit an impact assessment due to its insignificant effects, adversely impacted individuals may be able to challenge the agencies "threshold determination." Jacobsen, Kenneth A. "Environmental Law-Judicial Review Under NEPA," 1978

[99] An AIA is likely to be considered adequate if, "is prepared with objective good faith and contains sufficient information to enable the decisionmaker to fully consider and balance environmental factors." Jacobsen, Kenneth A. "Environmental Law-Judicial Review Under NEPA," 1978

[100] In the context of NEPA courts may only challenge the substantive merits of an agency's decision if was conducted in bad faith or if the cost-benefit analysis gave insufficient weight to environmental factors. Jacobsen, Kenneth A. "Environmental Law-Judicial Review Under NEPA," 1978

[101] While NEPA only applies to federal agencies, the California Environmental Quality Act (CEQA) creates a judicial review process for private actions that may similarly result in a court ordered injunction.

[102] Reisman, Dillon, Jason Schultz, Kate Crawford, and Meredith Whittaker. "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability." *AI Now Institute*, 2018, 1–22.

[103] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[104] WP29 (Article 29 Data Protection Working Party). "Guidelines on Data Protection Officers ('DPOs') 2016/243," 2016.

[105] WP29 (Article 29 Data Protection Working Party). "Guidelines on Data Protection Officers ('DPOs') 2016/243," 2016; Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[106] The government agency tasked with overseeing the monitoring and compliance of relevant laws will vary depending on the regulatory regime. For more information on proposed governance frameworks see section "Government Oversight and Regulation" on p. 34

[107] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[108] WP29 (Article 29 Data Protection Working Party). "Guidelines on Data Protection Officers ('DPOs') 2016/243," 2016.

[109] Balkin, Jack M. "Information Fiduciaries and the First Amendment." *UCDL Rev.* 49 (2015): 1183.

[110] Data Care Act of 2018, U.S. Senate S. 3744, U.S. Senate (115th Congress Sess. 2018)

[111] Khan, Lina, and David E Pozen. "A Skeptical View of Information Fiduciaries." *Harv* 133 (2019): 497.

[112]Data Care Act of 2018, U.S. Senate S. 3744, U.S. Senate (115th Congress Sess. 2018); New York Privacy Act of 2019, N.Y. Senate S5642, N.Y. Senate (2019th-2020 Legislative Session Sess. 2019); Balkin, Jack M. "Information Fiduciaries and the First Amendment." *UCDL Rev.* 49 (2015): 1183.

[113] Data Care Act of 2018, U.S. Senate S. 3744, U.S. Senate (115th Congress Sess. 2018); New York Privacy Act of 2019, N.Y. Senate S5642, N.Y. Senate (2019th-2020 Legislative Session Sess. 2019); Balkin, Jack M. "Information Fiduciaries and the First Amendment." *UCDL Rev.* 49 (2015): 1183.

[114] Data Care Act of 2018, U.S. Senate S. 3744, U.S. Senate (115th Congress Sess. 2018); New York Privacy Act of 2019, N.Y. Senate S5642, N.Y. Senate (2019th-2020 Legislative Session Sess. 2019).

[115] California Consumer Privacy Act, Cal.Civ.Code § 1798.100 (United States California)

[116] The GDPR guidelines further elaborate that, "Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees…due to the nature of the relationship between employer and employee." WP29 (Article 29 Data Protection Working Party); "Consent | General Data Protection Regulation (GDPR)." *Gdpr-Info.Eu*. accessed July 2, 2020 https://gdpr-info.eu/issues/consent/

[117] Moore, Adam D. "Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy." *Business Ethics Quarterly*, 2000, 697–709.

[118] "Consent | General Data Protection Regulation (GDPR)." *Gdpr-Info.Eu*. accessed July 2, 2020 https://gdpr-info.eu/issues/consent/

[119] (Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[120] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[121] California Consumer Privacy Act, Cal.Civ.Code § 1798.100 (United States California)

[122] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[123] "The Worker Privacy Act: Discussion Draft." *Georgetown Law Center on Privacy and Technology.* 2019.
https://drive.google.com/file/d/1Mi1JTezFbmTdJg2Fbp_MreFuSTWQ5QmK/view

[124] "Right of Access | General Data Protection Regulation (GDPR)." *Gdpr-Info.Eu*. accessed July 2, 2020 https://gdpr-info.eu/issues/right-of-access/.

[125] California Consumer Privacy Act, Cal.Civ.Code § 1798.100 (United States California); Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj; "The Worker Privacy Act: Discussion Draft." *Georgetown Law Center on Privacy and Technology.* 2019. https://drive.google.com/file/d/1Mi1JTezFbmTdJg2Fbp_MreFuSTWQ5QmK/view

[126] For example, data regarding an ongoing investigation may be withheld from the worker in order to ensure the integrity of the inquiry.

[127] Levinson, Ariana R. "Carpe Diem: Privacy Protection in Employment Act." *Akron L. Rev.* 43 (2010): 331; "Through the Keyhole: Privacy in the Workplace, an Endangered Right." *American Civil Liberties Union*. accessed June 30, 2020 https://www.aclu.org/other/through-keyhole-privacy-workplace-endangered-right; "The Worker Privacy Act: Discussion Draft." *Georgetown Law Center on Privacy and Technology.* 2019. https://drive.google.com/file/d/1Mi1JTezFbmTdJg2Fbp_MreFuSTWQ5QmK/view

[128] Melendez, Steven. "When Background Checks Go Wrong." *Fast Company*, November 17, 2016. https://www.fastcompany.com/3065577/when-background-checks-go-wrong.

[129]California Consumer Privacy Act, Cal.Civ.Code § 1798.100 (United States California); Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[130] Under the Fair Credit Reporting Act, individuals are able to dispute inaccurate information contained in consumer reports, such as credit reports or background checks. However, the burden of correcting credit reports falls on consumers and the process is difficult. Consumers wishing to dispute their credit report must carefully and consistently monitor their score and notify the credit agency if they identify an issue. The credit agency then may investigate the claim and determine if the information is accurate. If the credit agency decides to take no action, there is no appeal process and the agency may disregard future requests from the consumer as frivolous. While consumers can pursue judicial remedies, they must prove the agency's negligence and show concrete damages. Thrasher, Edward. "The Fair Credit Reporting Act: Deficiencies and Solutions." *Temp. Pol. & Civ. Rts. L. Rev.* 21 (2011): 599.

[131] Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[132] In the case of a disputed opinion, the record must at least show that the data reflects an opinion and attribute it to the appropriate source when appropriate. "Right to Rectification." *Information Commisioner's Office*. ICO. August 12, 2019. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/
[133] Levinson, Ariana R. "Carpe Diem: Privacy Protection in Employment Act." *Akron L. Rev.* 43 (2010): 331; "Through the Keyhole: Privacy in the Workplace, an Endangered Right." *American Civil Liberties Union*. accessed June 30, 2020 https://www.aclu.org/other/through-keyhole-privacy-workplace-endangered-right; "The Worker Privacy Act: Discussion Draft." *Georgetown Law Center on Privacy and Technology.* 2019. https://drive.google.com/file/d/1Mi1JTezFbmTdJg2Fbp_MreFuSTWQ5QmK/view

[134] California Consumer Privacy Act, Cal.Civ.Code § 1798.100 (United States California)

[135] "The Worker Privacy Act: Discussion Draft." *Georgetown Law Center on Privacy and Technology.* 2019. https://drive.google.com/file/d/1Mi1JTezFbmTdJg2Fbp_MreFuSTWQ5QmK/view

[136] WP29 (Article 29 Data Protection Working Party). "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679," 2016; Kaminski, Margot E. "The Right to Explanation, Explained." *SSRN Journal*, 2018. https://www.ssrn.com/abstract=3196985.

[137] WP29 (Article 29 Data Protection Working Party). "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679," 2016; Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[138] Moving to a new platform may require a worker to spend significant time rebuilding their reputation, during which they may lose work and earnings. This may inhibit workers from freely moving to competing platforms, even when they could earn more. Lack of portable reputation systems may contribute to the monopsony power of entrenched labor platform companies (Kelly, 2017).

[139] Mateescu, Alexandra, and Aiha Nguyen. "Explainer: Algorithmic Management In The Workplace." *Data & Society*, 2019. https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf

[140] Scholz, Trebor, and Nathan Schneider. *Ours to Hack and to Own: The Rise of Platform Cooperativism, a New Vision for the Future of Work and a Fairer Internet*. OR books. 2017.

[141] For example, a rideshare driver should be able to transfer their Uber reputation data to Lyft.

[142] One possible model for a worker owned reputation system is Driver's Seat, a driver-owned data cooperative that allows gig workers to pool trip data to better understand how to increase earnings. For more information see https://www.driversseat.co/

[143] This right may be limited in order to ensure the privacy, confidentiality, and safety of specific users,

[144] California Consumer Privacy Act, Cal.Civ.Code § 1798.100 (United States California); Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[145] California Consumer Privacy Act, Cal.Civ.Code § 1798.100 (United States California); Regulation (EU) 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)
OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
ELI: http://data.europa.eu/eli/reg/2016/679/oj

[146] Privacy for Consumers and Workers Act of 1993, U.S. House of Representatives H.R.1900, U.S. House of Representatives (103rd Congress Sess. 1993); Todolí-Signes, Adrián. "Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection." *Transfer* 25, no. 4 (2019): 465–8; Levinson, Ariana R. "Carpe Diem: Privacy Protection in Employment Act." *Akron L. Rev.* 43 (2010): 331

[147] "Asking someone to act on your behalf." Information Commissioner's Office. ICO. October 25, 2020. https://ico.org.uk/your-data-matters/data-protection-and-journalism/asking-someone-to-act-on-your-behalf/

[148] California Consumer Privacy Act, Cal.Civ.Code § 1798.140 (y) (United States California);

[149] Title VII of the civil rights act prohibits employment discrimination on the basis of race, religion, color, national origin, sex, sexual orientation, and gender identity. Title VII protects against disparate treatment, or explicit discrimination, and disparate impact where superficially neutral employment practices have discriminatory effects. Bogen, Miranda, and Rieke Aaron. *Help Wanted: An Exploration of Hiring Algorithms, Equity and Bias*, Upturn. 2018. https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf

[150] The NLRA codifies the rights of employees to form a union and engage in concerted activity to advance their interests. Sections 7 and 8(a)(1) of the NLRA prohibit employers from interfering with these rights.

[151] Holtom, Brooks, and David Allen. "Better Ways to Predict Who's Going to Quit." *Harvard Business Review*, August 16, 2019;
Bogen, Miranda, and Rieke Aaron. *Help Wanted: An Exploration of Hiring Algorithms, Equity and Bias*, Upturn. 2018.
https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf

[152] Kim, Pauline T. "Data-Driven Discrimination at Work." *Wm* 58 (2016): 857; Bogen, Miranda, and Rieke Aaron. *Help Wanted: An Exploration of Hiring Algorithms, Equity and Bias*, Upturn. 2018. https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf

[153] Learning algorithms construct models based on analysis of large "training data sets" of past information. However, "since many social patterns related to education and work reflect troubled legacies of racism, sexism, and other forms of socioeconomic disadvantage," algorithmic systems run the risks of reflecting and perpetuating these flaws. Bogen, Miranda, and Rieke Aaron. *Help Wanted: An Exploration of Hiring Algorithms, Equity and Bias*, Upturn. 2018. https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf

[154] Barocas, Solon, and Andrew D Selbst. "Big Data's Disparate Impact." *Calif* 104 (2016): 671.

[155] Under Title VII, employers may not discriminate against an employee on the basis of their race, color, religion, sex, national origin, or sexual orientation. For more information on how algorithms can discriminate against employees even when they do not explicitly evaluate these characteristics see Mann, Gideon, and Cathy O'Neil. "Hiring Algorithms Are Not Neutral." *Harvard Business Review*, December 9, 2016. https://hbr.org/2016/12/hiring-algorithms-are-not-neutral.

[156] For more on how predictive algorithms or decision-making algorithms can produce discriminatory outcomes, see "Big Data's Disparate Impact" and "Understanding Discrimination in the Scored Society." (Hao, 2017)

[157] Barocas, Solon, and Andrew D Selbst. "Big Data's Disparate Impact." *Calif* 104 (2016): 671.

[158] Kim, Pauline T. "Data-Driven Discrimination at Work." *Wm* 58 (2016): 858

[159] The EEOC is the Federal agency tasked with enforcing Title VII of the Civil Rights Act; Kim, Pauline T. "Data-Driven Discrimination at Work." *Wm* 58 (2016): 857; Bogen, Miranda, and Rieke Aaron. *Help Wanted: An Exploration of Hiring Algorithms, Equity and Bias*, Upturn. 2018. https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf

[160] Proxy variables are factors that serve as "mere 'stand-ins' for protected groups, such as zip codes as proxies for race (i.e. redlining), and height and weight as proxies for gender." (Zarsky, 2014). Sophisticated machine learning algorithms may be able to identify more subtle proxies for protected class status.

[161] Williams, Betsy Anne, Catherine F Brooks, and Yotam Shmargad. "How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications." *Journal of Information Policy* 8 (2018): 78–115

[162] Limit Predictive Analytics Use of 2019, HB3415, I.L. House of Representatives (Sess. 2019).

[163] These measures share similarities with some of the transparency and accountability interventions described above. However, they would be narrowly targeted at evaluating the potential for bias and discrimination.

[164] Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *Calif* 105 (2017): 735.

[165] Sale of automated employment decision tools, New York City Council Int. No. 1894, New York City Council (2020).

[166] "Interfering with Employee Rights (Section 7 & 8(a)(1))." *National Labor Relations Board*. accessed July 1, 2020 https://www.nlrb.gov/about-nlrb/rights-we-protect/the-law/interfering-with-employee-rights-section-7-8a1.

[167] Von Wilpert, Marni. "Union Busters Are More Prevalent than They Seem, and May Soon Even Be at the NLRB." *Working Economics Blog*, 2017.

[168] Newman, Nathan. "UnMarginalizing Workers: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace." *Available at SSRN 2819142*, 2016.

[169] Some examples of pre-hire tests commonly used in selection processes are physical ability tests, aptitude tests, personality tests, and honesty and integrity tests. "Screening by Means of Pre-Employment Testing." *Society for Human Resource Management*, September 10, 2018. https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/screeningbymeansofpreemploymenttesting.aspx.

[170] It is illegal under Section 8(a)(3) of the National Labor Relations Act (NLRA) to refuse to hire workers due to their feelings towards unions. However, employers may refuse to hire an employee based on the results of a pre-hire assessment as long as the test does not explicitly ask about union sympathies. Newman (2016) notes that many assessment companies advertise their services by implying that they can help weed out potential pro-union employees while carefully avoiding any explicit anti-union screening. Newman, Nathan. "UnMarginalizing Workers: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace." *Available at SSRN 2819142*, 2016.

[171] According to the "Uniform Employee Selection Guidelines Interpretation and Clarification" issued by the Equal Employment Opportunity Commission (EEOC) employers may be liable for Title VII disparate-impact discrimination claims based on their use of pre-hire tests. To avoid liability, employers are advised to document that the test accurately measures job-related factors by demonstrating validity. The EEOC has approved three forms of validity: "Content validity is appropriate when a job analysis defines a job in terms of the important behaviors, tasks or knowledge required for successful performance, and the assessment or test is a representative sample of those behaviors, tasks or knowledge (e.g., a typing or mathematics test, or an exam for certified public accountants)… Criterion-related validity relates to a test's ability to predict how well a person will perform on the job. The desired KSAOs[knowledge, skills, abilities and other characteristics] for job performance are the "criterion variables." Tests, or predictors, are then devised and used to measure different job dimensions of the criterion variables. "Tests" may include having a college degree, scoring a required number of words per minute on a typing test or having five years of medical transcription experience. These predictors are then validated against the criteria used to measure job performance, such as supervisor appraisals, attendance and quality of work performed… Construct validity refers to the extent to which a selection device measures a particular "construct" that, according to a job analysis, underlies the successful performance of the job in question. Typical constructs include intelligence, honesty, dependability and mechanical comprehension." "Screening by Means of Pre-Employment Testing." *Society for Human Resource Management*, September 10, 2018. https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/screeningbymeansofpreemploymenttesting.aspx.

[172] Newman, Nathan. "UnMarginalizing Workers: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace." *Available at SSRN 2819142*, 2016.

[173] Engagement surveys may also be referred to as "employee satisfaction surveys", "engagement audits." When they are explicitly intended to identify the likelihood of unionization they are often called "vulnerability surveys." Union-avoidance consultants, like the Labor Relations Institute (https://lrionline.com/about-lri/) offer vulnerability surveys as part of their risk mitigation services. Some large companies, like the

Amazon owned grocery store Whole Foods, have developed proprietary systems that combine "team member sentiment" data gathered through employee surveys with data on "external risks," and "store risks," to identify stores that are likely to unionize. Peters, Jay. "Whole Foods Is Reportedly Using a Heat Map to Track Stores at Risk of Unionization." *The Verge*, April 20, 2020. https://www.theverge.com/2020/4/20/21228324/amazon-whole-foods-unionization-heat-map-union.

[174] Newman, Nathan. "UnMarginalizing Workers: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace." *Available at SSRN 2819142*, 2016.

[175] The NLRB is the federal agency tasked with enforcing labor law established under the NLRA. Specifically, it is tasked with overseeing union elections, investigating charges of NLRA violations, facilitating settlements, deciding cases, and enforcing orders. The NLRB may also promulgate rules related to the NLRA. Garden, Charlotte. "Labor Organizing in the Age of Surveillance." . . *Louis ULJ* 63 (2018): 55.

[176] Consolidated Edison Co. of New York v. N.L.R.B., 305 U.S. 197 (United States 1938).

[177] Garden, Charlotte. "Labor Organizing in the Age of Surveillance." . . *Louis ULJ* 63 (2018): 56.

[178] Garden, Charlotte. "Labor Organizing in the Age of Surveillance." . . *Louis ULJ* 63 (2018): 55.

[179] Alexander, Charlotte S, and Elizabeth Tippett. "The Hacking of Employment Law." *Mo* 82 (2017): 973.

[180] Alexander, Charlotte S, and Elizabeth Tippett. "The Hacking of Employment Law." *Mo* 82 (2017): 973.

[181] Alexander, Charlotte S, and Elizabeth Tippett. "The Hacking of Employment Law." *Mo* 82 (2017): 973.

[182] Alexander, Charlotte S, and Elizabeth Tippett. "The Hacking of Employment Law." *Mo* 82 (2017): 973.

[183] The topic of liability is discussed in greater detail in section 5.c. Alexander, Charlotte S, and Elizabeth Tippett. "The Hacking of Employment Law." *Mo* 82 (2017): 973.

[184] Erratic and unpredictable shifts can cause income volatility, psychological distress, and exacerbate financial issues. The practice of "clopenings," where a worker receives back to back closing and opening shifts, is especially harmful and leads to severe psychological stress. Wykstra, Stephanie. "The Movement to Make Workers' Schedules More Humane." *Vox*, October 15, 2019. https://www.vox.com/future-perfect/2019/10/15/20910297/fair-workweek-laws-unpredictable-scheduling-retail-restaurants.

[185] For more information on these policies see The Fair Workweek Initiative. "Fact Sheets & Research." *Fair Workweek Initiative*. accessed July 1, 2020 http://www.fairworkweek.org/resources.

[186] Wolfe, Julia, Janelle Jones, and David Cooper. " 'Fair Workweek' Laws Help More than 1. 8 Million Workers." *Washington, DC: Economic Policy Institute Report*, 2018; Alexander, Charlotte, Anna Haley-Lock, and Nantiya Ruan. "Stabilizing Low-Wage Work." *Harv* 50 (2015): 1

[187] Sabine, Alix. "Right to Disconnect And The El Khomri Labour Law." *Avens*, April 4, 2017. https://www.avens.fr/en/right-to-disconnect-and-the-el-khomri-labour-law/.

[188] Ornstein, Daniel, and Jordan Glassberg. "More Countries Consider Implementing a 'Right to Disconnect.'" *The National Law Review*, January 29, 2019. https://www.natlawreview.com/article/more-countries-consider-implementing-right-to-disconnect.

[189] Private employees disconnecting from electronic communications during non-work hours. of 2018, New York City Council Int. No. 726, New York City Council (2018).

[190] American Management Association. "Electronic Monitoring & Surveillance Survey," 2007; "Being Watched at Work." *SimplyHired*. accessed July 1, 2020 https://www.simplyhired.com/guide/studies/being-watched-at-work.

[191] See note 161 for more on algorithmic management.

[192] Mateescu, Alexandra, and Aiha Nguyen. "Explainer: Workplace Monitoring & Surveillance." *Data & Society*, 2019. https://datasociety.net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf; Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *Calif* 105 (2017): 735; Garden, Charlotte. "Labor Organizing in the Age of Surveillance." . . *Louis ULJ* 63 (2018): 55; See section "Surveillance As Unfair Labor Practice" p.23

[193] "Managing Workplace Monitoring and Surveillance." *Society for Human Resource Management*, May 13, 2019. https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx. ;
Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *Calif* 105 (2017): 735.

[194] California, Illinois, and New York have laws that restrict monitoring in private areas

[195] "Through the Keyhole: Privacy in the Workplace, an Endangered Right." *American Civil Liberties Union*. accessed June 30, 2020 https://www.aclu.org/other/through-keyhole-privacy-workplace-endangered-right.

[196] Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *Calif* 105 (2017): 735. "The Worker Privacy Act: Discussion Draft." *Georgetown Law Center on Privacy and Technology.* 2019. https://drive.google.com/file/d/1Mi1JTezFbmTdJg2Fbp_MreFuSTWQ5QmK/view

[197] "Through the Keyhole: Privacy in the Workplace, an Endangered Right." *American Civil Liberties Union*. accessed June 30, 2020 https://www.aclu.org/other/through-keyhole-privacy-workplace-endangered-right; Fiore, Alexandra, and Matthew Weinick. "Undignified in Defeat: An Analysis of the Stagnation and Demise of Proposed Legislation Limiting Video Surveillance in the Workplace and Suggestions for Change." *Hofstra Lab. & Emp. LJ* 25 (2007): 525.

[198] Bohm, Wolf-Tassilo, and Lukas Strobel. "New Case Law on Restrictions for Employee Monitoring in the Workplace in Germany." *Hogan Lovells*, August 18, 2017. https://www.hldataprotection.com/2017/08/articles/international-eu-privacy/new-case-law-on-restrictions-for-employee-monitoring-in-the-workplace-in-germany/.

[199] Ciocchetti, Corey. "The Eavesdropping Employer: A Twenty-first Century Framework for Employee Monitoring." *American Business Law Journal* 48, no. 2 (2011): 285–369. See section "Data Protection Impact Assessments (DPIAs) p.14

[200] Fiore, Alexandra, and Matthew Weinick. "Undignified in Defeat: An Analysis of the Stagnation and Demise of Proposed Legislation Limiting Video Surveillance in the Workplace and Suggestions for Change." *Hofstra Lab. & Emp. LJ* 25 (2007): 525.

[201] Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *Calif* 105 (2017): 735.

[202] Conjunctive tests are multi-part inquiries. For a practice to be legally permissible, it must satisfy each prong of the test.

[203] Fiore, Alexandra, and Matthew Weinick. "Undignified in Defeat: An Analysis of the Stagnation and Demise of Proposed Legislation Limiting Video Surveillance in the Workplace and Suggestions for Change." *Hofstra Lab. & Emp. LJ* 25 (2007): 525

[204] Miles, John. "Interpretation of 29 CFR 1910.141(c)(1)(i): Toilet Facilities." Occupational Safety and Health Administration. 1998.

[205] Liao, Shannon. "Amazon Warehouse Workers Skip Bathroom Breaks to Keep Their Jobs, Says Report." *The Verge*, April 16, 2018. https://www.theverge.com/2018/4/16/17243026/amazon-warehouse-jobs-worker-conditions-bathroom-breaks.

[206] Tutt, Andrew. "An FDA for Algorithms." Admin 69 (2017): 83

[207] Tutt, Andrew. "An FDA for Algorithms." Admin 69 (2017): 83

[208] Tutt, Andrew. "An FDA for Algorithms." Admin 69 (2017): 83

[209] Tutt, Andrew. "An FDA for Algorithms." Admin 69 (2017): 83;. For more information on different liability standards and permutations of liability apportionment, see section "Liability for Algorithmic Harms" p. 37

[210] Tutt, Andrew. "An FDA for Algorithms." Admin 69 (2017): 83

[211] For example, the White House Office of Science and Technology Policy provides advice on scientific or technical issues that impact the economy, national defense, or other areas.

[212] Calo, Ryan. "The Case for a Federal Robotics Commission." *Available at SSRN 2529151*, 2014.

[213] The FDA's meat and pharmaceutical inspectors are examples of this function.

[214] The National Transportation Safety Board provides reports on aviation, highway, and marine accidents or incidents. These reports may include safety recommendations based on the findings.

[215] For example, the Environmental Protection Agency may provide planning oversight for Environmental Impact Assessments.

[216] Shneiderman, Ben. "Opinion: The Dangers of Faulty, Biased, or Malicious Algorithms Requires Independent Oversight." *Proceedings of the National Academy of Sciences* 113, no. 48 (2016): 13538–40.

[217] See section "Data Protection Impact Assessments (DPIAs)" p. 14 and "Algorithmic Impact Assessments (AIAs)" p.15

[218] The NLRB is one example of such an agency. The NLRB requires parties to exhaust administrative remedies prior to bringing civil actions.

[219] Tutt, Andrew. "An FDA for Algorithms." Admin 69 (2017): 83

[220] Tutt, Andrew. "An FDA for Algorithms." Admin 69 (2017): 83

[221] New, Joshua, and Daniel Castro. "How Policymakers Can Foster Algorithmic Accountability." *Center for Data Innovation*, 2018; Whittaker, Meredith, Kate Crawford, Roel Dobbe, Genevieve Fried, Elizabeth Kaziunas, Varoon Mathur, Sarah Mysers West, Rashida Richardson, Jason Schultz, and Oscar Schwartz. *AI Now Report 2018*. AI Now Institute at New York University New York. 2018. Tutt, Andrew. "An FDA for Algorithms." Admin 69 (2017): 83

[222] Bogen, Miranda, and Rieke Aaron. *Help Wanted: An Exploration of Hiring Algorithms, Equity and Bias*, Upturn. 2018. https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf

[223] Although issues of product liability for autonomous or semi-autonomous systems are most often discussed in the context of AVs, some of the discussion may be relevant to decision-making algorithms used in the employment context. It is beyond the scope of this paper to fully discuss issues related to insurance and liability that emerge in these contexts, however a robust discussion can be found in Smith, Bryant Walker. "Automated Driving and Product Liability." *Mich. St. L. Rev.*, 2017, 1 and Crane, Daniel A, Kyle D Logue, and Bryce C Pilz. "A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles." *Mich. Telecomm. & Tech. L. Rev.* 23 (2016): 191.

[224] Vladeck, David C. "Machines without Principals: Liability Rules and Artificial Intelligence." *Wash* 89 (2014): 117.

[225] Koene, Ansgar, Chris Clifton, Yohko Hatada, Helena Webb, and Rashida Richardson. *A Governance Framework for Algorithmic Accountability and Transparency*, European Parliamentary Research Service. 2019. https://www.europarl.europa.eu/stoa/en/home/highlights.