Breakout Sessions – Series 5

WORK RECONSTRUCTED

RISKS AND SOLUTIONS IN THE DIGITAL ERA

Gary D. Eisenstat (Moderator) – Ogletree Deakins (Dallas)

Jennifer Monrose Moore – Ogletree Deakins (Tampa)

Tibor Nagy Jr. – Ogletree Deakins (Tucson/Phoenix)
I. INTRODUCTION

“How do we improve our efficiency and productivity?” It is a question that business leaders face and ask routinely, often tapping technology as the answer. This is hardly new, and the digital or information age is only the latest iteration of machines recasting how work is done. Yet, the rate and breadth of change and the legal challenges that arise from these new technologies are unprecedented. Employers, courts, and regulators have struggled to keep pace with these often bewildering changes, while simultaneously constrained by outdated laws and regulations not suited for these new circumstances.

Likewise, the number of jobs or tasks that now involve or include the use of some form of digital technology is beyond any measure previously imagined. These changes have generated both significant opportunities and concurrent challenges, particularly as companies allocate their financial and labor resources. This, in turn, affects both organizational structure and workforce composition as companies determine what talent is needed, where, and how to best supervise and direct their workers.

A generation ago, few companies had IT departments or Chief Technology Officers. Most companies also hired their workers directly as employees, and many employees remained employed by those companies for the duration of their careers, retiring on company-sponsored pension plans. Companies also historically outsourced only small amounts of their work to independent contractors who were hired to perform specific tasks or projects.

Today’s workforce is increasingly impermanent, as demand has shifted towards flexibility and transformation. Progressively more workers are being hired on a temporary or contract basis, as companies reposition and reassess their work needs nearly as often as technology seems to change. The use of AI, robotics, and other technologies will inevitably increase as companies reassess what work they do and how it is accomplished.

In *Reinventing Jobs*,

the authors posit that when analyzing work for the application of AI and robotics, a first logical step is to understand the tasks at hand in terms of four factors: (1) the simplicity or complexity of the tasks, (2) the level of repetition or variability involved in the operations, (3) the amount of independence or interaction associated with the tasks, and (4) to what extent the work is physical versus mental or analytical. Tasks that are less complex, highly repetitive, and can essentially function independently, usually are better candidates for AI or robotics than are jobs requiring more complex, variable, interactive, and intellectual activities.

Once that analysis is “complete” – although it is undoubtedly a perpetual inquiry – an organization can determine how those tasks are best performed, by whom or what, when and even where. For example, if the work at issue transitions from technical, mechanical skills that is then performed robotically, the work force might need to be reconfigured to include fewer assembly workers in favor of those with more programming and robotics maintenance skills. This can trigger simultaneous work force reductions and searches for new workers, each of which pose unique risks.

Rapid changes in technology now require workers to adapt far more rapidly to their work environment. Rather than making a “career” out of a certain skill set, individuals may now be required essentially to “reinvent” themselves every 6-8 years to stay current with technological changes to remain relevant in a given work space. Those who are most adept at making these

---

changes are more likely to succeed, and ‘specialists,’ relatively speaking, run the risk of having their skills and expertise become obsolete after a certain period of time.

Meanwhile, corporate organizational structure and protection of proprietary information is impacted as work is reconstituted, reassigned and/or outsourced. For example, traditional corporate “in-house” tasks might be better suited for outsourcing, depending on the frequency and the urgency of the need for the task to be performed, and the complexity or training needed to accomplish the tasks. However, such outsourcing also impacts what corporate information is imparted, how, and to whom.

The recent explosion of ride sharing apps helps illustrate this point. The personal transportation industry has dramatically changed from domination by a few cab services in each city to a landscape where anyone with access to a vehicle and a smart phone is eligible to drive others for hire. This occurred just by converging the demand for paid rides with those who are able to supply those rides, all through the use of digital technology. This model seems destined to creep further into the workplace.

The growth and expansion of technology both in, and in relation to, the workplace, has other significant implications discussed below. For example, employees’ use of their own personal electronic devices, such as a smart phone, tablet, or laptop computer, for work purposes (so-called Bring Your Own Device or BYOD) raises a whole host of risk and compliance issues, as does allowing workers to access company email, documents, and data from remote locations or on those devices. The use of such devices in connection with work also implicates trade secret and data protection issues, privacy concerns, worker job classification and overtime work and pay issues, as well as safety issues and evidence preservation obligations.

Social media also raises broad legal implications for employers on many levels, ranging from protection of trade secrets and confidential information to workers’ rights under the National Labor Relations Act, as well as business disparagement and defamation concerns. The use of AI in such areas as job applicant screening and hiring decisions also carries legal risks, such as understanding the underlying assumptions built into selection criteria and the application of data AI uses to analyze applicants and determine job suitability.

Finally, while the use of robotics in the workplace promises many productivity benefits (e.g., work performed essentially nonstop and with higher levels of accuracy) it, too, holds risks, ranging from workplace safety issues to workplace accommodations, as well as worker displacement and retraining issues.

II. MOBILE AND OTHER PERSONAL ELECTRONIC DEVICES IN THE WORKPLACE AND THE “BYOD” CONUNDRUM

Smartphones and tablets are more and more a part of everyday life. In a June 2018 study by Oxford Economics, 80% of employees surveyed stated that they could not effectively do their work without a smartphone. This builds on a prior 2012 survey sponsored by Trend Micro showing that employees prefer companies that permit employees to use their personal electronic devices for work (aka BYOD), and executives believe that BYOD programs positively influence productivity and creativity. As a result, employers must keep pace in the race of ever-improving technology against legal and regulatory compliance – as well as protecting Company

---

assets in an employment setting where employees easily can create, store, and transmit work-related data.

The benefits and efficiencies of tech programs like BYOD or their hybrid cousins do not come without risk or cost to the employer. Oxford Economics’ study revealed that companies “go mobile” in different ways, and with each comes a different level of risk.

The greater the access, the greater the risk and responsibility of companies to ensure protection of assets and legal compliance. While there is certainly overlap, BYOD poses some issues distinct from those where employers issue company cell phones, PDAs, laptops or the like. Because the employer does not own the device with BYOD, the employer cannot prohibit the device from being used for personal reasons, automatically track and access the device, and demand return of the device upon an employee’s departure. These are just some of the issues that pose challenges to employers.

This section addresses some of the potential compliance and asset protection issues facing employers dealing with any form of BYOD or remote access technology, as well as some best practices to alleviate these concerns.

**A. Company Asset Protection: Trade Secrets**

While most employers today have policies and agreements identifying and protecting confidential trade secrets and proprietary business information, employers allowing any form of remote access should incorporate those specific prohibitions of copying of company data to any form of employee personal device. Employers need to consider the challenge that BYOD poses to their ability to protect trade secret information. For some, the risk may simply be too great altogether, while for others internal firewalls and restricted access may help lessen the risks. Additionally, employers that handle sensitive, confidential, or highly regulated information, like those employers governed by the Health Insurance Portability and Accountability Protection Act of 1996 (HIPAA) or financial regulatory privacy issues, including
banks, lending institutions, and credit reporting agencies, may mandate the exclusive use of corporate devices with remote access at only this highest of security levels.

The importance of ensuring that confidentiality agreements are up-to-date and employees are aware and understand that company data may not be deleted without authorization cannot be overstated. Additionally, procedures should be established to ensure that information from departing employees’ devices is sufficiently protected. Restricting BYOD and remote access to specific classes of employees may also limit liability and loss.

A strategic employer will train employees concerning their responsibilities and requirements for the privilege of using their personal device. In addition to such training, employers should implement safeguards and protocols for the deletion of data from employee owned devices, immediate revocation of network and server access, remote deletion of applications, and IT exit procedures. Additionally, such policies and practices also should include preservation of data from employee-owned devices that relate to business matters. Employers may go so far as having employees consent to a full factory reset of personal devices through mobile device management software if an employee fails to comply with IT exit procedures.

B. Complying With Legal & Regulatory Confidentiality Obligations

Allowing company data to be stored and transmitted using devices and networks an employer does not control poses a risk to the security of information that may expose companies to liability. For example, HIPAA requires some industries to implement safeguards for protected health information maintained in electronic form. In fact, in 2012, a Massachusetts health care provider and affiliated physician group paid $1.5 million to the federal government to resolve allegations that it violated the HIPAA security rule after a doctor’s laptop computer containing unencrypted patient data was stolen.

Individual states have also promulgated a patchwork of laws protecting individual privacy, including laws that are specifically directed to protect information online. For example, California has multiple statutory provisions designed to combat invasions of privacy both online and off, punishable by both criminal and civil penalties. In short, security breaches expose employers to government enforcement actions, civil penalties, and litigation. BYOD policies need to address these risks. Companies need to ensure they have legally defensible security measures in place to prevent unauthorized access to confidential information. At a minimum, employers should be able to demonstrate a considered and thorough approach to its BYOD policy and related data-security concerns.

Confidentiality policies and agreements are critical tools in combating confidentiality breaches, and in meting out consequences after the fact. Although confidentiality policies should be in place in any environment where proprietary information is shared, confidentiality agreements between employers and employees permit enforcement after the fact, that is, after the employment relationship has been severed and the employee is not clearly subject to the employer’s policies.

In addition to confidentiality policies and agreements, an employer should take, and be able to demonstrate, reasonable measures to protect confidential or other proprietary information. Company-issued mobile devices or laptops often contain company-vetted security applications that its IT department can support. If an employer allows an employee to connect

---

4 See 45 C.F.R. pts. 160, 162 and 164.
his or her own device to the company network to access company data, the employer needs to ensure similar security precautions are in place, and should obtain agreement to terms of use at its first opportunity. Any BYOD policy should require installation of security measures such as encryption software and require that the employee utilize strong passwords. Employees should also agree not to alter security settings.

The ability to delete or wipe data from a device remotely in the event of theft or loss is also a security essential. The BYOD policy should expressly require that employees promptly report a lost, stolen, or otherwise disabled device. An employer should also establish clear policies on the extent to which it will be able to access, monitor, and delete data on the employee’s personal device and whether, in specific circumstances, this may include the employee’s personal data. Employees should also be notified that they will be required to load software on their devices to allow for wiping, and that this could also wipe their personal photos, contacts, emails, and other software. Employers should have the employees sign a waiver consenting to wiping and holding the company harmless.

Employers should consider requiring and installing encryption and antivirus software, and enable remote wiping capabilities. Employers may also want to consider revising mobile device security, password, and loss reporting policies.

C. Investigations and Employee Privacy

Many courts recognize that an employee has “no reasonable expectation of privacy” in computer files, emails, and electronic data maintained at his or her workplace. The federal Computer Fraud and Abuse Act (CFAA) makes it a criminal offense to gain unauthorized access to a computer and may permit the recovery of civil damages. Several states have laws that specifically prohibit unauthorized computer access, and others have general statutes that permit prosecution for similar offenses. Accessing an employee’s personal device without prior written permission may subject the employer to liability. Therefore, at a minimum, employers should provide explicit notice to employees that the information on their devices, or even the devices themselves, may be discoverable in litigation and obtain prior written consent to access employees’ devices.

Consider the situation where a company is involved in litigation and an employee’s personal cell phone or tablet connected to work email and other company servers may have relevant information that may need to be examined for evidence and compliance with the rules of discovery. When an individual employee owns or possesses their device, it may be difficult to actually obtain possession of the device – especially where the employee (or former employee) him or herself is the subject of the investigation. An employer may mitigate this concern by maintaining a comprehensive archive of all business-related communications and requiring employees to access the corporate network in order to perform business tasks on the employee’s personal device.

From the outset, identify both the employer’s and employee’s rights and responsibilities, including what exactly can be accessed on a personal device, and exactly what will happen if the device is lost or compromised, or if the employee leaves the business. Make employees aware of their privacy limitations and agree to what constitutes a reasonable expectation of privacy within the realm of their personal device accessing company information and systems. Train employees on these policies so that all privacy-related issues are consented knowingly.

---

while utilizing systems that minimize potential exposure of employees’ personal and private information.

D. Claims & Litigation: Preserving, Destroying, and Producing Electronic Records

As discussed above, many companies, especially those dealing with financial and medical data, are subject to strict recordkeeping laws and regulations (e.g., HIPAA, the Fair Credit Reporting Act, etc.) that govern both the preservation and destruction of various types of electronic records. Some laws also require companies to notify their customers if personal information may have been compromised or accessed. Thus, having appropriate protocols in place for these obligations is key.

Lawsuits present a different set of challenges for in-house counsel and can be their own source of liability exposure, especially where an employee’s personal device may contain evidence relevant to the dispute, such as texts, private emails, documents on hard drives, etc. Specifically, both Fed. R. Civ. P. 34 and nearly every state law or rule patterned on it, require companies to produce documents (which includes electronic communications) that are deemed to be within their “possession, custody, or control.”

BYOD litigation and discovery disputes tend to center around whether a company is deemed to have “possession, custody, or control” over data stored on the personal devices of its employees. If the requested items are deemed to be within the company’s possession, custody, or control, the focus often turns toward whether the company (i.e., in-house counsel) has taken adequate steps to preserve that information, e.g., with a litigation hold letter. If the company has not preserved this evidence, it may face a spoliation or destruction of evidence claim or sanction. Rule 37(b)(2)(A) of the Federal Rules of Civil Procedure allows a court to impose various types of sanctions for discovery abuses, ranging from giving jury instructions regarding the content of the destroyed evidence, to striking pleadings, or dismissing the action, along with monetary sanctions if the court determines that the company failed to preserve relevant evidence.

Where spoliation is concerned, the remedy of outright dismissal of an offending party’s claim is sometimes imposed, although federal courts have come down on both sides of that issue. For example, in *E.I. Du Pont de Nemours & Co. v Kolon Indus.*, 803 F. Supp. 2d 469 (E.D. Va. 2011), the court held that a spoliation instruction should be given in a trade secrets dispute where the court found that the defendant had intentionally destroyed electronic evidence. Whereas, in *Taylor v. Mitre Corp.*, No. 1:11-CV-1247, 2012 WL 5473573 (E.D. Va. 2012), the plaintiff wiped the hard drive of his work computer and then destroyed it with a sledgehammer at some point after determining that litigation was likely. After he filed suit, the court then ordered the plaintiff to produce his laptop for a forensic examination. However, before doing so, the plaintiff ran two computer software programs designed to delete information on the hard drive and defeat forensic software. The court sanctioned the plaintiff by dismissing his claims and ordering him to pay monetary sanctions because the plaintiff had a duty to preserve relevant evidence, and had clearly and intentionally disobeyed the court’s orders.

In addition to a party’s preservation of evidence, in some states, like Florida, spoliation can be a cause of action of its own permitting a party to seek damages against a third-party who is on notice of the need to preserve evidence, but who (even negligently) destroys it. In this situation, the spoliating party may be subject to liability for civil money damages. *Hagopian v. Publix Supermarkets, Inc.*, 788 So. 2d 1088 (Fla. Dist. Ct. App. 2001).
E. BYOD Perilously Blurs the Line Between Work Life and Personal Life

Prudent employers typically avoid treading on employees’ personal lives. But where employees use their own personal devices with company approval, that line can be blurred and sometimes crossed – and the consequence can be dire.

1. Equal Employment Opportunity Concerns

State and federal laws require employers to provide employees and prospective employees with equal employment opportunities. In particular, federal law prohibits discrimination and harassment based on race, color, national origin, sex and religion, veteran status, genetic information, pregnancy, age, and physical or mental disability. Employers also must maintain a workplace free of unlawful harassment, including a hostile work environment, based upon any protected characteristic.

Employers should consider the danger that an employee may use his or her own personal device to view and/or exchange content that would violate company EEO policies. When that same device is brought into the workplace, the employee may not fully recognize the distinction between private and professional conduct. In other words, just because it is the employee’s own device does not make it acceptable to use it to view racially derogatory or sexually explicit content while at work, potentially creating a discriminatory or hostile work environment.

Evidence of supervisor/employee or employee/employee interaction on Company or personal devices is often the target of e-discovery in these cases. Any policy should contain a reminder that employees when utilizing personal devices for work purposes are subject to the company’s employment policies, including Equal Employment Opportunity, and policies prohibiting Harassment in the Workplace.

An employer should also consider whether a personal device may be used in order to accommodate an employee with a qualifying disability under the ADA or state law. When the need to accommodate a disabled employee or potential employee arises, an employer should consider whether an employee’s own device could provide the needed assistance and whether the employer should purchase or otherwise support the device as a reasonable accommodation. For example, an employee with a hearing or cognitive disorder may want to use their own device to record meetings and supervisor instructions. Employees in this situation should know the laws of consent to intercept aural communications and insure that all parties required to consent have done so before engaging in this type of self-help accommodation.

2. FMLA and Other Protected Leaves of Absence

One situation applicable to both non-exempt and exempt employees involves addressing access to work-related emails where an employee is on a leave of absence (e.g. FMLA, disability, maternity/paternity). Because communications do not cease when an employee takes

---

7 Title VII of the Civil Rights Act of 1964 (Title VII), 42 U.S.C. §§ 2000e et seq.
12 Americans with Disabilities Act, 42 U.S.C. §§ 12101 et seq.
13 See, e.g., EEOC v. R&R Ventures, 244 F.3d 334, 338 (4th Cir. 2001).
leave, employers must prevent employees from engaging in uncompensated work while on
leave. Additionally, as to FMLA, an employer may run a risk of interfering with an employee’s
leave. Under the FMLA, employers are prohibited from interfering with an employee’s exercise
of his or her FMLA rights. In part, this means employers cannot require employees on FMLA
leave to work while on leave. Thus, a policy that prohibits employees from working while on
leave may be helpful, but has practical limitations, particularly where an employee receives
notifications and alerts, or receives communications that call for a timely response.

The optimal solution would be to disconnect the employee from employer networks for
the period of the leave, or to redirect all communications to another employee in the first
instance. This approach has the added benefit of maintaining the lines of communication
between employer and employee for leave-associated communications. Whether or not an
employee’s access is shut off while on leave, employees on leave should be reminded that they
are not to access, read, or respond to work e-mails.

3. General Liability and Workers’ Compensation Claim Mitigation

Employers who allow employees to use mobile devices should consider policies and
parameters for use. Companies can always face potential liability exposure where employees
behave negligently. Mobile devices are fertile ground for just such a claim if, for example, a
worker is texting and driving, talking on the cell phone while driving, or even looking for
directions on a cellular device while moving, and then hits a car, pedestrian, or building.

III. PROTECTING WORKERS FROM R2D2: WORKPLACE SAFETY IN A ROBOTIC
ENVIRONMENT

The increased use of robotics in the workplace poses significant safety issues for
workers who interact with them, many of which are addressed in OSHA’s applicable Technical

Studies in Sweden and Japan indicate that many robot accidents do not occur under
normal operating conditions but, instead during programming, program touch-up or refinement,
maintenance, repair, testing, setup, or adjustment. During many of these operations the
operator, programmer, or corrective maintenance worker may temporarily be within the robot's
working envelope where unintended operations could result in injuries.

Some maintenance and programming personnel may be required to be within the
restricted envelope while power is available to actuators. The restricted envelope of the robot
can overlap a portion of the restricted envelope of other robots or work zones of other industrial
machines and related equipment. Thus, a worker can be hit by one robot while working on
another, trapped between them or peripheral equipment, or hit by flying objects released by a
gripper.

Likewise, a robot with two or more resident programs can find the current operating
program erroneously calling another existing program with different operating parameters such
as velocity, acceleration, or deceleration, or position within the robot's restricted envelope. A
component malfunction could also cause an unpredictable movement and/or robot arm velocity.

Additional hazards can also result from the malfunction of, or errors in, interfacing or
programming of other process or peripheral equipment. The operating changes with the process
being performed or the breakdown of conveyors, clamping mechanisms, or process sensors could cause the robot to react in a different manner.

To avoid injuries, OSHA recommends a multi-step approach considering the following elements:

- Risk Assessment
- Safeguarding Devices.
- Awareness Devices.
- Safeguarding the Teacher
- Operator Safeguards
- Attended Continuous Operation
- Maintenance and Repair Personnel
- Maintenance
- Safety Training
- General Requirements

Robots or robotic systems must also comply with the following regulations: Occupational Safety and Health Administration, OSHA 29 CFR 1910.333, Selection and Use of Work Practices, and OSHA 29 CFR 1910.147, The Control of Hazardous Energy (Lockout/Tagout).

IV. THE INTERSECTION OF SOCIAL MEDIA AND EMPLOYMENT LAW

A. Social Media and the Workplace – More Examples of Technology Blurring the Lines Between Work Life and Personal Life

Generally, employers face two types of risks relating to employee usage of social media: (1) business and legal risks stemming directly from employee use of social media; and (2) legal risks stemming from firing employees or taking other adverse action due to use of social media.

First, employers face significant risks relating to their employees’ off-duty and off-site use of social media. Before the rise of social media, off-duty and off-site conduct between employees could result in employer liability, particularly where an employee complains prior to the conduct or where the conduct occurs in a quasi-work setting. That risk is exponentially compounded when social media is an added ingredient.

Ultimately, employers face a host of business and legal risks arising from their employees’ use of social media, including:

- Offending customers and clients
- Negative publicity and damaging the company’s reputation or business
- Defamation
- Intellectual property infringement (including trademark and copyright)
- Trade secret disclosure
- Disclosure of private customer and client information
- Claims by coworkers against the company, such as for harassment, negligent retention or supervision, or infliction of emotional distress
- Tortious interference with current or prospective business relationships or contracts
- Fraud
Second, once employers become aware of conduct by employees relating to social media, employers must consider legal risks stemming from firing employees for use of social media, including the following potential claims by employees:

- Off-duty conduct laws (in many states)
- Discrimination and retaliation under Title VII and state laws
- Whistleblowing under SOX
- Concerted action under the NLRA
- Invasion of privacy
- Stored Communications Act, Wiretap Act, and electronic monitoring statutes

In light of the serious business and legal concerns outlined above, many employers actively police employee blogs and social networking sites, while others act on coworker reports about social media postings. Regardless of how an employer learns of the postings, employers continue to discipline and terminate employees due to postings on blogs and social networking sites. As discussed below, such scrutiny and action is fraught with legal risk.

1. **Off-Duty Conduct Laws**

Laws in many states prohibit an employer from discharging or disciplining an employee for using lawful consumable products (like tobacco and alcohol) off work premises during non-working hours. Thus, if an employee’s use of social networking sites or blogging concerns off-duty drinking or smoking, the employer likely should not take adverse action unless such conduct truly implicates workplace issues. For example, a drunken YouTube rant about a company client likely would not be protected.

Some states – like Illinois, California, New York, Colorado, and North Dakota (to name just a few) – have enacted broader laws protecting employees in their off-duty conduct, recreational activities, and political practices. For example, New York prohibits employers from firing or discriminating against employees for off-duty and off-site “legal recreational activities,” although the law has several exceptions, including where the employee’s activities “constitute habitually poor performance,” reflect “incompetence,” or “create[] a material conflict of interest related to the employer’s trade secrets, proprietary information or other proprietary or business interest.”

Blogging or posting likely qualifies as protected activity under many of these statutes, although employers will often be able to rely on the statutory and case law exceptions for situations damaging to the employer’s business. Thus, employers should always check a state’s off-duty conduct law before taking adverse action based on an employee’s use of social media.
2. Discrimination and Retaliation Under Title VII and State Laws

Employees terminated due to use of social media may argue discriminatory enforcement. Title VII establishes that it is unlawful for an employer to discriminate due to “race, color, religion, sex, or national origin.” The ADA and the ADEA offer similar protections to disabled employees and to employees over the age of forty. Some state laws also add sexual orientation, marital status, and status with regard to public assistance as protected classes.

Many individuals share personal demographic information on social networking sites or in the content of blogs, including sexual orientation, religion, age, medical conditions, marital status, race, and other protected categories. Some employee-bloggers may attempt to cloak themselves in the protection of an anti-discrimination statute by revealing their identification with these protected classes, such as a blogger who discusses his conversion to Islam may allege his subsequent termination was due to his religious beliefs in violation of Title VII.

The difficulty for employers in this type of lawsuit is the proverbial “un-ringning of the bell.” The employer is forced to argue that while it learned about a protected characteristic on line, this information did not sway its employment decision. Moreover, it has become fairly common for applicants to include LinkedIn links on their résumés that may reveal the above information as well as interests, recommendations, groups, associations, book reading lists, embedded videos, travel plans, documents, websites, and related Twitter accounts. Thus, while it might be difficult for an employee to prove that online disclosure of a protected characteristic resulted in termination (or other adverse employment decision), it also would be costly for an employer to successfully defend its actions in a lawsuit.

Employers also should consider the anti-retaliation provisions of federal and state employment laws before taking adverse action for on-line behavior. Title VII, for instance, prohibits an employer from retaliating against an employee for “oppos[ing]” any unlawful discriminatory practice. Some employees may attempt to “oppose” a discriminatory practice on a social networking site or blog, which means that subsequent adverse action by the employer could lead to a claim of retaliation.

Avoiding claims may be challenging for employers who may not be aware of every posting made by employees. Thus, an employer should take documented steps to ascertain whether it is imposing comparable discipline on other similarly-situated employees who are not members of the protected class before taking action against an employee based on a posting.

Also, many job applicants submit video résumés, which are usually a free-form creation from an applicant, submitted in random format not controlled or requested by the potential employer. Video résumés inevitably contain information regarding characteristics of the applicant that are unrelated to any job function (including protected class information), and provide more information than a paper résumé would, which creates the risk of discrimination claims.

Under Title VII, it is not illegal for an employer to learn the race, gender or ethnicity of a job seeker through a video clip. Likewise, it is not illegal under the ADA to learn or suspect that an individual has a disability after seeing his/her video clip. However, such knowledge could increase the risk of a discrimination claim. Employers need to train hiring officials and human resources staff about the appropriate responses when gender, race, ethnicity or disability is disclosed during recruitment. Obviously, employers reviewing video résumés need to focus on the person’s qualifications for the job.
3. Social Media and the NLRA

Before taking adverse action against an employee for social media postings, an employer should consider whether the postings are protected by the National Labor Relations Act (the “NLRA”).

During the Obama administration, on-line and other social media behavior by employees caught the National Labor Relations Board’s attention, resulting in a number of Board Complaints and Division of Advice memoranda on the subject in regards to disciplinary action for on-line criticism by employees of their employers. Such behavior often is regarded as protected concerted activity (“PCA”). Specifically, the NLRA grants employees the right to “engage in other concerted activities for the purpose of mutual aid and protection,” which applies to virtually all private-sector employers regardless of union representation.

The “bright line” between lawful and unlawful disciplinary action in these cases generally boiled down to whether the employee’s blog, post or tweet involved other employees or, even if other employees were involved, whether the communication addressed “terms and conditions of employment.” Concerted activity happens when an employee acts “with or on the authority of other employees,” or when the individual activity seeks to initiate, induce, or prepare for group action, or when the employee brings “truly group complaints to the attention of management.” The Board finds such activity is concerted even if it involves only one speaker and one listener, “for such activity is an indispensable preliminary step to employee self organization.” On the other hand, comments made “solely by and on behalf of the employee himself” are not concerted. “Comments must look toward group action; ‘mere griping’ is not protected.”

While individual incidents involving social media tend to be factually driven, the Obama Board was less forgiving with blanket employer rules, policies and procedures that impacted employee speech and communications, particularly on social media. A hallmark of that regulatory period was the NLRB General Counsel’s Memorandum 15-04, which strictly regulated employer policies and rules affecting employee conduct both in and outside of the workplace – such as behavior on social media.

The current General Counsel rescinded that Memorandum in late 2017 and in its place issued a new “Guidance on Handbook Rules Post-Boeing” in June 2018 (Memorandum GC 18-04). The latest Guidance expounded on the new standard adopted by the Board in its 2017 Boeing Company decision.14 According to that decision, an employer rule will only violate the NLRA if it would be reasonably interpreted to interfere with workers’ NLRA rights considering the balance between: (i) the nature and extent of the rule’s potential impact on protected rights, and (ii) the employer’s legitimate justifications for the rule.

The General Counsel’s New Guidance created three categories of employer rules: Category 1 rules are presumptively lawful; Category 2 rules warrant individualized scrutiny; and Category 3 rules are presumptively unlawful. The Guidance includes the following types of rules within Category 1, and therefore presumptively lawful.

Rules prohibiting employees from:

- Commenting for, or speaking on behalf of, the employer without prior written approval;

14 The Boeing Company, 365 NLRB No. 154 (2017).
• Making negative or disparaging remarks about other employees;
• Disclosing the employer’s confidential, proprietary, or trade secret information;
• Disclosing information concerning the employer’s clients or customers;
• Misrepresenting the employer’s products, services, or employees; and
• Using the employer’s logo, trademark, or graphics without prior written approval.

While such “facially lawful” rules might still be found unlawful if “applied unlawfully,” the Guidance confirms that their mere existence in an employer’s policies or handbook is no longer per se an unfair labor practice (ULP). Importantly, although not specifically mentioned in the Guidance or in the Boeing decision, it is reasonable to assume that these presumptively lawful rules also apply to an employer’s social media policies, such as rules regulating or addressing employee use of email or activities on social media sites.

However, employers should keep in mind that rules and policies that fall within Categories 2 and 3 of the Guidance should be avoided. These include comprehensive policies prohibiting or restricting employees from:

• Criticizing their employer;
• Making negative, disparaging or false or inaccurate statements about their employer;
• Discussing or disclosing wages, benefits, or working conditions;
• Joining outside organizations.

B. AI and Social Media in the Hiring Process

A substantial number of states have laws that restrict employers from accessing employees’ and applicants’ personal social media accounts. These laws vary significantly from jurisdiction to jurisdiction, though many prohibit employers from requiring job applicants or employees to disclose their social media usernames and passwords as a condition of employment; or authenticate or access a personal online account in the presence of the employer; or prohibit requiring a current or prospective employee to add another employee, supervisor, or administrator to the list or contacts associated with the employee’s social media account.

Employers also increasingly are turning to “algorithmic hiring” methodologies that rely on analytic and job testing software to replace human judgment when making hiring decisions. An algorithm is a process or set of rules to be followed in calculations or other problem-solving operations (typically using a computer), from calculating simple averages to performing complex statistical analyses. When evaluating applicants, algorithmic data can include résumés, publicly available information, as well as responses to candidate assessments that delve into personality, temperament, aptitude for skills such as problem solving. The rules and operations of this calculation might be as simple as a spreadsheet that consolidates multiple ratings of a candidate’s potential or as complex as state-of-the-art predictive analytics. Some hiring algorithms correlate candidate data with employment outcomes such as productivity and performance ratings.

According to ongoing studies for the National Bureau of Economic Research (“NBER”), the use of personality tests is a more effective way for employers to identify the best hires.
versus the traditional use of human discretion in hiring decisions. The researchers compared the longevity of employees hired solely with human feedback, versus those that were hired based on the algorithmic recommendations of personality test results. The study found that hires based on the algorithm produced better employees who had longer employment tenures. The study concluded that when faced with similar applicant pools, managers who exercise more discretion (as measured by their likelihood of overruling job test recommendations) systematically end up with worse hires.

The same study also concluded that “placing more weight on test scores may improve hiring decisions by reducing the influence of human bias or mistakes.” In other words, algorithms when used properly tend to eliminate (or at least limit) managerial bias (including the “unconscious” variety) from hiring decisions. However, this “Moneyball” approach to hiring does not (yet) work for executive recruitment given the insufficient available data and the small number of positions at that level.

By the same token, reliance on data analytics and test results may lead to unintended consequences and unlawful hiring decisions when the underlying data is flawed, misapplied, or not validated for employment assessment. Title VII provides that employers may “give and act upon the results of any professionally developed ability test provided that such test, its administration or action upon the results is not designed, intended or used to discriminate because of race, color, religion, sex or national origin.” However, those who challenge such tests frequently claim they disparately impact minority applicants and/or employees from hiring and promotion decisions. While most personality tests are facially neutral, by using them, employers risk allegations of inadvertent discrimination through the use of otherwise valid personality assessment tools.

Another potential risk of using data analytics in hiring may arise even before applicants are directly screened. In December 2017, the Communications Workers of America (“CWA”) filed a class action lawsuit against hundreds of large employers for allegedly excluding older workers from receiving job ads on Facebook for open positions at their companies. The lawsuit alleges that the companies and their employment agencies were illegally targeting their employment ads on Facebook (using algorithms) to exclude older workers who fall outside of specified age ranges (such as ages 18 to 40), thereby preventing older workers from seeing the ads or pursuing job opportunities. The case remains in litigation, but some of the defendants have sought dismissal, in part, by arguing that the content of the job ads in question are “facially neutral” and that the ads are available to all persons regardless of age through a wide variety of outlets, including publicly available websites.

On March 19, 2019, Facebook announced a settlement of a number of such lawsuits filed against it, in which the company agreed to no longer let businesses buy targeted ads that potentially discriminate against users who are women, people of color, or elderly. Under the

---

16 Id.
17 Id.
20 The EEOC warns that personality tests become problematic when an employer uses them in an intentionally discriminatory way, or when such tests “disproportionately exclude people in a particular group by race, sex, or another covered basis, unless the employer can justify the test or procedure under the law.” EEOC, Employment Tests and Selection Procedures Fact Sheet, December 2007.
21 [https://www.law360.com/articles/1119434](https://www.law360.com/articles/1119434)
settlement, Facebook agreed to withhold a wide array of detailed demographic information—including gender, age and zip codes, which are often used as indicators of race—from advertisers when they market housing, credit and job opportunities.

V. THE ROLE OF TECHNOLOGY IN A CHANGING WORKFORCE

The traditional 9 to 5 job, with a single employer, no longer applies to a substantial portion of the workforce. Empirical studies suggest that 16% to 27% of the U.S. workforce are now employed as “Independent Workers” – commonly referred to as “gig” workers. At least one study suggests that the number of individuals who are likely to participate in independent work in the future could rise to between 76 and 129 million individuals. As of 2017, thirty-one million individuals in the U.S. workforce derived their primary source of income from independent work, and another thirty-six million individuals supplement their income through gig work.

A. Risk Areas and Solutions to Address Risk

Gig work focuses on three key features: (1) a high degree of autonomy, control, and flexibility in determining workload and work portfolio; (2) payment by task, assignment, or sales; and (3) a short-term relationship between the worker and the customer. The growth of gig work—and in particular the technological innovations that foster such relationships, such as texting, smart phones and their “apps,” and remote work arrangements—has led to a number of legal risks.

1. Worker Classification Issues

One legal issue that has garnered headlines involves the “gig economy” and the alleged misclassification of those offering their services through the applicable technology. A host of lawsuits have been filed in California, Massachusetts, and other states asserting individual and class action claims under state and federal law over the alleged misclassification of gig workers as independent contractors. Derivative claims tied to this alleged misclassification include failure to provide minimum and overtime wages, wage statement violations, reimbursement claims, and meal and rest break violations.

Companies relying heavily on a supply of independent workers face a heavy challenge, as a 2006 Government Accountability Office Report stated: “The tests used to determine whether a worker is an independent contractor or an employee are complex, subjective, and differ from law to law.” Moreover, as varied as the tests are under federal law, many states are even more complex and varied, having been referred to as a “crazy quilt set of state laws.”

The consequences of misclassification can result in significant damages, with liability exposure in the millions, if not tens of millions, of dollars, including back pay and liquidated damages; back taxes, interest, and penalties; disqualification of company benefit plans; overtime liability if a contractor is deemed to be non-exempt; attorneys’ fees; and potential criminal liability.

While several legal tests exist for determining independent contractor status, most of them focus on the same general factors, including: (1) who controls the manner, method, and means of performance; (2) whether opportunities for profit or loss exist; (3) who provides the equipment and pays expenses; (4) the length of the relationship; (5) whether the services provided are an integral part of the business; and (6) the degree of the skill required. Other factors often considered in this analysis include whether benefits are provided, the intent of the
parties, and whether the individual is paid on a 1099 or W-2, is free to hire helpers or employees, is able to work elsewhere or have another business, and can or does operate as a separate legal entity.

2. Timekeeping Issues

Timekeeping issues can arise when employers allow employees to have flexible work arrangements and fail to acknowledge that workers who do not qualify as independent contractors must be compensated for all time “worked,” including activities such as answering texts and emails from managers and customers during all hours of the day or night, and expectations that the employee “check-in” on line.

The vast majority of modern class and collective actions seeking unpaid compensation (i.e., so-called off-the-clock or unpaid overtime cases) rely on IT-derived data, much of which is passive in nature (i.e., running in the background and metadata), or actively tracking employee conduct and behavior. These may include:

- Facility access (electronic and sign in) records;
- Computer terminals and related login and logout data;
- Emails sent and reviewed by employees;
- Text messages;
- Video surveillance;
- Equipment utilization meters;
- GPS tracking.

Not only are these sources of evidence often maintained, making them relevant for production in any alleged unpaid time litigation, but they are usually very costly to access, produce, and have analyzed, as will always be required in such cases.

3. Disability Accommodation Issues and Technological Advances

The rise of a more flexible, remote and technologically dependent (and savvy) workforce—one in which employees may be working remotely or on a reduced schedule or temporary basis—also presents employers with accommodation issues for workers with disabilities. For example, technological advancement continues to blur what constitutes direct communication in the workplace, particularly as millennials and their even younger Gen-Z compatriots alter the very essence of workplace communications (the much maligned trope of millennials texting to one another in the same room comes to mind). Thus, the age-old “essential” duty of having to report to a specific worksite is becoming increasingly challenged, especially in technology-driven jobs where monitoring is already relegated to AI-related technologies.

In the same vein, the rise of robotics and AI in the workforce suggests an expansion of potentially available accommodations for workers with disabilities. For example, the advent of so-called “augmenting robotics” (the science of robots that enhance capabilities a person already has, or replace capabilities that a person has lost) may soon require employers to consider previously unimaginable accommodations in the workplace. These include augmenting medical devices, such as a prosthetic limb. Modern prosthetics can be complex electronic devices that learn to respond to neural signals sent by the brain. Some prosthetic arms can be connected to muscles in the chest so that the individual moving those muscles can cause the arm to move in characteristic ways. This is a process called targeted muscle reinnervation.
Other examples of this rapidly evolving augmenting robotic technology are so-called “exoskeletons.” There are several examples of exoskeletons in development that can enhance a person’s existing capabilities (as opposed to prosthetics, which give a person a missing capability). The aim of these systems is typically to augment human strength without sacrificing speed or agility. However, some of these exoskeletons could eventually be used to allow individuals who are paralyzed, or suffering from some neuro-muscular disease like multiple sclerosis or Lou Gherig’s disease, to recover a full range of motor abilities. Some examples of exoskeletons are the Raytheon XOS2, the Hybrid Assisted Limb (HAL), and the eLegs from Berkeley Bionics.
Work Reconstructed: Risks and Solutions in the Digital Era

Presenters
Jennifer Monrose Moore (Tampa)
Tibor Nagy Jr. (Tucson/Phoenix)

Moderator
Gary D. Eisenstat (Dallas)

“Bring Your Own Device”
Risks & Rewards
Bring Your Own Device

Yesterday, your only female Sales Supervisor came to speak to you with concern in her voice. She told you that over the weekend her teenage daughter used her smartphone to pay her cheerleading club dues on the Sales Supervisor’s Venmo account. The daughter asked her mother why her “boss” – the Sales Manager – pays for “Hookers and Beer.” The Sales Supervisor said she scrolled down and saw several “Hookers and Beer” payments on the Venmo feed. She is very uncomfortable working for someone who disrespects females.

Later that night, you notice that the Sales Supervisor’s daughter posted a Facebook post of the “Hookers and Beer” screenshot with the #MeToo notation tagging her mother on the Sales Supervisor’s Facebook page.
Security Issues: Could This Really Happen?

- Lost or stolen devices.
- Family use of device – hacked.
- Terminated employees.
  - Remote wiping.
  - External drives and cloud accounts.

Duty to Preserve, Destroy, or Produce Electronic Data?

- Financial Sector – e.g., Fair Credit Reporting Act.
- Health Sector – HIPAA obligations.
- Duty to notify customers in event of breach?
- Litigation Spoliation
- Other applicable laws?
Litigation – Duty to Preserve

Documents (includes electronic communications and digital versions) must be produced if within a party’s “possession, custody, or control.”
(F.R.C.P. 34)

Is a personal device still in the company’s “possession, custody, or control?”
If so, and data is not preserved?

➢ **SANCTIONS:**
  ➢ Spoliation Instruction.
  ➢ Dismissal of Claims.
  ➢ Monetary Sanctions.

LABOR & EMPLOYMENT ISSUES

Use and content of personal device (e.g., sexual harassment, inconsistent application of company rules).
Fair Labor Standards Act – Off-the-Clock

What Might be Compensable?

➤ Texts after hours from a boss to non-exempt staff about follow-up tasks.
➤ Weekend emails from a manager giving assignments or “to-dos.”
➤ Such activities may be compensable depending on frequency, duration, and extent of work.
➤ Texts and emails create a clear record.

What to do

1. Is BYOD Advisable?
   If so, for everyone?
2. Technology Solutions?
   Virtualization apps (remote access but no storage).
   Walled garden (personal data segregated from work data).
   Limited separation.
3. Agreements with Employees
   a. Rights to inspect during and after employment (no privacy expectation).
   b. Rights to wipe, including remotely.
   c. Rights regarding external drives and cloud accounts.
   d. Require a list of all devices.
   e. Require immediate reporting of lost/stolen devices.
What to do

4. Require Password Protection.
5. Periodic IT Forensic Examinations.
7. Understand the Sources of Data: documents, emails, texts, voicemails, etc.
   Establish appropriate record keeping, policies and procedures.

   Issue promptly when litigation is reasonably anticipated.
   Know:
   • Who gets the letter.
   • Type and location of evidence.
9. Establish and consistently enforce appropriate device use rules.
10. FLSA – establish clear rules for after-hours work.
What to do

11. Know destruction, retention, reporting obligations – FCRA, HIPAA, ERISA, ... .

12. Become Tech Savvy:
   – Collaborate closely with IT.
   – You can’t plan for what you don’t understand. Stay current!
     Apps: Snapchat, CyberDust, etc.
     Cloud Accounts: iCloud, Dropbox, Google Drive, Evernote, etc.
GIG Economy — Defined

- Short-term engagements
- Freelance work

GIG Economy — How Big Is It?

- Per Gallup Polls: 57 million workers (one-third of U.S. workers)
- Per the Bureau of Labor Statistics — No one knows for sure . . .
GIG Workers

How many “gig” workers has your company hired in the last 12 months?

A. 0  
B. Under 10  
C. Under 100  
D. Over 100

Why the Growth in the GIG Economy?

Possible explanations:

- Economic necessity
- Generational values
- Technological changes
Economics and the Millennial Culture

- Average Millennial job tenure — 2 years
- Millennial entrepreneurial bent
- 74% want flexible hours
- High debt load — 2019 student debt passed $1.5 trillion!

Technology Advancements — AI and Robotics

“Work” Redefined

Jobs vs. Tasks —

- Simplicity vs. Complexity
- Repetition vs. Variability
- Independence vs. Interaction
- Physical vs. Mental / Analytical
“Tasks” Analysis

- What tasks actually need to be done?
- By whom or what?
- Can it be automated?
- Can it be outsourced, e.g., ride sharing?

Department of Labor Administrator’s Interpretation AI No. 2015-1 (Ex. B)

U.S. Department of Labor
Wage and Hour Division
Washington, D.C. 20210

Administrator’s Interpretation No. 2015-1

July 15, 2015

Issued by ADMINISTRATOR DAVID WEIL

GIG Worker Compliance

- Back taxes and lower tax revenue for federal/state government
- Social Security and Medicare taxes
- Workers’ Compensation
- Interest and civil penalties
- Criminal penalties
- IRS Audits
- State/DOL Audits
- Back wages and liquidated damages
- Health insurance and benefits (e.g., pension plan)
- Coverage under federal/state employment laws
- Uneven playing field for employers who properly classify workers

GIG Compliance Concerns

Trade Secret Protection —

- Who knows what and why?
- How is information communicated and protected with “task” reorganizations?
- NDAs?
GIG Compliance: Worker Classification Issues

- Employee vs. Independent Contractor
- FLSA Considerations
- Title VII and other liability risks

Workforce Retooling Issues

Job elimination and restructuring —

- Who is selected?
- Criteria used?
- Adverse impact analysis?

Collective Bargaining Agreements?
Common Mistakes

- Large percentage of workforce classified as independent contractors.
- Services performed are the essence of or integral to the business.
- Reliance on “industry” practice.
- Longstanding relationships of one year or more.
- Performing same work as an employee.
- Rehired as consultant but performing the same work as when employed.

Key Preventive Measures to Maintain Independent Contractor Status

1. Carefully drafted independent contractor agreement;
2. Separate policies/procedures;
3. Review benefit plans;
4. Management training;
5. Periodic audits; and
6. Avenue to raise business concerns.
Independent Contractor Agreements: Key Provisions

- Contractually declare independent contractor status.
- Avoid provisions suggesting that the company controlled the manner and means of the work.
- Include waiver of benefit provisions (e.g., right to receive retirement benefits, health insurance, etc.).

Independent Contractor Agreements: Key Provisions (Cont’d.)

- Require fee and invoicing payments – not steady salary compensation.
- Require contractors to purchase own business, workers’ compensation, and unemployment insurance.
- Permit contractors to work for others.
- Require contractors to pay their own expenses and taxes.
1. Maintain Separate Policies and Procedures
   - Different terms and conditions from employees (including separate internal management procedures/guidelines).
   - Different terminology/jargon.
   - Payment and ledger records.
   - Advertisements and public disclosures.
   - Rule of thumb: Assume jury/judge will see all internal documents!

and, most importantly, BE CONSISTENT!

2. Review Benefit Plans
   - Ensure benefit plans clearly define who is (and who is not) a plan participant.
   - Explicit exclusion of independent contractors—regardless of whether they are later deemed to be company employees.
   - Ensure terms of benefit plans are consistent with only employees receiving benefits.
3. Management Training

- Knowledge of the contract.
- Emphasize *new* type of relationship—differences in how to treat independent contractors vs. employees.
- Use correct terminology:
  - Independent contractor, *not* employee
  - Advise, *not* supervise
  - Breach of contract, *not* discipline
  - Retain or engage, *not* hire or employ
  - Terminate contract, *not* fire/discharge
  - Careful preparation of documents, including email, utilizing correct terminology
  - Develop sample breach scenarios

4. Periodic Audits

You have a carefully drafted agreement, you have trained your management, you have reviewed your benefit plans, . . . *BUT what is really going on out there?*
Social Media in the Workplace

- Privacy Concerns
- Recruitment and hiring
- NLRB considerations and protected speech

Employee Privacy in Social Media

- “Invasion of Privacy”
  - Does the employee have a “reasonable expectation of privacy?”
  - Key Question: Is the profile accessible to the public at large or only through friends?
- Employers are NOT prohibited from viewing publicly available content
- Problems arise when employers deceptively access social media
- Trend: Employee privacy interest outweighs employer need for access to private social media accounts
  - Don’t require employees to provide social media usernames and passwords
  - Don’t require employees to accept supervisors or co-workers as “friends” or “followers”
Personal Information Research on Social Media: What could possibly go wrong?

Big brother is watching …

When recruiting employees at your company, do you or your recruiting staff “research” an applicant’s social media profile?

A. Yes

B. No.

C. What’s a social media profile?
Big brother is watching ...

70% of employers use social networking sites to research job candidates during hiring process

TMI?

<table>
<thead>
<tr>
<th>Basic Info</th>
<th>Basic Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sex: Male</td>
<td>Sex: Male</td>
</tr>
<tr>
<td>Interested In: Men</td>
<td>Interested In: Women</td>
</tr>
<tr>
<td>Religious Views: Christian</td>
<td>Religious Views: Atheist</td>
</tr>
<tr>
<td></td>
<td>Relationship Status: Married</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Who's Checking and Why?

- Employers who use social networking sites to research potential job candidates are looking for:
  - Information that supports their qualifications for the job: 58 percent
  - If the candidate has a professional online persona: 50 percent
  - What other people are posting about the candidate: 34 percent
  - A reason not to hire the candidate: 22 percent

Big brother is watching ...

If you have “researched” an applicant’s social media profile, has what you found influenced you not to hire the candidate?

A. Yes
B. It caused me to do more research on the candidate
C. It caused me to contact our lawyers
D. No
Big brother is watching ...

Over half of employers (57%) have found content on social media that caused them NOT to hire a candidate.

Content that causes employers NOT to hire a candidate:
- Job candidate posted provocative or inappropriate photographs, videos, or information (40%)
- Job candidate posted information about them drinking or using drugs (36%)
- Job candidate had discriminatory comments related to race, gender, religion, etc. (31%)
- Job candidate was linked to criminal behavior (30%)
- Job candidate lied about qualifications (27%)
Big brother is watching …

Content that causes employers NOT to hire a candidate:
- Job candidate had poor communication skills (27%)
- Job candidate bad-mouthed their previous company or fellow employee (25%)
- Job candidate’s screen name was unprofessional (22%)
- Job candidate shared confidential information from previous employers (20%)
- Job candidate lied about an absence (16%)
- Job candidate posted too frequently (12%)

Big brother is watching …

Content that caused employers to be MORE likely to hire:
- Job candidate’s background information supported their professional qualifications for the job (37%)
- Job candidate was creative (34%)
- Job candidate’s site conveyed a professional image (33%)
- Job candidate was well-rounded, showed a wide range of interests (31%)
- Got a good feel for the job candidate’s personality, could see a good fit within the company culture (31%)
- Job candidate had great communications skills (28%)
Content that caused employers to be MORE likely to hire:

- Job candidate received awards and accolades (26%)
- Other people posted great references about the job candidate (23%)
- Job candidate had interacted with company’s social media accounts (22%)
- Job candidate posted compelling video or other content (21%)
- Job candidate had a large number of followers or subscribers (18%)

Do you ever “check on” current employees on social media, such as their Facebook pages?

A. Yes

B. No.
Big brother is watching ...

Nearly half of employers (48%) check up on current employees on social media.
10% do it daily!

Big brother is watching ...

Has an employee’s online social media posts ever influenced you to reprimand or terminate that employee (or another employee)?

A. Yes
B. No.
C. I plead the Fifth.
Big brother is watching ...

A third of employers have reprimanded or fired an employee based on content found online.

Recruitment and Hiring – Best Practices

- **Adopt and enforce a standard social media search policy:** Ensure all candidates are subject to the same social media background check.
- **Notify the candidates that publicly-available social media will be searched.**
- **Separate the Social Media Researcher:** Don’t let hiring committee members view applicant’s social media. Use a designated employee.
- **Search only information publicly-available:** Never ask candidates to provide passwords, accept friend requests, or otherwise disclose private social media information.
- **Delay the social media search until after the initial interview:** This will avoid allegations that the employer improperly awarded/withheld interviews based on protected classifications.
- **Only look for specific things to report to hiring committee:** Inappropriate photos; ties to a competitor; opposition to your business.
- **Document the reasons and notify the candidate:** If the candidate is not hired because of information learned, document the reasons and notify the candidate of the reason.
Gen Z* – Pulling the Curtain Shut

- Only about 1 in 10 teenagers say they share personal, religious, or political beliefs on social media.
- Gen Z has grown up with social media – cognizant of their image from an early age.
- Regularly “clean up” their online profiles – “re-curating”
  - Use clean-up apps like “TweetDelete”

*Age 22 or younger. Also referred to as “iGen” – is the post-millennial generation responsible for “killing” Facebook and for the rise of “TikTok.”

Beware of Apps & Ads that Target Mainly Young People

CWA Class Action Case

- National employers allegedly used Facebook to target job ads at younger workers (e.g., 18-40)
- ADEA “publication provision” – job ads can’t indicate preference or limit based on age
- Akin to job ads seeking recent college graduates, only worse
- Employers argue:
  - Facialy neutral ads and FB ads only part of the picture
  - Pre-Facebook ads placed in other media with discrete demographics
Targeted Advertising on FB Curtailed

- Facebook will no longer:
  - Let businesses buy targeted ads on the platform which may potentially discriminate against users who are women, people of color, or elderly.
  - Allow advertisers to target users by age, gender, or zip code if the ads are related to housing, employment, or credit offers. Ads related to other products and services will not be held to this standard.

The NLRB and Protected Speech

- NLRB: “10 to 20 percent of our case load has a social media component”

- NLRB enforces the National Labor Relations Act (NLRA)

- Applies to union and non-union employers
Concerted Activity on Social Media

- Unique social media issues
  - Facebook “Likes”
  - “Tagging” co-workers
  - Twitter “Re-Tweets”

“[Manager] is such a nasty MOTHER F***ER don’t know how to talk to people!!! F**k his mother and his entire f****ing family!!! What a loser!!! Vote yes for the Union!!!!!!!!”

Concerted Activity on Social Media

- While SM comments at the “outer-bounds of protected, union-related comments,” 2nd Circuit agreed that the employee’s conduct was *not* so opprobrious or egregious as to lose the protection of the NLRA
  - “Totality of the circumstances test” adequately balances an employer’s interest
  - Employer had not disciplined others for using such language
  - Employee was provoked by “tense debate over managerial mistreatment in the period before the representation election”

NLRB General Counsel’s New Employer Handbook Guidance

- NLRB reassessed its standard for when mere maintenance of a work rule violates Section 8(a)(1) *The Boeing Company* (2017)
- GC’s Guidance created 3 new rule categories:
  - Presumptively lawful
  - Warrants individualized scrutiny
  - Presumptively unlawful
Category 1 Rules: Presumptively Lawful

- Generally considered presumptively lawful if, when reasonably interpreted, they do not prohibit or interfere with NLRA rights or because potential impact on rights outweigh by the business justifications associated with the rules.
  - Civility Rules
  - No-Photography Rules and No-Recording Rules
  - Disruptive Behavior Rules
  - Rules Protecting Confidential, Proprietary, and Customer Information or Documents
  - Rules against Defamation or Misrepresentation
  - Rules against Using Employer Logos or Intellectual Property
  - Rules Requiring Authorization to Speak for Company
  - Rules Banning Disloyalty, Nepotism, or Self-Enrichment
  - Rules Against Insubordination, Non-cooperation, or On-the-job Conduct that Adversely Affects Operations

Category 2 Rules: Warrant individualized scrutiny

Not obviously lawful or unlawful, must be evaluated on a case-by-case basis.

- Broad conflict-of-interest rules that do not specifically target fraud and self-enrichment
- Confidentiality rules broadly encompassing “employer business” or “employee information”
- Rules regarding disparagement or criticism of the employer
- Rules regulating use of the employer’s name
- Rules generally restricting speaking to the media or third parties
- Rules banning off-duty conduct that might harm the employer
Category 3 Rules: Presumptively Unlawful

Confidentiality Rules Specifically Regarding Wages, Benefits, or Working Conditions such as:

- Rules prohibiting disclosure of wages, salaries, commissions, or contents of employment contracts
- Rules against making false or inaccurate statements
- Rules against joining outside organizations
- Rules prohibiting disclosing to any media source information regarding employment at the and working conditions

---

Work Reconstructed: Risks and Solutions in the Digital Era

Presenters
Jennifer Monrose Moore (Tampa)
Tibor Nagy Jr. (Tucson/Phoenix)

Moderator
Gary D. Eisenstat (Dallas)