MAY 2023

CLEARSTAR®

SCREENING COMPLIANCE UPDATE

CLEARSTAR OFFERS EEOC GUIDELINES COMPLIANCE ON CRIMINAL BACKGROUND CHECKS, GDPR & SOC TYPE 2 SECURITY CONTROL COMPLIANCE AND STAFFING COMPLIANCE.

Compliance is one of the most important parts of background screening, it involves following the rules and regulations set forth by the Fair Credit Reporting Act and local ordinances.

CLICK FOR PAST UPDATES

CLEARSTAR®

TABLE OF CONTENTS

SCREENING COMPLIANCE UPDATE | MAY 2023

Clearstar is happy to share the below industry related articles written by subject matter experts and published on the internet in order to assist you in establishing and keeping a compliant background screening program.

FEDERAL DEVELOPMENTS

HUD Outlines its Action Plan to Remove Unnecessary Barriers to Housing for People with Criminal Records

In weeks ahead, HUD will introduce rulemaking, establish a process for individualized assessments, and outline guidelines for public housing authorities. HUD Secretary challenges public housing authorities to review current processes.

U.S. Department of Housing and Urban Development (HUD) Secretary Marcia L. Fudge announced further steps HUD will take to ensure that qualified people are not denied the opportunity to access housing solely due to a criminal history record. In the weeks ahead, HUD will issue a Notice of Proposed Rule Making in which it proposes to change its regulations governing public housing agencies and HUD-subsidized housing providers to prevent unnecessary denials of housing assistance to people with criminal history records.

HUD will issue new guidance and technical assistance to assist PHAs and HUD-affiliated owners in determining what convictions are relevant to health and safety and how to conduct an individualized assessment when reviewing criminal history records. HUD will also provide technical assistance to encourage grantees, PHAs, and housing owners to use HUD programs to provide housing and services that support people's successful reentry from prisons and jails to the community, which enhances public safety.

"This Fair Housing Month and Second Chance Month, HUD recognizes that current criminal justice and housing policies have denied those seeking rehabilitation a chance to lead better lives," said **HUD Secretary Marcia L. Fudge**. "A year ago, I called on HUD programs to conduct a policy review of ways that we can remove barriers to safe, affordable housing for people with criminal history records. As we execute our action plan, I invite state and local housing agencies, owners, and property managers to partner with HUD to remove barriers to housing to people with criminal records and support people's successful reentry to the community. Research shows that providing safe and affordable housing and supportive services so that people succeed during reentry makes our communities stronger and safer."

The announcement follows a comprehensive review of HUD regulations, policies, and guidance geared toward increasing opportunities for qualified individuals and families to receive housing assistance from HUD. That review found that many of HUD's regulations and sub-regulatory provisions could be improved and clarified to ensure that PHAs and HUD-affiliated owners are following recognized best practices, including:

- Not automatically denying an applicant housing assistance simply based on the presence of a criminal conviction, other than where explicitly prohibited by federal law.
- Disregarding criminal history that is unlikely to bear on fitness for tenancy, such as arrest records, sealed or expunged records, older convictions, and convictions not involving violence or harm to persons or property.
- Using individualized assessments to determine whether applicants truly pose a future risk to persons or property, taking into account other factors such as the applicant's employment, engagement in alcohol or drug treatment, and constructive community involvement.
- Providing applicants with criminal history records with reasonable time and opportunity to provide supporting information regarding mitigating factors before an admission decision is made.

Many of these principles have already been implemented by many housing providers and public housing agencies who, in doing so, have preserved or improved the public safety of their communities. HUD's forthcoming notice of proposed rulemaking will propose to require other housing providers and PHAs to do the same.

New guidance and technical assistance issued by HUD will assist PHAs and HUD-affiliated owners in applying these principles.

HUD's forthcoming actions also will help PHAs and HUD-affiliated owners comply with the Fair Housing Act. Black and Brown people, other people of color, and people with disabilities are disproportionately involved in the criminal justice system. As a result, policies that unnecessarily deny housing because of a criminal history record can violate the Fair

Housing Act of 1968, pursuant to the discriminatory effects rule that HUD recently reinstated. To ensure these reforms are successfully implemented, HUD is also stepping up Fair Housing investigations and enforcement. Fair Housing staff and grantees receive numerous complaints where exclusions based on criminal history records discriminate based on race, disability, or other protected classes.

In addition to addressing barriers to HUD housing assistance, HUD will also provide new tools and technical assistance on ways that HUD programs can support the successful reentry to the community from prisons and jails. For example, HUD will highlight communities that are using Community Development Block Grants to provide reentry services and programs, including counseling and legal assistance, and PHAs that are partnering to provide housing assistance to people reentering the community. HUD will also highlight ways that Emergency Solutions Grants and Continuum of Care Program grants can create models of housing to address homelessness among formerly incarcerated people. Taken together, these approaches make our communities stronger and safer.

The proposals announced today will codify protections against housing discrimination as HUD works to provide secure avenues for successful community-oriented rehabilitation and reentry.
CLICK HERE.

CFPB Says Furnishers' Investigative Duties Extend to Legal Disputes

On April 20, the CFPB filed an amicus brief in a case before the U.S. Court of Appeals for the Eleventh Circuit arguing that the duty to investigate a consumer's credit dispute applies not only to factual disputes but also to disputes that can be labeled as legal in nature. The plaintiffs entered into a timeshare agreement with the defendant hotel chain and made monthly payments for nearly two years but then stopped. The plaintiffs disputed the validity of, and attempted to rescind, the agreement. The defendant did not agree to the rescission and continued to record the deed under the plaintiffs' names. The plaintiffs later obtained copies of their credit reports, which showed past-due balances with the defendant, and subsequently submitted letters to a credit reporting agency (CRA) disputing the credit reporting. After the defendant certified the information was accurate, the plaintiffs sued the defendant and the CRA alleging that the defendant violated the FCRA by failing to conduct a proper investigation. The defendant moved for summary judgment, arguing that the issue of whether the debt is owed—the basis of the plaintiffs' FCRA claim—constitutes a legal dispute and is not a factual inaccuracy. The defendant further maintained that there was no legal error because the plaintiffs owed the money as a matter of law. Last December, the U.S. District Court for the Middle District of Florida granted partial summary judgment in favor the defendant after concluding, among other things, that because the plaintiffs' dispute centered on the legal validity of their debt, rather than a factual inaccuracy, the investigation requirement was not triggered and the claim was "not actionable under the FCRA."

The Bureau argued in favor of the plaintiffs-appellants. According to the Bureau, the district court "unduly narrow[ed] the scope of a furnisher's obligations by holding that furnishers categorically need not investigate indirect disputes involving 'legal' inaccuracies." This position, the Bureau maintained, contradicts the purpose of the FCRA's requirement to conduct a reasonable investigation of consumer disputes and "could reduce the incentive of furnishers to resolve 'legal' disputes, and, in turn, could increase the volume of consumer complaints about credit reporting issues that the Bureau receives and devotes resources to address."

Explaining that the FCRA does not distinguish between legal and factual disputes, the Bureau stated that the district court's conclusion "is not supported by the statute, risks exposing consumers to more inaccurate credit reporting, conflicts with the decision of another circuit, and undercuts the remedial purpose of the FCRA." The Bureau presented several arguments to support its position, including that a reasonable investigation is required under the FCRA, and that while the reasonableness of an investigation is case specific, it "can be evaluated by how thoroughly the furnisher investigated the dispute (e.g., how well its conclusion is supported by the information it considered or reasonably could have considered)."

The Bureau also claimed that the Congress did not intend to exclude disputes that involve legal questions. "[M]any inaccurate representations pertaining to an individual's debt obligations arguably could be characterized as legal inaccuracies, given that determining the truth or falsity of the representation could require the reading of a contract," the Bureau wrote. Moreover, an "atextual exception for legal inaccuracies will create a loophole that could swallow the reasonable investigation rule," the Bureau stressed. The agency urged the court to "reject a formal distinction between

factual and legal investigations because it will likely prove unworkable in practice" and said that allowing such a distinction would "curtail the reach of the FCRA's investigation requirement in a way that runs counter to the purpose of the provision to require meaningful investigation to ensure accuracy on credit reports."

As previously covered by InfoBytes, the CFPB and the FTC filed an amicus brief presenting the same arguments last December in a different FCRA case on appeal to the 11th Circuit involving the same defendant.
CLICK HERE.

DOT Expands Drug Testing Options to Include Oral Fluid

The Department of Transportation on Monday filed a Final Rule that will allow oral fluid as an authorized testing method for the presence of unlawful drugs. The 227-page final rule is scheduled for publication in the Federal Register May 2 and will become effective 30 days later.

In order for an employer to implement oral fluid testing under DOT's regulation, the U.S. Department of Health and Human Services (HHS) will need to certify at least two laboratories for oral fluid testing, which has not yet been done. In essence, the DOT on Monday cleared a regulatory hurdle that allows for oral fluid testing, but those tests are not yet authorized until HHS makes its certifications.

DOT in February proposed amending the transportation industry's drug testing program procedures regulation to allow oral fluid testing in lieu of urine testing, giving "employers a choice that will help combat employee cheating on urine drug tests and provide a less intrusive means of achieving the safety goals of the program."

The measure comes as the number of drivers flagged for drug infractions continues to climb at a break-neck pace. As of January 1 last year, 81,052 professional drivers were in Prohibited Status with FMCSA's Drug and Alcohol Clearinghouse with a violation. A year later that number reached 120,345, and less than nine weeks ago was at 125,810.

Oral fluid collection mitigates cheating since the test is administered face-to-face, usually with a sample collector swabbing inside the cheek of an applicant, and the DOT contends "adding oral fluid testing as an option is consistent with the careful balancing of an individual's right to privacy with the Department's strong interest in preserving transportation safety by deterring illicit drug use."

Prior to Monday's issuing of the Final Rule, urinalysis and blood analysis (in limited circumstances) were the only acceptable means to conduct DOT drug screenings.

Among benefits for trucking companies of oral testing, DOT said, are that it's generally cheaper than urine testing (DOT estimates between $10 and $20 cheaper per test versus urine). DOT also notes that by giving the option of both urine and oral testing, employers can use one or the other depending on the situation due to the different detection windows associated with each.

The department says the generally narrower detection window offered by oral fluid testing could give fleets a better chance at detecting recent drug use, such as for a post-accident drug test, adding "while oral fluid testing may provide a better indicator of an employee's recent use of the drug, it also detects frequent users... [but] we note that oral fluid windows of detection will likely be shorter than for urine. Employers, working in conjunction with their service agents, should determine whether urine or oral fluid collection is best for their program and in what contexts."

There has been an ongoing push to recognize hair testing. The FAST Act transportation bill, signed into law by President Obama in December 2015, allows for hair follicle drug testing as a DOT-approved method, but not until HHS establishes guidelines for testing. The FAST Act mandated that those guidelines be developed within a year of the FAST Act becoming law, but HHS did not publish proposed guidelines until September 2020. HHS has not yet issued a final version of those guidelines.
CLICK HERE.

DOT Rule Allows Oral-Fluid Specimen Testing for Drugs

It's been a long time in the works, but the U.S. Department of Transportation has published a final rule that amends the federal regulated industry drug-testing program to include oral fluid specimen testing as an alternative to urinalysis. This adjustment aims to alleviate privacy concerns over the collection of urine samples in terms of constitutional protections against invasive searches and seizures.

"This additional methodology for drug testing will give employers a choice that will help combat employee cheating on urine drug tests and provide a less intrusive means of achieving the safety goals of the program," DOT stated in its notice, to be published in the *Federal Register* for May 2, 2023.

Another Delay from HHS

While the final rule is effective 30 days from date of publication, DOT clarified that before an employer may implement oral fluid testing, the Department of Health and Human Services (DHHS) will need to certify at least two laboratories to handle the testing.

There must be one HHS-certified laboratory to conduct the screening and confirmation drug testing on the primary specimen. And there must be a different HHS-certified laboratory to conduct split specimen drug testing on the secondary specimen, if the employee requests split specimen testing for a non-negative result. As of now, DOT stated that "HHS has not yet certified any laboratories to conduct oral fluid testing."

The rule enables employers to use oral fluid testing instead of urine testing — it does not require that they do so. Instead, the aim is to afford employers flexibility in the type of specimen they collect.

As DOT sees it, that flexibility will provide key benefits. For example, when an employer determines that a DOT post-accident or a reasonable cause/ suspicion test is needed, oral fluid collection could be done at the scene of the accident or incident. The collection could be done by any oral fluid collector qualified under Part 40 — either an external contractor or a DOT-regulated company employee. Also, there are fewer requirements for oral fluid collection sites.

Nor is the agency proposing to eliminate urine testing. There are different windows of detection that employers should consider when deciding whether to use a urine test or an oral fluid test as the preferred form of testing for any specific test reason, including the window of detection. Probably the largest difference in the testing window is for marijuana. The oral fluid testing window for cannabis is only up to about 24 hours; for urine testing, it's anywhere from 3 to 67 days.

Detecting Recent Drug Use vs. Identifying a Pattern

If an employer is looking to detect recent drug use, (i.e., reasonable cause/suspicion, post-accident), the more immediate window of detection associated with oral fluid specimens may be acceptable for the company. However, if an employer is looking to detect a pattern of intermittent drug use through pre-employment, random, return-to-duty, and follow-up testing, the delayed windows of detection afforded by urine samples may be preferred.

The advantage of oral fluid collection, according to DOT, is that it can be directly observed, as opposed to most urine collections, which are unobserved.
CLICK HERE.

EEOC Offers "Promising Practices" for Battling Workplace Harassment

The Equal Opportunity Employment Commission (EEOC) released what it describes as "" with detailed recommendations in the categories of (1) Leadership and Accountability, (2) Comprehensive and Effective Anti-Harassment Policy, (3) Effective and Accessible Anti-Harassment Program and (4) Effective Anti-Harassment Training.

While specifically aimed at anti-harassment efforts in federal agencies, the EEOC guidance expressly notes the practices are helpful for employers in the private sector. Some of the EEOC's relevant recommendations applicable to private workplaces are as follows:

Leadership and Accountability

- Issue and distribute to all employees and prominently post an annual anti-harassment policy statement signed by the agency head stating harassment will not be tolerated, the type of conduct that is prohibited, how to report harassment and the consequences of engaging in harassment and retaliation. The statement should be posted in an electronic and accessible form readily available to all employees (including those with disabilities).
- Ensure that anti-harassment policies clearly set forth who is responsible for taking corrective action when allegations are substantiated and an individual is found to have engaged in conduct that violates the anti-harassment policy.
- Acknowledge and reward employees, supervisors and managers for creating and maintaining a culture in which harassment is not tolerated.
- Acknowledge and reward supervisors and managers for taking actions to prevent harassment.
- Consider the extent to which agency personnel should be ineligible for promotions, performance awards or serving in a supervisory capacity when they violate an anti-harassment policy.
- Incorporate performance measures on harassment prevention and response into the performance evaluations of any staff with supervisory or managerial responsibility.

Comprehensive and Effective Anti-Harassment Policy

The EEOC recommends that employers adopt and regularly disseminate to all employees an anti-harassment policy that includes the following:

- Clear, easy to understand explanation of prohibited conduct that includes the definition of prohibited harassment.
- Prohibition against harassment on all federal EEO protected bases, including race, color, sex (including sexual orientation, gender identity and pregnancy), national origin, religion, disability, age (40 years or older), genetic information (including family medical history) and retaliation.
- Description of the employers' anti-harassment program that includes multiple channels to report harassment, including to personnel outside the supervisory chain of command.
- Protection for employees who engage in protected activity, such as making complaints of harassment or providing information related to such complaints.
- Surety that the employer will take corrective action to prevent or address harassing conduct before it becomes unlawful.
- Assurance that employer representatives will keep the identity of individuals who report harassment, alleged victims, witnesses, and alleged harassers (as well as information related to harassment investigations) confidential to the extent possible, consistent with legal obligations and the need to conduct a thorough and impartial investigation.
- Prompt, thorough and impartial investigation of harassment allegations.
- Immediate and appropriate corrective action when harassment is found to have occurred.
- Explicit assurance that the policy applies to employees at every level, as well as to applicants.
- Periodic reviews and updates as needed to incorporate legal developments, trends in harassment and changes in procedures.

Effective and Accessible Anti-Harassment Program

- Allow for anonymous reporting of harassment through platforms, such as hotlines and websites. In providing multiple avenues and methods to report harassment beyond the supervisory chain-of-command, the program should also consider using portals, ombudspersons, human resources officials and anti-harassment program personnel.
- Dispel the assumption that nothing can be done about anonymous harassment that occurs on the employer's virtual network. Employers may be able to track down the identity of individuals who engage in harassment anonymously (for example, anonymously posting sexually or racially offensive comments or images during a virtual work meeting) on the employer's network.
- Ensure that reports of harassment or harassing conduct are well-documented through a complaint tracking system. This tracking system may be designed, for example, to record when the employer was notified of harassment allegations, the identity of the alleged harasser, details about the alleged harassment, the EEO bases involved, the dates of the alleged harassment or harassing conduct,

when the investigation of allegations began and concluded, the identity of the investigator, whether harassment or harassing conduct was found to have occurred, any preventative or corrective action taken, and the identity of the person responsible for taking corrective action.
- Conduct investigative interviews with the alleged victim, the alleged harasser and third parties who could reasonably be expected to have relevant information.
- Ensure investigations are not conducted by individuals who have a conflict of interest or bias in the matter.
- Convey the outcome of the investigation (i.e. whether the allegations were substantiated and/or the policy found to have been violated) to the alleged victim and the alleged harasser, as well as the preventative and corrective action taken, where appropriate and consistent with relevant legal requirements.[43]

Effective Anti-Harassment Training

- Is provided periodically to non-supervisory employees as well as supervisors and managers at all levels of the agency.
- Is accessible to all employees, including through the provision of reasonable accommodations to individuals with disabilities.
- Includes a clear, plain language definition of unlawful harassment and prohibited unwelcome conduct.
- Encourages employees to report unwelcome conduct before it rises to the level of unlawful harassment or becomes severe or pervasive.
- Includes details on how to report alleged harassment in accordance with the employer's policies and procedures.

In addition, the EEOC advises that the effectiveness of anti-harassment training will be enhanced if it is:

- Championed by senior management.
- Regularly revised and updated as needed.
- Tailored to the specific workforce and workplace and includes examples relevant to the specific workplace setting.
- Conducted (virtually or in-person) in smaller groups that foster more employee engagement and participation. Followed by solicitation of feedback and input from participants to improve its effectiveness.

CLICK HERE.

FTC Warns Companies about Generative AI

On May 1, the Federal Trade Commission (FTC) released a blog post cautioning companies about the use of generative AI tools to change consumer behavior. Generative AI is a subset of AI that can generate new text, images, and other media based on patterns learned from existing data. The machine-generated content often feels authentic and realistic and is convincingly similar to that of a real human.

This FTC guidance is significant because the agency makes clear that manipulative use of generative AI can be illegal even if not all customers are harmed and even if those harmed do not comprise a class of people protected by anti-discrimination laws. Furthermore, the blog post indicates that the agency is carefully scrutinizing AI products under all prongs of the agency's authority under the FTC Act.

FTC has previously focused on AI-related deception, such as companies making unsubstantiated claims for AI products or the use of generative AI for fraud. In this recent post, though, the agency also highlights the unfairness prong of the FTC's authority, noting that a practice is unfair if it causes more harm than good. The FTC is aware of generative AI steering people to make harmful decisions in areas such as finance, health, education, housing, and employment and the agency is focusing intensely on the substantial consumer impact of these technologies across these broad sectors.

Human-like Interactions and The Risk of Unearned Consumer Trust
In evaluating the risks of generative AI, the FTC uses the example of chatbots designed to provide information, advice, support, and companionship, noting that companies use such tools to influence consumers' beliefs, emotions, and behavior. Many of these chatbots are built to persuade and are designed to answer questions in confident language, even when answers might be fictional.

In addition, machines are becoming increasingly human-like by using personal pronouns and emojis in their output responses. This type of system design results in people potentially placing undue trust in these machines. Automation bias refers to people's tendency to over-rely on automated systems and machines because their answers are designed to seem neutral or impartial. Generative AI tools can build consumer trust and lead consumers to believe that the tool understands them as a real human would.

Generative AI Design and Consumer Manipulation
The FTC alerts organizations to be cognizant of design elements that could trick consumers, warning that these have been a common element in recent FTC actions where system design elements manipulate consumers into making harmful choices. Manipulation can be unfair or deceptive under the FTC Act when it causes people to take actions contrary to their intended goals.

The agency specifically focuses on new uses of generative AI, such as customizing ads to specific audiences and placing ads within a generative AI feature. The FTC notes that it has consistently provided guidance on online ads and avoiding deception or unfairness, including work related to dark patterns and native advertising.

Key Takeaways for Businesses
For companies using generative AI tools, the FTC provides clear guidance in this blog post:

1. It should always be clear that an ad is an ad.
2. People should know whether they're communicating with a real person or a machine.
3. Companies should be aware of downstream uses of generative AI tools and should train employees accordingly.
4. Any generative AI output should distinguish clearly between what is organic and what is paid.
5. Consumers should know if an AI product's response is steering them to a particular website or product because of a commercial relationship.
6. Companies should monitor and address the actual use and impact of any generative AI tools they use.

CLICK HERE.

EEOC Releases New Guidance for AI Algorithms in Employment Decisions

On May 18, 2023, the EEOC released guidance on the use of Artificial Intelligence ("AI") tools in employment decisions. Though primarily focused on the selection and hiring of candidates, the same general guidance on AI tools would apply to their use in all employment decisions or personnel actions. The bulletin is short and worth reading. The EEOC's guidance on the topic should hopefully not be surprising to employers, as it follows established disparate impact analysis. More specifically, when using AI tools, employers should be cautious of using selection procedures that have a disproportionately negative effect on employees or applicants who have characteristics protected by Title VII.

The EEOC guidance also highlights some key reminders for employers that use algorithmic decision-making tools for selection and hiring:

- Employers should conduct ongoing analysis of any of their AI tools to determine whether their employment practices have a disparate impact.
- Employers may still be liable even if a problematic test was developed or implemented by a third party on their behalf (such as a recruiting agency).
- Employers should make direct inquiries to any third party as to the potential disparate impacts of any AI tools used.
- If in deciding on which tools to use, failure to adopt a less discriminatory algorithm considered during the development process may give rise to liability.

The takeaway from this guidance is that employers should not turn a blind eye to the use of AI tools by their own

employees or any third party or agent acting on their behalf. Direct inquiry, analysis and confirmation that any AI tool usage for employment decisions does not result in disparate impact is critical and should be periodically reviewed. CLICK HERE.

EEOC Title VII: What It Means for AI & Pay Equity Compliance

Employers that use AI and automated systems such as pay equity software to streamline workplace processes have received a stark reminder about potential employment discrimination violations.

On May 18th, the EEOC released a technical assistance document outlining the application of Title VII of the Civil Rights Act of 1964 to automated systems incorporating artificial intelligence (AI) in HR-related uses. The document aims to prevent discrimination caused by AI to job candidates and employees, including areas affecting pay equality.

Without effective safeguards, employers are at risk of violating Title VII during hiring, when managing performance and in determining fair pay. The rationale behind the document was explained by EEOC Chair, Charlotte A. Burrows: "As employers increasingly turn to AI and other automated systems, they must ensure that the use of these technologies aligns with the civil rights laws and our national values of fairness, justice and equality."

What does EEOC Title VII mean for employers?
EEOC Title VII prohibits discrimination in the workplace based on race, color, religion, sex (including pregnancy, sexual orientation, and gender identity) or national origin. The technical assistance guidance contains implications for employers regarding potential "disparate impact" or "adverse impact" cases, and discrimination which could violate employment law.

"Disparate impact" refers to discrimination that occurs "when a policy or practice has a significant negative impact on members of a Title VII-protected group but is not job-related and consistent with business necessity," according to EEOC guidance. It applies to all employment decisions, including those on compensation, and affects employers using algorithmic decision-making tools, such as pay equity software, to identify and remedy pay disparities across the organization.

"Disparate impact" analysis is the focus of the technical assistance document.

How does AI develop bias?
AI bias arises when the data used by algorithms is chosen by humans, who also decide how the results of the algorithms are applied, perpetuating biased models. For instance, in 2018, Amazon scrapped a recruiting tool that demonstrated bias against women. Its computer models were trained to vet applicants by observing patterns in resumes over a 10 year period. Effectively, the system taught itself to prioritize male candidates.

EEOC Title VII guidance is part of a wider trend surrounding AI
As AI becomes more prevalent in all areas of life and work, Title VII is part of the EEOC's Artificial Intelligence and Algorithmic Fairness Initiative, and a wider federal trend, which extends to pay discrimination.

On April 25th, the Consumer Financial Protection Bureau (CFPB), Department of Justice (DOJ) Civil Rights Division, the Equal Employment Opportunity Commission (EEOC) and the Federal Trade Commission (FTC) issued a joint statement confirm their intention to work collaboratively to "monitor the development of automated systems." That includes AI as well as other software and algorithmic processes. The intention is to prevent any form of bias which results in discrimination against protected classes.

Further, the White House released a "Blueprint for an AI Bill of Rights" that aims to protect civil rights in the building, deployment, and governance of automated systems. It also intends to examine the use of automated tools and AI that monitor and manage workers.

It is also worth noting that restrictions on automated employment decision tools will come into force in New York City on July 6th, 2023, less than a year after the introduction of pay transparency laws in NYC.

Employers may be liable for discrimination
The EEOC made it clear that employers cannot delegate responsibility for discrimination to a third party software provider, nor on their vendor's assurance that its software complies with EEOC Title VII. If your pay equity software violates workplace laws you, as an employer, may be held liable.

EEOC guidance states that "in many cases", an employer is responsible under Title VII for its use of algorithmic decision-making tools even if the tools are designed or administered by a software vendor, "if the employer has given them authority to act on the employer's behalf."

Partnering with a pay equity software vendor
Selecting the right pay equity software vendor is more critical than ever for employers. When choosing a partner, the EEOC recommends that organizations:

- Ask vendors what steps have been taken to evaluate whether their software might cause an adverse disparate impact
- Determine whether the vendor relied on the four-fifths rule
- Carry out an evaluation of employment-related AI tools to ensure compliance with workplace laws. This includes carrying out an auditing process on all AI functions.
- Conduct an ongoing self-analysis to determine whether your use of technology could result in discrimination

That applies to pay equity software. If the vendor's assessment of its software is inaccurate, and results in disparate impact discrimination relating to pay transparency, for example, employers could still be liable.

The EEOC makes it clear that someone with an Equal Pay Act claim may also have a claim under Title VII.

Partner with a trusted pay equity software provider
Companies that rely on AI and automated systems should prepare for increased scrutiny, and not just in the US.

On May 11th, 2023, the EU adopted a draft negotiating mandate on the "first ever rules for Artificial Intelligence." If passed, it will become the world's first Artificial Intelligence Act to impose transparency requirements on AI-decision making. The aim is to promote transparency and reduce risk, and it will also include the right to complain about AI systems. Like the Pay Transparency Directive, it seems highly probable that the EU will lead the way in creating a blueprint for legislation related to transparency in the use of AI.

Partnering with a trusted pay equity software provider to eliminate bias is essential for all employers. Trusaic works with organizations to minimize risk, increase compliance, and achieve authentic change:

Identify and remedy potential bias: Trusaic's PayParity identifies and corrects the root causes of pay disparities by utilizing advanced analytics and algorithms that pinpoint biases, faulty systemic processes, and other factors, providing you with pay ranges to create a robust compensation strategy, remain competitive and avoid the creation of future disparities. It also carries out an equity audit across your workforce in a single statistical regression analysis delivering a clear picture of pay gaps and risk areas across groups of employees, at every level. Pay equity software can also help your organization to comply with pay transparency legislation affecting job listings.

Stay up to date with pay transparency legislation: Working with a trusted pay equity software provider ensures employers not only comply with EEOC Title VII and the EU's Pay Transparency Directive, but with regular updates to pay transparency and pay equity laws. Most recently, these include expanded SB 1162 pay data reporting requirements in California.
CLICK HERE.

FTC Issues Policy Statement on Biometric Information, Signaling a New Enforcement Priority

At the Federal Trade Commission's (FTC or Commission) May 2023 Open Commission Meeting, the FTC voted unanimously to approve a Policy Statement on Biometric Information and Section 5 of the FTC Act (the Policy Statement). The Policy Statement reveals a growing skepticism towards biometric technologies from the Commission

"with respect to consumer privacy, data security, and the potential for bias and discrimination." It builds on previous enforcement actions involving biometric information, but also describes new and relatively prescriptive steps that the agency expects companies to take when collecting and using biometric data.

Overall, the Statement should be considered to be an indication of what the Commission will look for in investigations of biometric data-related practices and a roadmap for companies in evaluating their biometric data practice. Further, the Statement is a preview of considerations that will likely inform the FTC's ongoing privacy rulemaking.

The Policy Statement Builds on Previous Enforcement Actions

The Policy Statement explains that the FTC has been monitoring and evaluating biometric technology for "over a decade," beginning with the "Face Facts: A Forum on Facial Recognition Technology" workshop in 2011.[1] The Policy Statement notes that since 2012, facial recognition technologies "have made significant advances," and that the Commission has brought enforcement actions alleging that companies misrepresented their use of facial recognition technology.

In Everalbum, for example, the FTC alleged that the company violated Section 5 of the FTC Act by misrepresenting (1) users' ability to control the Everalbum app's face recognition feature, and (2) the deletion of users' photos upon account deletion. According to the FTC's complaint in that action, the FTC alleged that Everalbum automatically activated its facial recognition feature, and that the feature could not be turned off. The Commission also argued that Everalbum failed to honor commitments to consumers that the company would delete photos and videos of users who deactivated their accounts.

The Policy Statement Uses an Expansive Definition of Biometrics

The Policy Statement adopts a broad definition of the term "biometric information." Specifically, the Policy Statement defines "biometric information" as including "depictions, images, descriptions, or recordings of an individual's facial features, iris or retina, finger or handprints, voice, genetics, or characteristic movements or gestures." The definition also encompasses "depictions, images, descriptions, or recordings" that make it reasonably possible "to identify the person from whose information the data had been derived."[2] The Policy Statement provides an example of this, noting that both a photograph of a person's face and "a facial recognition template, embedding, faceprint, or other data that encode measurements or characteristics of the face" constitute biometric information. This definition therefore applies to not just data points such as particular facial characteristics or retina scans, but also photos and voice recordings.

The Policy Statement Identifies Several Perceived Harms Associated with Biometric Information Collection and Use

The Policy Statement enumerates a number of potential societal harms resulting from the use of biometric information technology, including the production of counterfeit videos or voice recordings ("deepfakes") that facilitate fraud or defamation, heightened risks of data breaches due to the existence of large repositories of biometric information, and the disclosure of sensitive information about a consumer's health care, attendance at religious services, or attendance at political events or union meetings.

Separately, the Policy Statement discusses that certain biometric technologies such as facial recognition technology can perform differently across demographic groups. According to the Policy Statement, for example, this can lead to higher false positives for women than men, and for elderly people and children, as compared to middle-aged adults. The FTC states that both false positives and false negatives are particularly harmful when biometric technologies are used to determine when consumers can "receive important benefits and opportunities" or are subject to penalties or other less desirable outcomes. For example, the Policy Statement notes that a false positive "may result in individuals being falsely accused of crimes, subjected to searches or questioning, or denied access to physical premises."

The Policy Statement Itemizes Potentially Deceptive or Unfair Practices Related to the Use of Biometric Information Technologies

Deceptive Practices. The Policy Statement notes that as with other types of technology, "false or unsubstantiated marketing claims" that relate to the accuracy, bias, and reliability of biometric information technologies can constitute deceptive practices under Section 5 of the FTC Act. Specifically, the Commission cautions that companies making these claims must "have a reasonable basis" for their claims that is based on their validity and accuracy across various populations through testing using real-world conditions. Additionally, the Policy Statement warns companies against making blanket claims that biometric information technologies will deliver particular results or outcomes.

Deceptive Statements About Collection and Use of Biometric Information. The Policy Statement also notes that false or misleading statements "about the collection and use of biometric information" and "failing to disclose any material information needed to make a representation non-misleading" constitute violations of Section 5 of the FTC Act.

Unfairness Factors. The Policy Statement also enumerates factors that the Commission will consider when investigating whether a company's use of biometric information technologies is an unfair practice under Section 5 of the FTC Act. The Statement's discussion of these factors signals that the FTC expects companies dealing with biometric information to adopt particular kinds of practices going forward. The Policy Statement's factors are:

- Whether the company has conducted a holistic assessment of the relevant benefits and harms of deploying biometric information technology before doing so. According to the Policy Statement, the results of testing "should be evaluated in light of how well the testing environment mirrors real world implementation and use," including the context for deployment.
- Whether the company promptly addressed known or foreseeable risks, such as adopting policies and procedures to limit organizational access to biometric information, or timely software and hardware updates to relevant information systems.
- Whether the company engages in "surreptitious and unexpected" collection and/or use of biometric information. The Policy Statement indicates that the FTC will consider whether there was a clear and conspicuous disclosure about the collection and use of the biometric information of consumers, and that consumer injuries are compounded if companies do not have a mechanism for accepting and addressing complaints.
- Whether the company conducts third-party oversight of affiliates, vendors, and end users who will be given access to consumer biometric information.
- Whether the company provides appropriate training for employees and contractors handling biometric information and/or biometric information technologies.
- Whether the company conducts ongoing monitoring of biometric information technologies "to ensure that the technologies are functioning as anticipated, that users of the technology are operating it as intended, and that use of the technology is not likely to harm consumers."

The FTC Is Likely to Remain Focused on Biometric Information Technologies from Both an Enforcement and a Rulemaking Perspective

The Policy Statement clearly signals an increased enforcement environment in the area of biometrics, which also may inform the Commission's ongoing "Commercial Surveillance and Data Security" rulemaking following the Advance Notice of Proposed Rulemaking (ANPR) released this past fall (we summarized the Commission's ANPR here). In the Commercial Surveillance and Data Security ANPR, the FTC asked several questions about the collection and use of biometric information by companies.[3] In the ANPR, the Commission also asked the public whether the agency should limit the use of "facial recognition, fingerprinting, or other biometric technologies. . ."[4]

Accordingly, companies that collect, use, or process "biometric information" should carefully review the Policy Statement and consider whether additional steps need to be taken to address the FTC's latest guidance.

[1] FTC, *Face Facts: A Forum on Facial Recognition Technology* (Dec. 8, 2011), https://www.ftc.gov/newsevents/events/2011/12/face-facts-forum-facial-recognition-technology.
[2] Note that the Everalbum Consent Order defined "biometric information" to similarly cover "data that depicts or describes the physical or biological traits of an identified or identifiable person, including depictions (including images), descriptions, recordings, or copies of an individual's facial or other physical features (e.g., iris/retina scans), finger or handprints, voice, genetics, or characteristic movements or gestures." *In re Everalbum, Inc., also d/b/a Ever and Paravision, a corporation*, Decision, Docket No. C-4743, at 2 (May 6, 2021) ("Everalbum Consent Order").
[3] *Trade Regulation Rule on Commercial Surveillance and Data Security*, Advance Notice of Proposed Rulemaking, 87 Fed. Reg. 51273, 51283, ¶¶ 37-38 (Aug. 22, 2022).
CLICK HERE.

Ready or Not: Form I-9 Flexibilities are Winding Down

On May 4, 2023, the U.S. Department of Homeland Security (DHS) and U.S. Immigration and Customs Enforcement (ICE) announced the official sunset date for COVID-19 related Form I-9 physical inspection flexibilities: July 31, 2023. Additionally, ICE advised that employers would have 30 days, or until **August 30, 2023**, to complete an in-person verification of all employees that were virtually verified since March 2020. Yesterday's announcement put an end to the speculation of whether the remote policy would run past July, and whether employers would only have three days after the termination of the flexibilities in which to update I-9s. No and No.

What were the temporary COVID-19 flexibilities?
In March 2020, ICE issued a press release stating that, in light of the COVID-19 national emergency, employers could temporarily defer physical inspection of employee identity and work authorization documents related to Form I-9 completion. Instead, employers could virtually verify employees' documents via video or via fax/email (collectively, "remotely"). Initially, the ICE guidance mandated that the business was *completely* shut down to benefit from this flexibility and that all employees verified remotely would need to physically present their documents in-person for inspection "once normal operations resume." A year later, on March 31, 2021, ICE relaxed the requirement relating to the operational status of the employer, and instead, focused on the employee, allowing for remote inspections to continue where employees were working from home *due to* COVID-19. In our April 1, 2021 blog, we discussed the expansion of the "in-person" exemption, which then offered flexibility for companies that were phasing back in employees, as doing so no longer triggered the in-person inspection requirement for all new hires. ICE updated their instructions to replace the phrase "once normal operations resume" with "until [the employee] undertakes non-remote employment on a regular, consistent, or predictable basis, or the extension of the flexibilities related to such requirements is terminated, whichever is earlier." At this point, if mistakes were made in terms of applicability of the policy, companies can only move forward and ensure they are remediating as quickly and accurately as possible.

While ICE needed to be more precise with employers, their guidance never applied to permanent remote employees. Actual remote employees, who were allowed to work from anywhere without expecting to return to an in-person setting, were never offered the COVID virtual flexibilities. Understandably, many employers misapplied the applicability standards and incorrectly allowed for remote inspection. In this case, an authorized representative should be used if an employee cannot appear at the worksite to update the I-9 with a physical inspection – see more below.

Thoughts on Timing?
With the end of the national emergency, the COVID-19 flexibilities will expire after three years of extensions on July 31, 2023. Employers will have an additional 30 days from that date, or until August 30, 2023, to complete a physical examination of documentation and update all Forms I-9 for employees that have yet to complete an in-person inspection. Until now, ICE had not opined how much time employers would have to complete in-person verification once an employee returned to the office. While many feared the three-day rule would be applied, our bets were always on ICE landing between 90-120 days. Since ICE started the clock in early May, they actually provided slightly under 120 days for employers to comply. Alternatives should be immediately considered for companies whose workforces remain remote due to COVID; the summer always comes and goes quickly.

So what is the Authorized Representative method?
With the burden of updating hundreds, or thousands of remote Forms I-9, many employers implemented an Authorized or Third-Party Representative model – what we refer to as a "friends and family" process. In earlier blogs Hidden ICE Guidance On Virtual I-9s, and The 2020 Summer Defrost Continues: ICE Extends I-9 Flexibility, we noted employers have always been allowed to utilize a third party as an authorized representative to complete Section 2 (or Section 3) of the Form I-9 on an employer's behalf. However, things heated up during the pandemic, and employers were forced to think outside the box. We saw employers becoming more comfortable with designating a friend, relative, colleague, neighbor, barista, mail carrier, etc., with reviewing identity and employment eligibility documents. Working with these employers, we created SOPs and directives outlining compulsory post-verification completion audits and document ***copy*** mandates to ensure accuracy and compliance. Since the representative's actions are imputed on the company, adding guardrails is critical.

Walk me through this.

1. Identify all Forms I-9 requiring updates. How you do this depends upon how your company stores I-9s (paper or electronically), how careful you were in terms of coding COVID I-9, and how you organize your system. Hopefully, you've been tracking your completed COVID I-9s from the start.
2. Create a project plan. The plan should ensure that the entire population is notified and provided background on what is required, the requisite timing for compliance, and the repercussions for not cooperating. The project plan should also outline how updates will be tracked.
3. Decide if your physical inspection will occur at the worksite (forcing folks still working from home to come in), or if you will use an Authorized Representative model (or hybrid offering). Regardless, examine the workflow offerings and limitations associated with paper completion or with your vendor.
4. Train your employees conducting physical inspections and create guidance for any authorized representatives assisting in the process. Ensure they are aware of the nuanced rules surrounding documents not found on the List of Acceptable Documents and automatic extensions of EADs.
5. Provide samples and guidance to your HR teams, or authorized representatives, describing how to physically update the Forms – see below for more information.
6. Allow employees to present their choice of identity and work authorization document(s) when updating Forms I-9. They do not need to present the same document(s).
7. Ensure that you did not miss updating any expired List B documents. See, *The End is Near: COVID-19 List B Document Temporary Policy Ends*.
8. Ensure that E-Verify queries were run and correctly closed, where applicable.
9. Tidy things up, and ensure that you have the required "written documentation" outlining your "remote onboarding and telework policy for each employee" required by ICE in the original March 20, 2020 announcement.
10. Plan on scheduling an assessment of your company's current state of immigration compliance oversight, management and related risks in September, after the long summer of 2023 and COVID I-9 updates are over.

How do I update my Forms I-9?

This is the tricky part. How you update your Forms I-9 will depend on whether you use paper I-9s or an electronic I-9 system. Each electronic I-9 vendor, hopefully, offers a specific workflow to update COVID I-9s. Companies using electronic I-9s should work with their vendor to:

- Understand how to identify remote COVID I-9s in the system;
- Confirm a workflow exists to update these remote COVID I-9s with a physical inspection; and,
- Ensure the system tracks the completion of updates to remote COVID I-9s.

As for how to update a Form I-9, government guidance is limited. Despite requests for further clarification, ICE and US Citizenship and Immigration Services ("USCIS") have only provided partial (and somewhat contradictory) guidance for updating Forms I-9 once the physical inspection occurs (see USCIS examples here; ICE removed their narrative from the website).

The guidance is clearly tailored for paper I-9 completion and does not contemplate the substantial number of employers using electronic I-9 systems. Accordingly, judgment calls will need to be made, and companies should work closely with experienced compliance counsel to ensure there are no missteps.

Same Documents

If the employee presents the same documents that were presented virtually, employers should note in the Additional Information field "Documents Physically Examined" with the date of inspection. Do not forget to initial and date the comment.

Different Documents

Employees have their choice of documents to present for physical inspection updates. In the event an employee presents documentation that is different than the documentation presented for their remote verification, employers have two options:

1. Complete a new Section 2 (many electronic I-9 systems force a new I-9 due to system limitations) and note "Documents Physically Examined" with the date of inspection in the *Additional Information* Employers should then attach the new Section 2 to the original I-9; **OR,**
2. Record the new document information in the *Additional Information* box of the original Section 2 and note "Documents Physically Examined" with the date of inspection. Remember to initial and date your comment.

Different I-9 Completer
If the person who performed the remote inspection is not the person performing the physical inspection, USCIS guidance states that the new I-9 completer should indicate the date they physically examined the documents as well as their full name and title in the *Additional Information* field.

ICE representatives have stated that the preferred option would be to complete a new Section 2, thereby having the I-9 properly certified with the requisite attestation. Considering ICE will be doing I-9 inspections, this seems like a reasonable way to go but either choice will suffice. Remember to attach the new Section 2 to the original I-9.
For more information on COVID-19 policies, check out I-9 Central's Questions and Answers Related to COVID-19 for additional FAQs.

What about Permanent Virtual and the New I-9?
The waiting game continues. There was so much excitement as the government finally issued their notice of proposed rulemaking ("NPRM"), *Optional Alternatives to the Physical Document Examination Associated With Employment Eligibility Verification (Form I-9)*, in August of 2022. DHS is still considering these alternative procedures but we expect some sort of regulatory update by the end of the year. Whether or not the release of new Form I-9 will be tied to this is still uncertain.
CLICK HERE.

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

Chicago's Amended "Ban the Box" Ordinance Imposes Stricter Criminal History Use and Notification Requirements on Employers

Chicago has amended its "Ban the Box" Ordinance (the "Ordinance") to further align with Illinois law. The Ordinance, which originally took effect in 2015, provides protections for both prospective and current employees. Historically, the Ordinance restricted when Chicago employers with fewer than 15 employees and certain public employers could inquire about or consider an individual's criminal record or criminal history. The new amendments, which took immediate effect, expand application of the Ordinance to almost all Chicago employers and impose significant new assessment and notice requirements thereon. The amendments also expressly incorporate into the Ordinance provisions from the Illinois Human Rights Act (IHRA) that prohibit employers from inquiring about or considering an individual's arrest record. The amendments did not modify the Ordinance's penalties, however, so employers are still liable for fines of up to $1,000 per violation, license-related disciplinary actions, and potential discrimination charges before the Chicago Commission on Human Relations.

New Employer Coverage
When initially enacted, the Ordinance was only applicable to employers not subject to the Illinois Job Opportunities for Qualified Applicants Act (i.e., employers with fewer than 15 employees and certain public employers). The Ordinance now applies to all employers that have at least one employee and are required to: (1) have a Chicago license to conduct business and/or (2) maintain a facility within Chicago.

New Individualized Assessment Requirements
Similar to the IHRA, the Ordinance now distinguishes employers' obligations depending on whether the employer intends to consider arrest records or conviction records (both of which are now defined terms).

The updated Ordinance, like the IHRA, prohibits employers from inquiring or using arrest records as a basis for refusing to recruit, hire, promote, renew, train, discharge, or discipline an individual, or for establishing other conditions of employment. Arrest records are broadly defined as: (1) an arrest not leading to conviction; (2) a juvenile record; or (3) criminal history record information that has been expunged, sealed, or impounded. Certain exceptions apply, including when employers use sealed felony convictions during legally required criminal background checks as a basis for evaluating the qualifications or character of a prospective employee.

Also similar to the IHRA, the Ordinance now requires employers to conduct individualized assessments to determine if/when they may rely on conviction records to make an employment decision. Specifically, the Ordinance prohibits employers from taking adverse action against an applicant or current employee based on that individual's conviction record unless one of the following applies:

- Applicable law requires the exclusion of the applicant or employee from the position based on the conviction record;
- A fidelity or similar bond is required for the position and the individual's conviction of more than one criminal offense would disqualify them from obtaining the bond;
- There is a substantial relationship between one of more of the individual's criminal offenses and the employment sought or held; or
- Granting or continuing employment would involve unreasonable risk to the property, safety, or welfare of others or the general public.

In determining whether a "substantial relationship" exists, employers must consider: (1) the length of time since the conviction(s); (2) the number of convictions; (3) the nature and severity of the conviction(s) and its relationship to the safety and security of others; (4) the age of the individual at the time of the conviction(s); (5) the unique circumstances surrounding the conviction(s); and (6) evidence of rehabilitation efforts.

New Notice Requirements
The Ordinance also now implements stricter notification requirements for employers, similar to those outlined in the IHRA. If an employer makes a preliminary decision that the prospective or current employee's conviction record

disqualifies them from employment, the employer must provide the individual with a written notice that contains the following information:

- A description of the disqualifying conviction(s), along with the employer's reasoning for the disqualification;
- A copy of the conviction record; and
- An explanation of the individual's right to respond to the notice at least five (5) days prior to the decision becoming final, and that any such response may include, but is not limited to, evidence challenging the accuracy of the conviction record or mitigating evidence, such as evidence of rehabilitation.

If, after considering any response from the employee or prospective employee, the employer determines that the individual remains disqualified or that adverse action is otherwise justified, the employer must also give written notice to the employee or prospective employee of this final decision. The final written notice must describe the disqualifying conviction(s), identify any internal recourse the individual may have to appeal the final decision with the employer, and state that the individual has the right to file a complaint with the Chicago Commission on Human Relations.
CLICK HERE.

New Illinois Equal Pay Bill Would Require More Transparent Job Postings: 4 Things Employers Need to Know

The Illinois Equal Pay Act has been around for a decade, but it's seen many changes in the past few years. The act was amended in 2021 to impose new equal pay compliance requirements and create new obligations for private employers with more than 100 employees. Then, in 2022, the Illinois Department of Labor finally provided some guidance for employers on those new requirements. Most recently, on February 16, Illinois legislators introduced a new pay equity bill that would amend the act again and require organizations with at least 15 employees to include benefits and pay scale information in job postings. Although the bill is still working its way through the legislative process, you should be aware of your potential obligations should it pass and ultimately be signed into law. What are the top four points you should note for now?

1. New Job Posting Requirements
The new pay equity bill, HB3129, would amend the Illinois Equal Pay Act to require covered organizations to provide pay scale and benefits information in their job postings. What exactly does that mean? "Pay scale and benefits" include "the wage or salary, or the wage or salary range, and a general description of the benefits and other compensation the employer reasonably expects to offer for the position." Additionally, if passed, the bill would require you to announce, post, or otherwise make known all job opportunities to all current employees no later than the same day that you post the job. Notably, however, if you do not use job postings, the bill clarifies that it does not create any new requirement for you to do so.

2. Record-Keeping Requirements
The bill would also require employers to adhere to certain record-keeping requirements, including the obligation for you to preserve records of the pay scale and benefits information for each posted position for at least five years, or in the event of an ongoing investigation or action under the act, until their destruction is authorized by the Department of Labor or court order.

3. Potential Liability for Third-Party Job Postings
More concerning for Illinois employers, the bill will hold employers liable for a third party's failure to include the pay scale and benefits information in a job posting on behalf of the employer. Accordingly, Illinois employers would need to work closely with any third-party they use to assist with job postings and recruitment.

4. Violations Could Be Costly
If passed, the bill would grant the Illinois Department of Labor authority to initiate investigations into alleged violations of the newly amended subsections of the act. If the Illinois Department of Labor determines a violation has occurred, the employer would have seven days to remedy the violation upon receiving notice of a violation. If the employer does not demonstrate that the violation has been remedied, the employer would be subject to a civil penalty of $100 per day for each day that a violation continues following the seven-day notice period. Each job posting that fails to comply with

the act would be deemed a separate violation.

Conclusion
Given the growing state-law trend across the nation requiring employers to disclose detailed pay scale and benefits information in their job postings, we recommend Illinois employers gear up and begin revising their job postings in anticipation of the bill becoming law.
CLICK HERE.

Colorado and Connecticut Privacy Laws Take Effect in Two Months; Are You Ready For It?

The Colorado Privacy Act (CPA) and the Connecticut Data Privacy Act (CTDPA) take effect on July 1, 2023. The CPA regulations take effect at the same time. And if you are subject to California's laws, this is the enforcement date for California Consumer Privacy Act, as amended by California Privacy Rights Act.

Whether you are just now in the reach of US state privacy laws under the Colorado or Connecticut thresholds or you have an existing US privacy program for California or Virginia laws, you may need to take affirmative steps prior to July 1. The states do not converge on all topics, so existing programs may need updates. For example, the CPA regulations include topics not addressed in the current California privacy regulations such as data protection impact assessments and more discussion of loyalty programs. Consider also if your privacy statements need updates to speak to Colorado and Connecticut consumers about their data rights and your response processes are ready to respond to Colorado and Connecticut consumer requests. There is still time to make these updates before the summer vacation season begins.
CLICK HERE.

Method and Madness Behind New California and Washington Cannabis Laws

On September 18, 2022, California amended its primary employment discrimination law to specifically regulate the drug testing methodologies that employers may use when making hiring, termination, and other employment decisions relating to cannabis users. More recently, on May 9, 2023, Washington Governor Jay Inslee signed similar legislation relating to initial hiring decisions. Both laws, which will be effective January 1, 2024, are the first of their kind because they require employers to have a basic understanding of a somewhat complicated issue — the science behind cannabis testing.

Testing for THC
The primary psychoactive agent — the thing that gets people high — in cannabis is delta-9-tetrahydrocannabinol (THC). At present, most employers use urine drug tests, which target the cannabis metabolite THCA, which is nonpsychoactive. Thus, when an employer receives a urine test result, all the employer knows is that the person has used cannabis at some time in the recent past (from days to several weeks); exactly when, however, is unknown. THC is the primary target and is found in greater concentrations in drug tests that use saliva specimens, which in turn leads to test results that are tied to or related to psychoactive effect.

None of the scientifically valid drug tests, including those that use saliva specimen, inform an employer whether a person is impaired at or near the time they provide a specimen for testing.

California's AB 2188
On September 18, 2022, California Governor Gavin Newsom signed AB 2188, which amended the Fair Employment and Housing Act (FEHA) to essentially make cannabis users a protected class in California. Effective January 1, 2024, it will be unlawful for most employers to discriminate against a person in connection with hiring, termination, or another employment decision if the discrimination is based upon *either*:

(1) The person's use of cannabis off the job and away from the workplace. This paragraph does not prohibit an employer from discriminating in hiring, or any term or condition of employment, or otherwise penalize a person based on scientifically valid preemployment drug screening conducted through methods that do not screen for nonpsychoactive cannabis metabolites.
(2) An employer-required drug screening test that has found the person to have nonpsychoactive cannabis metabolites in their hair, blood, urine, or other bodily fluids.

There are several exceptions to the new employment discrimination prohibitions: (1) employees in the building and construction trades; (2) applicants or employees hired for positions that require a federal government background investigation or security clearance in accordance with Department of Defense regulations, or equivalent regulations applicable to other agencies; and (3) applicants and employees required to be tested under state or federal laws and regulations or as a condition of an employer receiving federal funding or federal-licensing benefits or entering into a federal contract.

What does this mean? Subparagraph (2) focuses solely on the type of test. More specifically, employers cannot take an adverse employment action against an applicant or an employee based on a drug test that targets nonpsychoactive cannabis metabolites. As explained above, this effectively makes urine tests useless (and unlawful) to California employers. As a result, covered employers who wish to test for cannabis should consider discontinuing urine testing on or before January 1, 2024, regardless of whether the test is for a job applicant or a current employee.

What about saliva/oral fluids testing? The answer seems to depend on whether the test is for a job applicant or a current employee. Subparagraph (1) states that an employer can reject a job applicant if the cannabis test does not screen for nonpsychoactive metabolites, suggesting that an employer can rely on a pre-employment saliva/oral fluids test that targets the parent drug THC. The same may hold true for hair testing.

However, even if an employer uses a saliva/oral fluids test for a current employee that complies with subparagraph (2), it still must consider the first sentence of subparagraph (1), which prohibits employers from taking action against someone because of their "use of cannabis off the job and away from the workplace." Oral fluids tests might provide a close-in-time correlation as to when employees use cannabis, but they do not prove that employees actually are impaired or used cannabis on the job or at work. As a result, even if an employer uses a lawful testing methodology for a current employee, an employer that takes action against an employee for cannabis use still has significant risk under FEHA because it likely will be difficult to rebut the employee's assertion that they used "off the job and away from the workplace."

Washington's SB 5123

SB 5123, which takes effect January 1, 2024, states that a Washington employer cannot discriminate against a person in the *initial hiring* for employment if the discrimination is based on: their use of cannabis off the job and away from the workplace *or* an employer-required drug test that has found the person to have nonpsychoactive cannabis metabolites in their hair, blood, urine, or other bodily fluids. However, the law does not "[p]rohibit an employer from basing initial hiring decisions on scientifically valid drug screening conducted through methods that do not screen for nonpsychoactive cannabis metabolites." Accordingly, Washington employers can reject job applicants for cannabis use if the employer uses the appropriate drug testing methodology.

From a testing methodology perspective, Washington's SB 5123 is the same as California's AB 2188. It differs, however, insofar as the Washington law only regulates pre-employment cannabis testing, leaving in place the right of an employer to maintain a drug-free workplace and policy and to test current employees for cannabis using any scientifically-valid methodology. This is consistent with the Washington legislature's intent — "to prevent restricting job opportunities based on an applicant's past use of cannabis."

SB 5123 contains a broad list of exceptions, including for positions: (1) requiring a federal government background investigation or security clearance; (2) law enforcement, fire department, or other first responder positions; (3) corrections officers; or (4) in the airline or aerospace industries. The law also does not apply if the applicant will work in a "safety sensitive position for which impairment while working presents a substantial risk of death." If an employer takes advantage of this exception, it must provide notice to the applicant prior to their application for employment that the position sought is "safety sensitive." Moreover, the law does not preempt state or federal laws requiring applicants to be tested for controlled substances.

A practical provision was added to the bill as it made its way through the legislative process: an employer can continue to test applicants for cannabis, presumably irrespective of the methodology utilized by the employer, as long as the cannabis results are not provided to the employer.

Next Steps for Employers

Employers have little more than six months to prepare for these new laws, both of which are effective on January 1, 2024. The California Civil Rights Division is expected to issue regulations, but whether those regulations will be finalized before the end of 2023 is unclear. In the meantime, California and Washington employers would be well-advised to consult with their drug testing laboratories to ensure their drug testing methodologies will comply with these new laws. This is especially true in California where cannabis users (applicants and employees) are essentially a protected class, which makes them eligible for the full range of FEHA damages available (*e.g.*, compensatory damages, attorneys' fees, and costs) if an employer is determined to have violated the law.

CLICK HERE.

Kentucky's New Medical Marijuana Law: What Employers Need to Know (and Do)

Kentucky Governor Andy Beshear recently signed Senate Bill 47 into law, legalizing* medical marijuana in Kentucky. Starting in 2025, Kentuckians will be able to apply for a medical marijuana card after obtaining a written certification from their medical practitioner showing a qualified medical condition. Those conditions are as follows:

- Any type or form of cancer regardless of stage;
- Chronic, severe, intractable, or debilitating pain;
- Epilepsy or any other intractable seizure disorder;
- Multiple sclerosis, muscle spasms, or spasticity;
- Chronic nausea or cyclical vomiting syndrome that has proven resistant to other conventional medical treatments;
- Post-traumatic stress disorder; and
- Any other medical condition or disease for which the Kentucky Center for Cannabis established in KRS 164.983, or its successor, determines that sufficient scientific data and evidence exists to demonstrate that an individual diagnosed with that condition or disease is likely to receive medical, therapeutic, or palliative benefits from the use of medicinal cannabis.

*Note: Medical marijuana remains illegal under federal law, and therefore a Kentucky employer subject to the federal Drug-Free Workplace Act must continue to prohibit employee medical marijuana use accordingly to avoid consequences thereunder.

How This New Law Will Impact Employers in Kentucky

While the new law may legalize medical marijuana, employers will have substantial legal safeguards allowing them to restrict the use of medical marijuana in the workplace. Specifically, employers may:

1. Prohibit an employee who is a registered qualified medical marijuana cardholder from using equipment, machinery, or power tools if the employer believes such use poses an unreasonable safety risk.
    - The law also restricts cardholders from consuming medical cannabis or being under the influence when performing certain tasks (e.g., operating, navigating or being in control of a common carrier aircraft, vehicle, vessel or other machine-powered device).
2. Continue to operate as a drug-free workplace and prohibit medical marijuana usage through reasonable detection and enforcement.
    - Employers will be permitted to perform marijuana drug testing and act in accordance with test results. Indeed, employers can test employees in "good faith" to determine whether the cardholder has worked while impaired. This determination requires a behavioral assessment for impairment and a test to find the presence of marijuana through established methods. If an employer determines that a cardholder employee is impaired by cannabis use based on a behavioral impairment assessment and a cannabis test as a secondary step, the burden of proving non-impairment will shift to the employee to refute.
3. Rely upon the new statute as a shield against lawsuits and unemployment benefit costs.
    - Notably, employees do not have the right to make a claim against their employer for wrongful discharge or discrimination when the adverse action is premised upon cannabis misuse.
    - An employee who is discharged from employment for consuming medical marijuana,

working while under the influence of the same, or testing positive for a controlled substance will be ineligible for unemployment if such actions are in violation of an employment contract or established personnel policy.

Although the law does not go into effect until January 1, 2025, Kentucky employers should proactively review the law and their policies, including drug testing policies, to determine whether any revisions to existing policies or other employment documentation are necessary.
CLICK HERE.

New York Updates Sexual Harassment Prevention Model Policy and Training Materials

In 2018, New York became one of the first states to enact legislation requiring employers to provide all employees with annual sexual harassment prevention training and to maintain a sexual harassment prevention policy that meet or exceed certain minimum statutory standards. The New York State Department of Labor (NYSDOL), in consultation with the New York State Division on Human Rights (NYSDHR), recently made significant revisions to its model Sexual Harassment Prevention Policy and training materials, making it necessary for employers to take action.

Updated Model Policy
While the underlying statutory requirements have not changed, the NYSDOL recently finalized revisions to its model Sexual Harassment Prevention Policy, making substantial changes to its old model.

Key revisions in the recently published model policy include:

- adding language that explains that sexual harassment does not need to be severe or pervasive to be illegal;
- defining sexual harassment as a form of "gender-based" discrimination, and explaining gender diversity (including definitions of "cisgender," "transgender" and "nonbinary");
- explaining that the intent of behavior is not a defense and that conduct is evaluated objectively from a reasonable victim's standpoint;
- adding a section on bystander intervention;
- addressing harassment in the remote workplace;
- updating examples of conduct that may constitute sexual harassment, including those in the context of the remote workplace and relating to gender expression;
- outlining the responsibility of supervisors and managers to report harassment and discrimination and to be mindful of the impact of investigations;
- supplementing examples of retaliation (e.g., labeling an employee "difficult" or excluding an employee from projects);
- providing information about the NYSDHR's new sexual harassment hotline; and
- clarifying that the New York State Human Rights Law protects against discrimination based on all protected classes.

Updated Training Materials
In addition to updating its model harassment prevention policy, the NYSDOL enhanced its mandatory training toolkit to align with the revised model policy. The updated training materials include new case studies and examples of how sexual harassment is affected by remote work and other issues.

Other key revisions to the model training materials include:

- instructing trainers to provide a warning that the "subject matter can be sensitive or difficult for some employees, including those that might have experienced harassment, discrimination or violence in the past";
- recommending that trainers make clear to those attending that anyone needing to step out briefly on behalf of their mental health may do so;
- adding a section addressing gender identity that includes defining "cisgender," "transgender" and "nonbinary";
- setting forth additional case scenarios that focus on sex stereotyping, remote work and gender identity; and

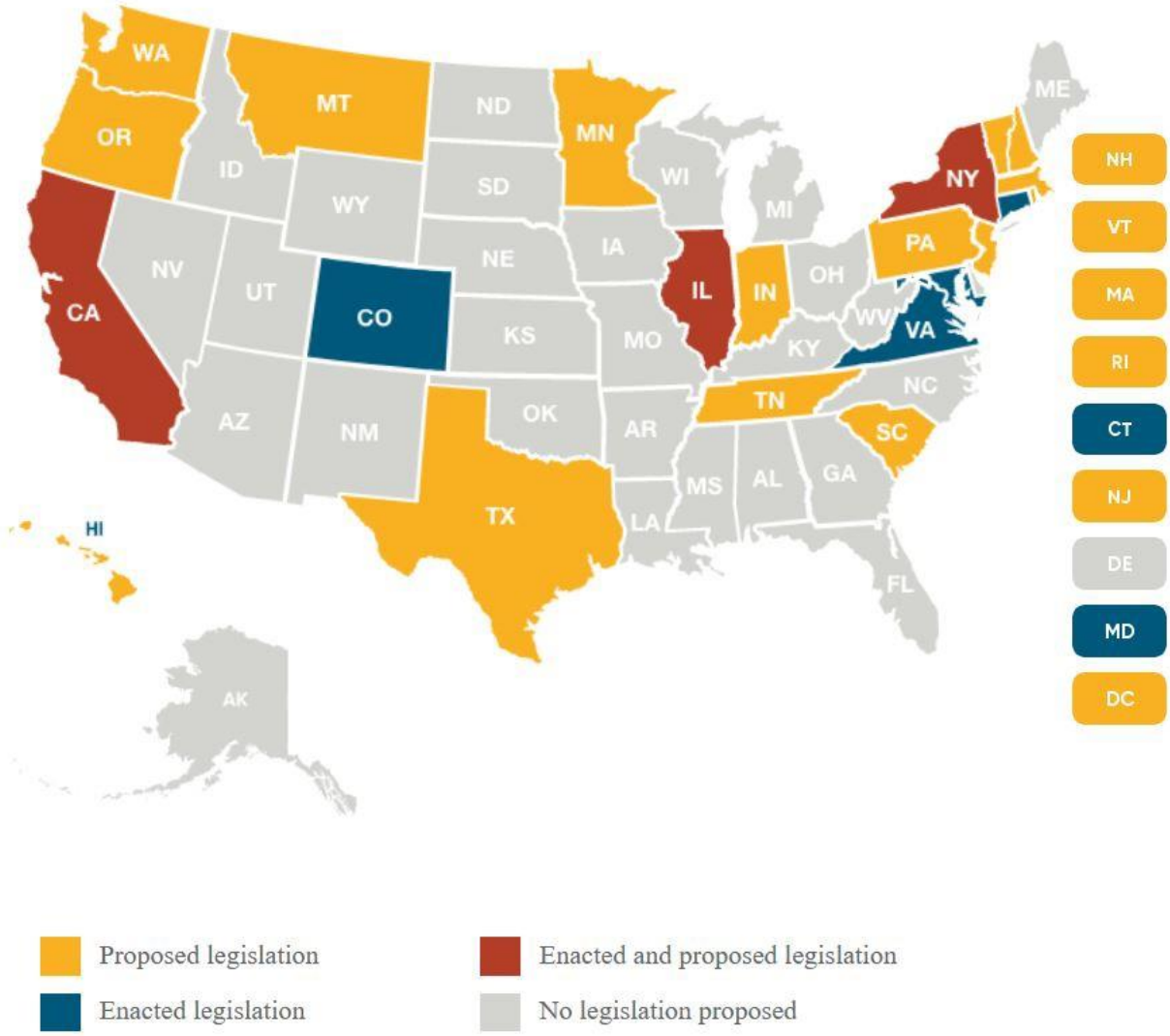
- providing examples of potential methods of bystander intervention.

As part of its revisions to the training materials, the NYSDOL also issued a new training video, which employers can use when conducting their annual trainings. Employers should note, however, that the video alone is not considered interactive and would not satisfy New York's requirement that the training be interactive.

What Should Employers Do Now?
The NYSDOL's revisions to its model policy and training materials are significant. As such, employers should review their handbooks and consider whether they should update their anti-harassment policies. In addition, employers should review their harassment prevention training materials, make sure they comply with New York's requirements and, most importantly, ensure that employees are timely trained on an annual basis. Employers with any questions about how the NYSDOL's revisions affect their policies and training materials should speak with legal counsel for guidance.
CLICK HERE.

2023 State-by-State Artificial Intelligence Legislation Snapshot

Artificial Intelligence (AI), once limited to the pages of science fiction novels, has now been adopted by more than 1/4 of businesses in the United States, and nearly half of all organizations are working to embed AI into current applications and processes. As companies increasingly integrate artificial intelligence in their products, services, processes, and decision-making, they need to do so in ways that comply with the different state laws that have been passed and proposed to regulate the use of AI.



For more information, please click on:
CLICK HERE.

New York AG Releases Guide for Businesses on Effective Data Security

As noted in a prior post, New York's Attorney General ("NYAG") has made enforcement of the New York SHIELD Act an enforcement priority. The SHIELD Act requires organizations handling personal information related to New York residents to maintain reasonable safeguards to protect that information. Maintaining its focus on this area, the NYAG recently released a guide to help organizations strengthen their data security programs and "to put [them] on notice that they must take their data security obligations seriously, and at a minimum, take the reasonable steps outlined" in the NYAG's guide (the "Guide").

The Guide is based on the NYAG's experiences in investigating and prosecuting organizations in the wake of data incidents. It states that the NYAG received 4,000 data breach notifications in 2022 and penalized organizations millions of dollars for failing to comply with their data security obligations.

In the Guide, the NYAG recommends action in nine areas. Specifically, it directs organizations to:

1. Maintain controls for secure authentication to ensure only authorized individuals have access to data.
2. Encrypt sensitive customer information
3. Ensure service providers use reasonable security measures
4. Know where the business is keeping consumer information
5. Guard against data leakage in web applications
6. Protect customer accounts impacted by data security incidents
7. Delete or disable unnecessary accounts
8. Guard against automated attacks
9. Provide clear and accurate notice to consumers

The Guide recommends best practices related to each of the above recommendations and also highlights relevant cases the NYAG has investigated that implicate these areas. Additionally, it incorporates by reference guidance the NYAG issued in 2022 regarding credential stuffing attacks, which outlines four areas in which safeguards should be maintained and certain safeguards may not be effective.

In light of the NYAG's aggressive enforcement of the NY SHIELD Act, and the sharp rise in data breach-related litigation, organizations should take a close look at their data security programs – with the Guide as one reference point – to ensure they are appropriately managing risk.
CLICK HERE.

Florida Poised to Require Employers to Use E-Verify with New Hires: Your 5 Key Takeaways

As part of a potentially growing trend, a new law in Florida will require private employers with at least 25 employees to use E-Verify – the digital immigration verification tool – during their onboarding process starting July 1. Governor Ron DeSantis is anticipated to soon sign SB 1718 into law, which will also increase penalties for noncompliance and for employers who knowingly hire undocumented workers. Notably, if employers use the E-Verify system in good faith – whether use is mandatory or voluntary – the government will presume they have not knowingly hired unauthorized workers. What do you need to know about the new law and how will it impact your new hire process?
[Editor's Note: Governor DeSantis signed SB 1718 into law on May 10.]

Refresher on E-Verify and Employment Verification
All employers are required to complete the I-9 form within three days of a new hire's start date to verify identity and ensure employment authorization in the U.S. for every employee. E-Verify is an online tool that is operated by the U.S. Department of Homeland Security and allows employers that have completed Form I-9 to then electronically verify employment eligibility for their new hires. Employers that use E-Verify may not do so selectively. Rather, they must use the system to verify all newly hires regardless of whether they are U.S. citizens.

Currently, use of the E-Verify system is mandatory in Florida for public employers and for private employers contracting

with state and local governments or receiving state incentive dollars. The new law expands that requirement to private employers with at least 25 employees.

Employers that want to enroll in E-Verify can do so by visiting the official website.

5 Key Takeaways for Employers on the New Law

Employers that will be newly covered by the E-Verify requirement should review their obligations as soon as possible. Here are five key takeaways regarding the new law:

1. **Compliance dates for covered businesses.** Private employers with 25 or more employees must utilize the E-Verify system in addition to completing Form I-9. The law applies to new employees hired on or after July 1, 2023.
    - E-Verify utilizes information available to the Social Security Administration and Department of Homeland Security to confirm records and identity. If the records do not match, the system will notify of a "Tentative Nonconfirmation" (mismatch) result. You must give the notice to the employee who then has 10 days from the issuance of the mismatch to notify you whether they will resolve the mismatch. If the employee cannot resolve the mismatch, they are no longer eligible to continue employment.
    - "Employee" is defined as an individual filling a permanent position under the control of employer. Independent contractors and casual laborers are not considered employees.
2. **Record retention requirements.** For at least three years, the employer must retain a copy of the documentation, as well as any official verification generated, if applicable.
3. **Compliance presumed.** Employers that use the E-Verify system establish a rebuttable presumption that they have not knowingly employed an unauthorized worker. If the E-Verify system is down for three days and you cannot timely complete the process for a new hire, you can still benefit from the rebuttable presumption by completing Form I-9 and taking a screenshot each day documenting that the system is unavailable or retaining any official notice or communication you received about the system being down.
4. **Annual certification required.** Each employer that is required to use the E-Verify system must certify compliance on its first return when making contributions to or reimbursing the state's unemployment compensation or reemployment assistance system. An employer that voluntarily uses the E-Verify system may also make such a certification on its first return each calendar year in order to document such use.
5. **Penalties for noncompliance.** Penalties will go into effect on July 1, 2024. Businesses have 30 days to cure noncompliance after receiving notice from the Department of Economic Opportunity (DEO), and the new law requires DEO to notify a business prior to issuing penalties for violation.
    - If the DEO determines that an employer failed to use the E-Verify system as required three times in any 24-month period, the department must impose a fine of $1,000 per day until the employer provides sufficient proof that the noncompliance is cured.
    - An employer's first violation results in a one-year probationary period with reporting requirements to put a business on a path to compliance prior to any licenses being revoked.

Benefits for Small Businesses

Businesses with fewer than 25 employees can continue to use the Form I-9 to verify employment eligibility or choose to take the extra step of using E-Verify, which comes with heightened immunity protections. Employers that voluntarily use the E-Verify system may also submit annual certifications for documentation purposes.

Conclusion

Employers that operate in multiple jurisdictions will need to track this potential trend. If you have any questions about I-9 or E-Verify compliance and how these requirements may affect your business, please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Florida offices or Immigration Practice Group. We will continue to monitor developments and provide additional guidance as warranted. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information.
CLICK HERE.

New York City Council Passes Bill Barring Discrimination Based on Height or Weight

Characteristics would become protected classes under the city's Human Rights Law
The New York City council passed a bill on May 11, 2023, prohibiting discrimination on the basis of an applicant's or employee's actual or perceived height or weight. The bill would amend the New York City Human Rights Law to add "height" and "weight" to its list of protected classes and becomes effective 180 days after it is signed into law, which New York City Mayor Eric Adams is expected to do.

Exemptions and Affirmative Defenses
Exemptions – The bill provides for the following exemptions to the general prohibition on discrimination on the basis of height and weight:

- Such action is required by federal, state, or local law or regulation;
- Such action is permitted by regulation adopted by the New York City Commission on Human Rights ("NYCCHR") identifying particular jobs or categories of jobs for which:
    - A person's height or weight could prevent performing the essential functions of the job; and
    - The NYCCHR has not found alternative action that covered entities could reasonably take to allow persons who do not meet the height or weight criteria to perform the essential functions of the job or category of jobs; or
- Such action is permitted by regulation adopted by the NYCCHR identifying particular jobs or categories of jobs for which consideration of height or weight criteria is reasonably necessary for the execution of the normal operations of the employer.

Affirmative Defenses – The bill provides the following affirmative defenses related to height and weight discrimination:

- A person's height or weight prevents the person from performing the essential functions of the job, and there is no alternative action the employer could reasonably take that would allow the person to perform the essential functions of the job; or
- The employer's decision based on height or weight criteria is reasonably necessary for the execution of the normal operations of such employer.

Next Steps - While there are no immediate steps to take in response to the bill, employers should:

- Review current employment policies and practices to ensure workers are evaluated on their skills and performance rather than their physical appearance;
- Consider incorporating examples of discrimination on the basis of height or weight into training programs and materials; and
- Be cognizant of necessary adjustments that may be needed in physical spaces, like larger armchairs or step stools.

Notably, the bill permits employers to offer incentives that support weight management as part of a voluntary wellness program.
CLICK HERE.

Washington Amends Law to Protect Off-Duty Marijuana Use in 2024

On Tuesday, May 9, 2023, Governor Inslee signed into law Senate Bill No. 5123, which will protect prospective employees from discrimination in hiring due to their lawful, off-duty use of marijuana. With this law, Washington will join the growing list of states offering some workplace protections to workers who engage in "off-duty" marijuana use. The new law is not a "go-ahead" for all Washington employees to engage in recreational marijuana use without employment consequences, however. Governor Inslee has emphasized the law does not protect all such use and does not prevent employers from establishing policies regarding a drug-free workplace. The new law goes into effect on January 1, 2024.

The new law prohibits employers from "discriminating" against a person in hiring based on the person's lawful use of cannabis off the job and away from the workplace. Specifically, employers will be unable to rely upon pre-employment drug tests that screen for the presence of "non-psychoactive" cannabis metabolites to make hiring decisions. Washington

has long been a state where marijuana use, in various forms, is lawful – the state has permitted medicinal use since 1998 and recreational use since 2012.[1]

The law's stated purpose is to bring marijuana as a substance on the same footing as alcohol for consideration in pre-employment testing, stating:
Applicants are much less likely to test positive or be disqualified for the presence of alcohol on a preemployment screening test compared with cannabis, despite both being legally allowed controlled substances. The legislature intends to prevent restricting job opportunities based on an applicant's past use of cannabis.

What the New Law Requires and Notable Exceptions
The new law makes it unlawful for an employer to "discriminate against a person in the initial hiring for employment" if the discrimination is based upon either (i) "the use of cannabis off the job and away from the workplace" or (ii) based on a drug screening test "that has found the person to have nonpsychoactive cannabis metabolites in their hair, blood, urine, or other bodily fluids."

Consistent with the prohibition on relying upon non-psychoactive test results, employers that continue to conduct pre-employment testing for marijuana must use tests that are "scientifically valid drug screening conducted through methods that do not screen for nonpsychoactive cannabis metabolites."

There are certain notable exceptions to this blanket rule limiting an employer's ability to act based on an individual's off-duty marijuana use. Specifically, testing for marijuana will continue to be allowed in the following situations:

- When testing for purposes other than pre-employment testing;
- When employers use "scientifically valid" testing in pre-employment screenings that do not screen for non-psychoactive cannabis metabolites;
- When state or federal law requires the applicant to be tested or dictates the way tests are administered, as a condition of employment, receiving federal funding or federal-licensing-related benefits, or as required by a federal contract; or
- When an applicant seeks a position: (i) requiring a federal government background investigation and security clearance; (ii) involving work with public safety agencies such as law enforcement agencies, fire departments, and first responders (including dispatchers); (iii) as a corrections officer; (iv) within the airline or aerospace industries; and/or (v) another "safety sensitive" position. "Safety sensitive" positions are defined as those "for which impairment while working presents a substantial risk of death." Employers will be required to identify which positions they consider safety-sensitive prior to the applicant's application for employment.

Conclusion
Washington employers should prepare for the January 1 implementation date by reconsidering which applicants they will test for cannabis. Then, either ensure the positions fit within one of the enumerated exceptions, including whether such positions fall within the narrow "safety sensitive" definition, or test using methods that seek only the presence of psychoactive THC in the individual's test sample. Finally, where necessary, Washington employers should update their drug and alcohol testing policies and hiring materials to ensure compliance with the new law.

Footnotes
[1] State court decisions interpreting the Washington Medical Use of Marijuana Act do not recognize a broad public policy that would impose accommodation obligation on employers.
CLICK HERE.

As Minnesota Nears Broad Marijuana Legalization, Employers Should Anticipate Testing, Policy Changes

With just days remaining in the legislative session, Minnesota lawmakers remain on track to legalize recreational marijuana, significantly modify the state's drug-testing law, and limit employers' rights to prohibit employee off-duty marijuana use and impose discipline for marijuana-related conduct, among other changes to the laws surrounding marijuana use in the state.

On May 16, a conference committee adopted final provisions of a bill that resolve differences between the versions passed by the House and Senate earlier this month—including Article 6, which addresses employer-mandated testing of applicants and employees for cannabis. The committee bill is expected to return to each chamber for a final vote before the legislative session ends on May 22. Governor Tim Walz has indicated he will sign the bill if given the opportunity. If enacted, the employment-related provisions of the bill would go into effect on August 1, 2023.

Although the bill is not yet law, the conference committee's adoption of the employment-related provisions and the general momentum toward legalization in Minnesota should prompt employers to reevaluate their drug-testing needs and anticipate rule changes. If enacted, the new law would require employers to treat cannabis differently than other drugs and even alcohol—with limited testing opportunities, higher thresholds for discipline, and more nuanced policy requirements.

Drug, alcohol and "cannabis testing"

Minnesota's Drug and Alcohol Testing in the Workplace Act (DATWA) currently allows employers to test for "drugs," which the statute defines by referring to the state's schedules of controlled substances. When Minnesota lawmakers legalized low-dose hemp-derived THC edibles in 2022, a question arose regarding whether such products, or cannabis more generally, were controlled substances. The recreational marijuana bill specifies that cannabis[1] would no longer be a "drug" under DATWA but would allow testing through a new category of "cannabis testing." If enacted, this change would require employers to decide whether to test individuals for cannabis, reevaluate the circumstances in which they require cannabis testing, and amend their written policies to address new cannabis testing requirements.

Position classes determine which testing rules apply

The proposed bill addresses cannabis testing by first creating two classes of positions—one class that would remain subject to existing DATWA testing requirements and another class that would be subject to the new cannabis testing rules. The distinction arises from draft language that says, for certain positions, cannabis and its metabolites would continue to be considered a "drug" despite the state's broader legalization.

The first class of positions—which would continue to be subject to existing DATWA requirements and would be exempt from the new cannabis testing rules—includes (1) safety-sensitive positions; (2) peace officers; (3) firefighters; (4) positions requiring face-to-face care, training, education, supervision, counseling, consultation or medical assistance to children, vulnerable adults, or healthcare patients; (5) positions requiring a commercial driver's license or subject to federal or state motor vehicle regulations requiring testing; (6) employment positions funded by a federal grant; and (7) positions for which state or federal law requires cannabis testing.

"Safety-sensitive position" would continue to mean a job, including any supervisory or management position, in which impairment caused by drug, alcohol or cannabis usage would threaten the health or safety of any person.

The second class of positions would consist of all positions not included in the first (*i.e.*, positions that are not safety-sensitive and do not fall within another exception). For this class, employers would be *prohibited* from requiring cannabis testing for the sole purpose of determining the presence or absence of cannabis. That means employers could no longer require pre-employment testing or random testing for cannabis. Employers could conduct reasonable suspicion cannabis testing as defined in the statute. Specifically, the employer could continue to require cannabis testing if it reasonably suspects that the employee: (1) is under the influence of drugs or alcohol; (2) violated the employer's written rules prohibiting the use, possession, sale or transfer of drugs, alcohol, or cannabis during work; (3) has sustained a personal injury or caused another employee to sustain a personal injury; or (4) has caused a work-related accident or was operating or helping to operate machinery, equipment, or vehicles involved in a work-related accident.

Notably, these changes apply only to testing for cannabis. Testing for other substances, including illegal drugs and alcohol, would remain subject to current DATWA requirements.

Limited discipline for policy violations related to cannabis

The position-class distinction described above would apply only to testing and would not limit employers' ability to discipline workers for other policy violations related to cannabis.

The committee bill permits employers to prohibit employees from using or being impaired by cannabis during work and clarifies the circumstances under which discipline may be imposed. Specifically, the bill states that employers may

discipline, discharge, or take other adverse personnel action against an employee for cannabis use, impairment, sale or transfer while the employee is working, while the employee is on the employer's premises, or while the employee is operating the employer's vehicle, machinery, or equipment if the employer has enacted work rules regarding cannabis and cannabis testing in a DATWA-compliant policy.

Employers may also impose discipline if, as the result of consuming cannabis, the employee "does not possess the clearness of intellect and control of self that the employee otherwise would have" or the employee has a confirmed positive result on a cannabis test. Employers are also allowed to take action if authorized under state or federal law or regulations, or if failing to do so would cause the employer to lose a federal monetary or licensing-related benefit.

DATWA's existing "second chance" rule for employees who test positive for the first time would continue to apply to instances where an employee tests positive for cannabis for the first time, regardless of which job classification the employee held.

Clarification on "lawful consumable products" law

The recreational marijuana bill also provides clarity regarding Minnesota's "lawful consumable products" law, which generally prohibits employers from refusing to hire or disciplining an individual because the individual uses lawful consumable products outside of work. This law traditionally has protected the off-work use of foods, alcohol, and tobacco. Whether existing cannabis products, such as medical cannabis and low-dose hemp-derived THC products, qualify as lawful consumable products has been a gray area in the law.

With the proposed bill, existing law would be amended to explicitly state that cannabis products are lawful consumable products regardless of their status under federal and other state laws. That change would reinforce the policy that employers generally could not take adverse action based on an individual's decision to consume cannabis outside of work premises and working hours, similar to the current status of alcohol under the law.

There are important exceptions to this law, however, even with the proposed changes. Mirroring the changes to DATWA, employers would retain the ability to prohibit use, possession, and impairment from cannabis products during work hours, on work premises, or while operating the company's vehicle, machinery, or equipment. Employers could also take action if failing to do so would violate federal or state law or regulations or cause the loss of federal money or licensing-related benefits. Existing exceptions for bona fide occupational requirements and to avoid conflicts of interest would also remain intact.

Conclusion

If Minnesota lawmakers and the governor approve the recreational marijuana bill, employers should be prepared to reconsider if and when they will test employees for cannabis and how they will respond to cannabis use and impairment in the workplace. Employers that want to continue testing for cannabis will need to evaluate which positions are safety-sensitive or subject to other exceptions and determine when testing can occur. Even employers that will no longer test for cannabis should consider adopting and communicating written rules that expressly prohibit use, possession, impairment, sale, and transfer of cannabis on at work and during work hours.
CLICK HERE.

Montana Consumer Data Privacy Act Signed Into Law

Montana Governor Greg Gianforte signed the Montana Consumer Data Privacy Act (MTCDPA) on May 19, 2023, after unanimous passage through the state legislature, and the Act will go into effect October 1, 2024. Montana is now the ninth state to enact a comprehensive state privacy law, joining California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, and Tennessee, but is the first state to ban TikTok. The ban has been challenged in federal court as "a prior restraint on expression that violates the First Amendment," and it so dominated Montana news that the MTCDPA was relegated to "also-signed" status lumped in with 200 other bills.

The MTCDPA looks a lot like the Connecticut Data Privacy Act (CTDPA) in several key respects. In particular, MTCDPA resembles Connecticut in:

- Providing consumers the right to revoke their consent to data processing;[1]
- Requiring businesses to recognize universal mechanisms for opting out of sales of personal data and

targeted advertising[2] without having to verify their identities;[3] and
- Permitting a consumer to request deletion of all personal data about the consumer in the possession of a business, as opposed to just personal data a business collected directly from the consumer.

Also like the Connecticut law, the MTCDPA prohibits businesses from selling personal data or processing the personal data of a consumer for the purposes of targeted advertising without consent when a controller has actual knowledge that the consumer is at least 13 years of age but younger than 16 years of age (if data on a child under 13, compliance reverts to COPPA). Only California and Connecticut have similar provisions concerning privacy protections for a sub-set of minors. We highlight other key provisions of the MTCDPA below.

Application Thresholds
The MTCDPA applies to companies that conduct business in Montana or target products or services to Montana residents that:

- The MTCDPA has the lowest applicability threshold of any of the nine comprehensive data privacy laws enacted. Most other state privacy laws apply to a business that controls or processes the personal data of 100,000 residents and the lower threshold likely accounts for Montana's smaller population.
- Control or process the personal data of not less than **50,000** state residents, excluding personal data controlled or processed solely for purposes of completing a payment transaction; ***or***
- Control or process the personal data of not less than **25,000** state residents and derive more than 25 percent of gross revenue from the sale of personal data.

Exemptions
Consistent with most other state data privacy laws, MTCDPA contains entity-level, data-specific, and employment-related exemptions.

Entity-level exemptions:

- government entities,
- nonprofit organizations,
- higher education institutions,
- registered securities associations,
- financial institutions covered by the Gramm-Leach-Bliley Act (GLBA), and
- "covered entities" under the Health Insurance Portability and Accountability Act (HIPAA),

Data-specific exemptions:

- protected health information under HIPAA,
- certain other health- and patient-related information under federal regulations and state laws, and
- information governed by and/or processed in accordance with other privacy laws, including the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, the Driver's Privacy Protection Act, and several others.

Employment-related exemption:

- personal information relating to applicants for employment and employees whose "communications or transactions occur within the context of that individual's role" with the employer, including emergency contact information and benefits.

Processing-related exemptions:

- The MTCDPA does not restrict a controller or processor from collecting, using, or retaining personal data to:
    - Comply with federal, state, or municipal ordinances or regulations;
    - Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons, by federal, state, municipal, or other governmental authorities;
    - Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably, and in good faith, believes may violate federal, state, or municipal ordinances or regulations;

        - Investigate, establish, exercise, prepare for, or defend legal claims;
        - Provide a product or service specifically requested by a consumer;
        - Fulfil the terms of a written warranty;
        - Conduct internal research to develop, improve, or repair products, services, or technology;
        - Effectuate a product recall;
        - Identify and repair technical errors that impair existing or intended product functionality; or
        - Perform internal operations that are reasonable based on consumer expectations or the consumer relationship.
    - A controller processing data under these exemptions "bears the burden of demonstrating that the processing qualifies for the exemption," and the processing must be "reasonably necessary and proportionate to the purposes listed."

Privacy Notices
The MTCDPA requires controllers to provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

- The categories of personal information processed by the controller;
- The purpose for processing personal information;
- The categories of personal data that the controller shares with third parties, if any;
- The categories of third parties, if any, with which the controller shares personal data;
- An active email address or other mechanism that the consumer may use to contact the controller; and
- How consumers may exercise their rights, including how a consumer may appeal a controller's decision with regard to the consumer's request.

In addition, the MTCDPA states that a controller shall "establish and describe" in a privacy notice one or more secure and reliable means for consumers to submit a request to exercise their consumer rights, including the right to opt out of the sale of personal information to third parties and the right to request deletion or correction of certain personal information.
A controller may not require a consumer to create a new account to exercise consumer rights but may require a consumer to use an existing account.

Sensitive Data Defined
Like the Virginia, Connecticut, and Colorado laws, the MTCDPA prohibits businesses from collecting and processing "sensitive data" without obtaining the consumer's consent (or the parent's if under 13). The MTCDPA defines "sensitive data" as:

- Personal data revealing:
    - Racial or ethnic origin;
    - Religious beliefs;
    - Mental or physical health diagnosis;
    - Sexual orientation; or
    - Citizenship and immigration status;
- Genetic and biometric data that identifies an individual;
- Precise geolocation data (location within a radius of 1,750 feet); and
- Personal data collected from a known child (i.e., someone under the age of 13).

If the sensitive data pertains to a known child, compliance with the COPPA (verifiable parental consent) is required.

"Sale of Personal Data" Defined
The MTCDPA defines "sale of personal data" as the exchange of personal data for "monetary or other valuable consideration by the controller to a third party." The law excludes the following usual disclosures:

- To a processor that processes the personal data on behalf of the controller;
- To a third party for the purposes of providing a product or service requested by the consumer;
- To an affiliate of the controller;
- When the consumer directs the controller to disclose the personal data or intentionally uses the controller

to interact with a third party;
- Personal data that the consumer intentionally made available to the public via a channel of mass media and did not restrict to a specific audience; and
- Disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

As in other states that adopt this broader definition of "sale," consumers may opt out of disclosures to third parties for marketing, analytics, and other purposes for something of value other than monetary consideration.

Consumer Rights
As with other state privacy laws, the MTCDPA gives consumers the rights to confirm the processing of, and access to, their personal data; request that a controller correct inaccuracies in the consumer's personal data; delete personal data provided by the consumer or obtained by a controller regarding the consumer; and obtain a copy of the data in a portable and readily usable format.

As provided in other state privacy laws, controllers must respond to such requests within 45 days (with a 45-day extension available, if "reasonably necessary") and must offer consumers the right to appeal an adverse decision. The appeal response must be delivered by a controller to a consumer within 60 days, and if controllers deny an appeal, as in Virginia, controllers must provide a consumer with a method for contacting the attorney general to submit a complaint.

Required Recognition of Universal Opt-Out Mechanisms
Following California, Colorado and Connecticut, the MTCDPA requires controllers to recognize universal opt-out mechanisms for sales of personal data and targeted advertising. The MTCDPA states that, no later than January 1, 2025, covered companies must process opt-out requests submitted by consumers via universal opt-out mechanisms that are "consumer-friendly and easy to use" and "must allow the controller to accurately determine whether the consumer is a resident of the state and whether the consumer has made a legitimate request to opt out of any sale of a consumer's personal data or targeted advertising."

Data Protection Impact Assessments
Like the laws in Virginia, Connecticut, and Colorado, the MTCDPA requires controllers to conduct data protection assessments for each of the controller's processing activities that presents a heightened risk of harm prior to engaging in various processing activities, including:
- Processing personal data for targeted advertising;
- Sale of personal data;
- Processing sensitive data; and
- Processing of personal information for profiling if the profiling presents a reasonably foreseeable risk of unfair or deceptive or unlawful disparate impact on consumers, "intrusion upon seclusion," or other financial, reputational, or physical harms.

Impact assessments must weigh the benefits to the controllers against the risks to consumers' rights as mitigated by any safeguards, and assessments conducted in accordance with other state laws will comply with the MTCDPA, provided that those assessments are "reasonably similar in scope and effect" to an assessment required by the Montana law. The MTCDPA requires prospective data protection impact assessments for processing activities "created or generated" after January 1, 2025.

Processor Contracts
The MTCDPA uses a controller-processor framework and requires that controllers and processors memorialize their agreement through the usual contractual arrangements, including allowing and cooperating with reasonable assessments of the processor by the controller or its agent.

Consent Defined
"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer. The term may include a written statement, a statement by electronic means, or any other unambiguous affirmative action. Like California and Colorado's privacy laws,

the MTCDPA prohibits the use of so-called "dark patterns" in obtaining consent from a consumer.

Enforcement
There is no private right of action afforded to consumers for violations under the MTCDPA or "any other law." The MTCDPA is only enforceable by the state attorney general's office.

Temporary Cure Period and Sunset Provision
The Montana attorney general must give businesses notice and the opportunity to cure an alleged violation within 60 days of receiving the notice. If a controller cures the alleged violation within the allotted 60-day cure period and provides an express written statement to the attorney general confirming the alleged violations were corrected, then the attorney general may not initiate an action against the controller.

However, the right to cure sunsets on April 1, 2026. After that, the attorney general will not have to give notice or wait to bring an enforcement action, and can pursue enforcement even if the violation was corrected.
CLICK HERE.

COURT CASES

Meaningful consent and data protection of third-party apps: Federal Court dismisses Privacy Commissioner's complaint against Facebook

On April 13, 2023, the Federal Court handed down its decision in a case brought by the Office of the Privacy Commissioner of Canada (the "**OPC**") against Facebook Inc. ("**Facebook**").[1] The case centers around Facebook's obligations with respect to third-party applications' data protections. It also provides helpful insight on the interpretation of "consent" under Canadian private-sector privacy law, commenting specifically on what constitutes *meaningful* consent in the social media context where third-party applications collect information. The Court decided against the OPC, ruling in favour of Facebook, which could have a significant impact on the interpretation of "meaningful consent" in the digital age.

The Joint Investigation into Facebook
The proceedings before the Federal Court arose from a complaint received by the OPC in March of 2018 which raised concerns about Facebook disclosing information to a third-party application, "thisisyourdigitallife" ("**TYDL**"), without obtaining meaningful consent. TYDL was an application launched by a Cambridge professor on the Facebook platform that allowed users to fill in a "personality quiz" about themselves and their friends. TYDL was given access to Facebook profile information of everyone who installed the app as well as information about their Facebook friends.

The OPC and the Information and Privacy Commissioner for British Columbia ("**OIPC**") conducted a joint investigation to determine whether Facebook's actions constituted a breach of the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") and BC's private-sector privacy law, the *Personal Information Protection Act* ("**PIPA**").

On April 25, 2019, the OPC and the OIPC issued its Report of Findings which concluded that Facebook failed to obtain valid and meaningful consent from app users and their Facebook friends when sharing information with TYDL. It also found that Facebook did not adequately safeguard user information.[2] The information collected by the TYDL was then sold to third-parties, most notably to Cambridge Analytica, the consulting firm known for its involvement in targeted messaging during U.S. political campaigns.[3] Facebook estimated that the 272 installations of the TYDL led to a potential disclosure of personal information of more than 600,000 Canadians.[4]

The Federal Court proceeding
However, under current privacy legislation, the OPC does not have order-making power and is unable to issue penalties. Under sections 14 and 15 of PIPEDA, the OPC may, in certain circumstances, apply for a hearing before the Federal Court of Canada in respect of any matter referred to in the Commissioner's report of findings from an investigation.[5] Pursuant to these provisions, the OPC commenced an application at the Federal Court of Canada to have the court make the same determination and issue orders against Facebook. This is a *de novo* hearing meaning that while the Report of Findings can be entered as evidence, it is not owed deference.[6]

The Federal Court considered whether: (1) Facebook breached PIPEDA by failing to obtain meaningful consent; (2) Facebook failed to adequately safeguard user information; and (3) if Facebook breached PIPEDA, whether it is protected by estoppel or officially induced error on the basis that in the OPC's 2008-2009 Investigation of Facebook, the OPC approved Facebook's processes.

The OPC did not meet its burden with respect to obtaining meaningful consent
The Federal Court found that the OPC had not proved that Facebook failed to receive meaningful consent for the collection of personal information.[7] In particular, the Federal Court negatively commented on the fact that the OPC did not use the broad powers under section 12.1 of PIPEDA to compel evidence from Facebook. The OPC stated that they did not exercise these powers because Facebook would not have complied; however, the Federal Court found the burden to establish a breach of PIPEDA rests with the OPC and speculation and inferences would not meet this burden in the absence of material evidence.[8] The Federal Court notably stated that they were in an "evidentiary vacuum."[9]

Moreover, in discussing whether meaningful consent was obtained, Justice Manson asked "whether Facebook made reasonable efforts to ensure users and users' Facebook friends were advised of the purposes for which their information would be used by third-party applications."[10] He went on to state that the lack of evidence made it difficult to assess the reasonableness of meaningful consent in "an area where the standard for reasonableness and user expectations may be

especially context dependent and are ever-evolving."[11] This comment has impacts for meaningful consent under PIPEDA. In particular, it suggests that as technology evolves, the rights of individuals surrounding the protection of their data may change.

Facebook adequately safeguarded personal information

Additionally, Justice Manson did not agree with the OPC's argument that Facebook failed to protect user data.[12] Although Justice Manson agreed with the OPC that Facebook is required to protect their users' data, Justice Manson did not agree that Facebook was obligated to continue its protection once the users agreed to download and use the TYDL app.[13] The Federal Court decided in favour of Facebook that it was no longer required to protect the data of individuals when that data was in the hands of the app and not Facebook.

The 2008-2009 OPC approval

Facebook's Granular Data Permissions ("**GDP**") process required app developers to display an installation screen listing categories of information that the app would receive and provide a link to a privacy policy. Facebook argued that the OPC had approved their GDP process in the 2008-2009 investigation, citing the approval as a defence to any breaches of PIPEDA that allegedly occurred.

The Federal Court did not address this issue as Facebook was not found liable for breaches of PIPEDA; however, it will be interesting to see whether OPC approval of processes can be waged as a defence to breaches of PIPEDA in the future given changing conceptions of privacy protections and privacy reform.

What's Next? Bill C-27 and the Canadian Privacy Landscape

PIPEDA is currently undergoing significant reform. Bill C-27 will introduce three new pieces of legislation. Two of the three acts, the *Consumer Privacy Protection Act* ("**CPPA**") and the *Personal Information and Data Protection Tribunal Act* ("**PIDPT**"), were previously proposed in Bill C-11 and aim to establish a new enforcement regime, which will impose stricter privacy regulations on corporations and empower not only the Commissioner with new powers but also establish a new tribunal geared to resolving privacy complaints.[14] As well, Bill C-27 introduces the *Artificial Intelligence and Data Act* ("**AIDA**"), the federal government's first attempt to regulate AI.

Borrowing from the enforcement regime in the EU's *General Data Protection Regulation*, if passed, Bill C-27 will place Canada's privacy laws as some of the most punitive amongst the G7 countries[15] as the Bill introduces new enforcement powers for the OPC, empowers a specialized tribunal to handle privacy complaints and institutes a broad private right of action for privacy breaches.

Importantly, the CPPA will grant order-making powers to the Commissioner who can also make recommendations to the Data Protection Tribunal to impose fines of up to 5% of the revenue of the non-compliant company or up to $25 million, whichever is greater[16] and administrative monetary penalties of up to 3% of revenue or $10 million, whichever is greater.[17] If enacted, the OPC would not have to commence an application before the Federal Court to issue orders against Facebook.

The PIDPT will set up a new data protection tribunal, the first of its kind in Canada, to hear appeals of findings and orders made by the OPC, and determine whether the penalties recommended by the Commissioner are appropriate.[18] The tribunal will be held to a stricter standard of review compared to the current standard in federal court appeals under PIPEDA.[19]

In light of the Federal Court's finding in this case, it will be interesting to see what evidentiary standards the OPC and the Data Protection Tribunal implement in enforcing breaches of PIPEDA.

The CPPA also introduces added exceptions to knowledge and consent. In particular, Bill C-27 enables the collection and use of personal information without knowledge or explicit consent if the collection or use is made for the purpose of an activity in which the organization has a "legitimate interest." It will be intriguing to see how this exception will work in the context of third-party applications on social media platforms.[20]

If Bill C-27 had already been enacted, the consequences for Facebook would likely have been very different. If the legitimate interest exception was found not to apply, the strengthened enforcement regime would have allowed the OPC to issue orders

and recommend fines against Facebook, without assistance from the Federal Court. In light of privacy law reform, organizations need to ensure compliance with existing privacy laws and be aware of reform initiatives coming down the pipeline.

To view all formatting for this article (eg, tables, footnotes), please access the original here.
CLICK HERE.

Washington Federal Court Reiterates Distinction Between Furnishers' and CRAs' FCRA Investigatory Obligations and the Necessity of Alleging an Inaccuracy in a Consumer Report

A district court in the Western District of Washington held that the Fair Credit Reporting Act (FCRA) does not require a consumer reporting agency (CRA), as part of its investigative duties, to issue an opinion on the legal validity of a consumer's debt. Through its holding, the court denied the plaintiff's motion for reconsideration and motion to amend her complaint ruling that its previous decision, granting judgment on the pleadings for the CRA, did not conflict with the Ninth Circuit's decision in *Gross v. CitiMortgage, Inc.*

In *Riser v. Central Portfolio Control, Inc.*, the plaintiff disputed the legal validity of a debt she incurred while insured by Medicaid. The plaintiff relied primarily on *Gross*, which generally addressed furnishers' reporting duties and applied its reasoning to the reporting of a "past due" junior mortgage that was abolished by Arizona state law. The Ninth Circuit panel in *Gross* held that the reasonableness of the furnisher's investigation was a genuine factual dispute and that furnishers could be required to address and resolve an issue of legal significance, like the legality of debt abolished by state law, in a consumer credit dispute because furnishers have familiarity and closer relationships with consumers.

In *Riser*, the plaintiff argued that the *Gross* decision supported her theory that a CRA can be held liable for failing to conduct a reasonable investigation of a consumer's dispute even when the dispute involves documents of legal significance and resolving the issue would require the equivalent of a legal opinion or legal determination from the CRA. The district court found two flaws in the plaintiff's argument. First, the court distinguished the plaintiff's claims because *Gross* pertained to furnishers while the plaintiff's case involved a CRA. Second, the court found that nothing in *Gross* superseded the Ninth Circuit's decision in *Carvalho v. Equifax Information Services, LLC*, holding that CRAs are not required in their reinvestigation duties to provide legal opinions on the validity of debts.

In addressing the first flaw, the court explained that furnishers and CRAs have different investigatory obligations. Furnishers may be required to investigate, highlight, or resolve more extensive issues than CRAs because furnishers often are more directly involved with consumers. CRAs, on the other hand, often "are third parties that 'lack[ ] any direct relationship with the consumer,' so they must rely on the representations of the furnishers who usually own the debt."

The court also found that even if CRAs were not categorically exempt from conducting investigations into legal disputes, for the reasonableness of an investigation to be evaluated, the plaintiff must first make a *prima facie* showing of an inaccuracy in the consumer report. The court reiterated that this requires the consumer to show that her report is "patently incorrect or materially misleading" so that a CRA would not need to undertake an unduly burdensome inquiry into the consumer's legal defenses to identify the inaccuracy. Here, because the plaintiff's dispute involved an ambiguous legal and factual area and the plaintiff argued she was not legally obligated to pay the debt, she failed to make the required showing. Therefore, the court was not obligated to consider the reasonableness of the CRA's investigation.

The district court also denied the plaintiff's motion to amend the complaint to reconcile it with *Gross*, holding that even with the sought-after amendment, the plaintiff failed to make the necessary *prima facie* showing of an inaccuracy.
CLICK HERE.

ID Verification Provider to Pay $28.5 Million to Settle BIPA Allegations

On May 5, the U.S. District Court for the Northern District of Illinois preliminarily approved an amended class action settlement in which an identification verification service provider agreed to pay $28.5 million to settle allegations that it violated the Illinois Biometric Information Privacy Act (BIPA). According to the plaintiffs, the defendant collected, stored, and or used class members' biometric data without authorization when they uploaded photos and state IDs on a

mobile app belonging to one of the defendant's customers. After the court denied the defendant's move to compel arbitration and determined the plaintiff had standing to pursue his BIPA claims, the parties entered into settlement discussions without the defendant admitting any allegations or liability. The court certified two classes: (i) Illinois residents who uploaded photos to the defendant through the app or website of a financial institution (class members will receive $15.7 million); and (ii) Illinois residents who uploaded photos through a non-financial institution (class members will receive $12.8 million). A final approval hearing will determine attorney's fees and expenses and incentive awards. CLICK HERE.

British Columbia's Family Status Discrimination Test: More Employer-Friendly Than Family-Friendly?

In *British Columbia (Human Rights Tribunal) v. Gibraltar Mines Ltd.*, 2023 BCCA 168 ("*Gibraltar*"), the British Columbia Court of Appeal clarified the test for establishing *prima facie* family status discrimination. In British Columbia, employees are still required to establish that a term or condition of employment results in a serious interference with a substantial parental or other family duty or obligation. However, *Gibraltar* clarifies that a change in a term or condition of employment is not a precondition to a finding of *prima facie* discrimination.

In our previous post on the issue of family status discrimination, we highlighted that there is no unified test in Canada for establishing *prima facie* family status discrimination. Instead, different Canadian jurisdictions apply different tests. In 2021, the Court of Appeal of Alberta ("ABCA") affirmed the applicable test for Alberta employees, as discussed in our previous post. A full panel of the Court of Appeal for British Columbia ("BCCA" or "Court") has now clarified the applicable test for British Columbia employees in its recent *Gibraltar* decision.

In British Columbia, the leading authority on family status discrimination is *Campbell River & North Island Transition Society v. H.S.A.B.*, 2004 BCCA 260 ("*Campbell River*"). *Campbell River* has given rise to conflicting interpretations and has received criticism from other courts, including from the ABCA, for setting a higher threshold for establishing discrimination based on family status relative to other prohibited grounds of discrimination.

In *Gibraltar*, the Court focused on the proper interpretation of the *Campbell River* test. The Court held that the *Campbell River* test does not require a change in a term or condition of employment as a precondition to a finding of *prima facie* discrimination. However, the Court affirmed that *Campbell River* defined the scope of family status discrimination to include only serious interference with a substantial parental or other family duty or obligation. The Court also emphasized the materiality threshold created by the "serious" and "substantial" requirements.

Facts and Summary of Previous Decisions
The complainant in the underlying human rights complaint was a journeyman welder who worked 12-hour shifts. Her spouse also worked for Gibraltar Mines Ltd. ("Gibraltar Mines"). After the birth of their child, the complainant requested a change to her, and her spouse's, work schedule to accommodate childcare arrangements. The parties were unable to reach a suitable accommodation. The complainant subsequently filed a human rights complaint alleging discrimination based on family status (among other grounds).

Tribunal Decision
Gibraltar Mines argued that the family status complaint should be dismissed as there had been no change in a term or condition of the complainant's employment. The British Columbia Human Rights Tribunal ("Tribunal") concluded that *Campbell River* did not stand for the proposition that a change in a term or condition of employment was necessary before *prima facie* family status discrimination could be established. The Tribunal decided to allow the family status complaint to proceed to a hearing.

BCSC Decision
Gibraltar Mines sought judicial review of the Tribunal's decision. The Supreme Court of British Columbia ("BCSC") quashed the Tribunal's decision, finding that *Campbell River* required a change in a term or condition of employment as a precondition to a finding of *prima facie* discrimination.

BCCA Decision
The Tribunal appealed the BCSC decision. The BCCA found that the Tribunal had standing to bring the appeal and allowed the appeal.

The appeal focused on the proper interpretation of the *Campbell River* test for establishing *prima facie* family status discrimination. The test set out in *Campbell River* was as follows:

Whether particular conduct does or does not amount to *prima facie* discrimination on the basis of family status will depend on the circumstances of each case. **In the usual case** where there is no bad faith on the part of the employer and no governing provision in the applicable collective agreement or employment contract, it seems to me that **a *prima facie* case of discrimination is made out when a change in a term or condition of employment imposed by an employer results in a serious interference with a substantial parental or other family duty or obligation of the employee.**
[Emphasis added.]

In *Gibralter*, the Court concluded that the reference to "a change in a term or condition of employment" was not to be taken as an exhaustive statement of the test for *prima facie* discrimination. The Court gave three reasons for this interpretation:

1. the question of whether a change in the employee's circumstances could lead to a term or condition of employment resulting in a serious interference with a substantial parental or other family duty or obligation was not before the Court in *Campbell River*. Rather, the issue in *Campbell River* was the meaning and scope of family status;
2. British Columbia's *Human Rights Code* ("Code") does not require a change in a term or condition of employment to trigger *prima facie*discrimination; and
3. it has consistently been held that human rights legislation is characterized as quasi-constitutional and must be given a broad and liberal interpretation.
4.

As such, the Court concluded that a change in a term or condition of employment is not a precondition to a finding of *prima facie* discrimination. However, the Court upheld the materiality threshold set out in *Campbell River* which requires a **serious** interference with a **substantial** parental or other family duty or obligation.

The Court acknowledged that *Campbell River* has been criticized for requiring a higher threshold for establishing discrimination based on family status relative to other prohibited grounds of discrimination. However, the Court dismissed such criticism as misconceived, noting that the materiality threshold does not create a "different test" for family status, but rather provides a workable definition of family status. The Court noted this was particularly important in British Columbia (as opposed to other jurisdictions as "family status" is not defined the Code. The Court emphasized the importance of the materiality threshold to prevent any family obligation that is impacted by an employee's conditions of employment from constituting *prima facie* discrimination.

Ultimately, the Court set out the test for establishing *prima facie* family status discrimination as follows:

1. the complainant must establish that their family status includes a **substantial** parental or other family duty or obligation;
2. the complainant must establish that they suffered a **serious** adverse impact arising from a term or condition of employment; and
3. the complainant must establish that their family status was a factor in the adverse impact.

Key Takeaways
Gibraltar has clarified the test for establishing *prima facie* family status discrimination in British Columbia. The BCCA has made it easier for employees to claim family status discrimination by confirming that a change in employment terms is not a precondition to a finding of *prima facie* discrimination. However, the BCCA has maintained an otherwise stringent test for family status discrimination. In particular, the materiality threshold means employees are still required to establish a **serious** interference with a **substantial** parental or family duty or obligation. As noted in *Gibraltar*, this threshold is meant to ensure that not every conflict between work and family obligations is considered to be discriminatory.

Additionally, while *Gibraltar* clarifies the test for family status discrimination in British Columbia, employers must continue to be aware that the test differs in other Canadian jurisdictions. Responses to requests for accommodation based on family status must therefore be tailored accordingly.
CLICK HERE.

CJEU Determines that a Mere Infringement of the GDPR is not Sufficient to Require Compensation

On May 4, 2023, the Court of Justice of the European Union ("CJEU") issued a judgment in the Österreichische Post case (C-300/21). In the decision, the CJEU clarified that a mere infringement of the EU General Data Protection Regulation ("GDPR") is not sufficient to give data subjects the right to receive compensation under Article 82 of the GDPR. Article 82 provides that "any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."

Background
The case dates back to 2017 when the Austrian Post ("Österreichische Post") collected data relating to the political affinities of Austrian residents. In particular, the Austrian Post used an algorithm to define "target group addresses" based on selected socio-demographic features, and classified individuals into target groups. The data was subsequently sold to various organizations to enable them to send targeted advertising in relation to political elections.

One individual filed a complaint relating to this practice and claimed €1,000 in non-material damage.

The CJEU Decision
According to the CJEU, a broad interpretation of the GDPR provision regarding the right to compensation would be contrary to the text of the law. The CJEU highlighted that compensation is required only when three conditions are met: (1) personal data is processed in a manner that infringes the GDPR; (2) the data subject suffered damage; and (3) there is a causal link between the unlawful processing and the damage suffered.

The CJEU also rejected the proposition of a required minimum threshold to award compensation for non-material damage under the GDPR. Instead, the CJEU found that the GDPR requires "full and effective compensation for the damage" and that establishing a minimum threshold would risk undermining the coherent application of the GDPR.

Finally, the CJEU confirmed that, in the absence of rules in the GDPR on the assessment of damages, the matter should be regulated at the EU Member States level, including, in particular, "the criteria for determining the extent of the compensation payable in that context, subject to compliance with [the] principles of equivalence and effectiveness."
CLICK HERE.

INTERNATIONAL DEVELOPMENTS

EU Whistleblower Directive – Where Are We Now?

As the last of the EU member states implement the Whistleblower Directive, we recap the new rules employers need to be aware of, and give our views on whether a 'one size fits all' approach is feasible.

Background: the Directive

Back in October 2019, the EU 'Whistleblower Directive'[1] became effective, requiring EU member states to pass local laws providing minimum standards. Most missed the original deadline of 17 December 2021, but more recently, implementation has picked up pace. This alert gives an update on the status of these new whistleblowing standards across Europe, and recaps the key actions for employers.

Recap: whistleblower standards

The purpose of the Directive was to require EU Member States to establish common minimum standards to ensure that:

1. Companies with at least 50 employees must set up internal reporting channels to allow workers to report breaches of EU law[2]; and
2. Persons who report (whether internally or externally, i.e., to the relevant authorities) or publicly disclose breaches are legally protected against retaliation from their employer or colleagues.

The Directive applies to persons working in the private or public sector who acquire information on a breach "in a work-related" context. Protection also extends to "facilitators" (i.e., persons who assist a whistleblower in the reporting process at work), and to "third persons" (i.e., people such as colleagues or relatives who are connected with the whistleblower and could suffer retaliation at work).

Note: the Directive only covers breaches of certain specified areas of EU law, such as public health, protection of the environment, product safety, financial services and markets, and data privacy. Member States are however free to choose whether to establish whistleblower reporting channels and protections in relation to breaches of other laws, and a number have done that.

Conditions for protection

Under the Directive, a whistleblower is entitled to protection, provided:

1. They had reasonable grounds to believe that the information on the breach reported was true at the time of reporting, and that information fell within the scope of the Whistleblowing Directive; and
2. They reported the breach (or made a public disclosure about it) in accordance with the relevant requirements of the Directive.

Note: the Directive does not require whistleblowers, in the first instance, to use internal reporting channels; the protection applies even if they go directly to the competent authorities to report the breach. However, protection in relation to public disclosures normally only applies if the whistleblower has first reported the breach either internally or externally and no action has been taken within a defined period.

Protection from retaliation

The Directive requires Member States to prohibit any form of retaliation (such as dismissal, disciplinary sanctions, or demotion) against the whistleblower. It also provides for a reversal of the burden of proof in cases of alleged retaliation: once a worker proves in court that they reported a breach and suffered a detriment, the employer must then prove that the detrimental treatment was based on duly justified grounds.

Local country status

Member States had until 17 December 2019 to implement the Directive (save that companies with 50 to 249 employees could be given until 17 December 2023 to set up internal reporting channels).

Most countries have now passed legislation with only seven stragglers remaining, including Germany, Poland, and Luxembourg. As usual, it has not led to a totally level playing field for employers: although all countries have applied

the minimum standards in the Directive, many have gone further in protecting a wider scope of reports (rather than just breaches of EU law), allowing anonymous reporting (albeit in some countries, with a lower level of protection), the types of internal reporting channels to be used, and the level of sanction against employers for breach.

What should employers be doing now?
Employers will want to check that their internal reporting procedures comply with local law in each European country in which they have an entity with a headcount of at least 50 workers, even if that country has not yet implemented the Directive.

However, multinational employers will prefer to adopt a uniform reporting procedure across Europe, in order to ensure consistency of approach.

Checking compliance with local law in each EU State could in any case be time-consuming and costly, so multinationals might consider a more pragmatic initial approach of checking that their reporting procedure at least complies with the minimum requirements of the Directive, in particular as regards:

- Who is allowed to file a report. According to the Directive, this should include not only a current employee, but also a candidate, former employee, worker, self-employed person, volunteer, or trainee. Personnel working under the supervision of contractors, subcontractors, and suppliers are also included;
- The types of breach that can be reported via the company's internal channel;
- Whether to allow anonymous report: in most countries this should be allowed, but the data privacy considerations need careful handling. Ensuring reports can be made to an in-country reporting line avoids some of these issues, but in some countries employee representative obligations will still be triggered;
- Arrangements for receiving reports (to ensure the confidentiality of identity of the whistleblower, and to prevent access by unauthorised personnel);
- Acknowledgement of receipt of the report within seven days;
- Designation of a person or team to follow up on the report, maintain communication with the whistleblower and provide feedback to them within three months on the action envisaged or taken and the grounds for it.

This approach does not guarantee full legal compliance in each country, so multinationals are advised to make strategic choices as regards checking local laws in key locations depending upon their particular footprint in Europe. There are also broader questions for employers to address, for example as to whether reporting is handled via an outsourced provider or internally (in which case, a local reporting route should be available rather than relying on a centralized hotline), and how information from reports is shared and acted on across a group of companies.

What about the UK?
As a footnote, the UK (although no longer part of the EU and so not covered by European Directives) has recently announced a review of its own whistleblower framework. The driver is however to address potential weaknesses in the UK's longstanding whistleblower protection regime, rather to align with the new EU regime. So, any changes may put the UK further out of alignment with the EU, for example in terms of reporting mechanisms, which individuals are protected, and levels of protection (with whistleblower remedies already higher than most EU countries, although well below the US). But our experience is that multinational employers are able to create a framework that takes a reasonably consistent approach across Europe, by accepting this will go beyond the minimum rules in some countries.

[1] More properly known as Directive (EU) 2019/1937 on the protection of persons who report breaches of EU law.
[2] There is no minimum headcount threshold for employers in financial services and other specific sectors.
CLICK HERE.

New Mandatory Reporting Requirement for Businesses: Canada's Modern Anti-Slavery Bill Becomes Law

Bill S-211, *Fighting Against Forced Labour and Child Labour in Supply Chains Act* (the "**Act**"), Canada's modern slavery legislation, passed in the House of Commons today. As a result, businesses and government bodies will be required to annually report on their efforts to prevent or mitigate the risk that forced labour or child labour exists in their supply chains.

The first such report will need to be filed with the government by May 31, 2024, and will need to be published prominently on the business' website.

The Act aims to combat the prevalence of forced labor in global supply chains by requiring companies to disclose information on their efforts to address forced labour in their operations and supply chains. This includes information about the company's policies and due diligence processes, as well as the actions taken to address identified risks.
Failure to comply with the reporting obligations under the new Act can result in fines and reputational damage and creates liability for directors and officers.

Reporting requirements are mandatory for companies listed on a Canadian stock exchange or have a nexus to Canada. Nexus to Canada is established by having assets, a place of business, or doing business in Canada, and meeting two of the three following thresholds: $20 million in assets, $40 million in revenue, or 250 employees. For more details, see our previous bulletin on Bill S-211.

The legislation also creates a prohibition on importing goods made of child labour, which will be enforced by Canada Border Services Agency, in line with the prior-enacted prohibition on goods made of forced labour.
CLICK HERE.

EU-U.S. Transfers: Privacy Shield replacement not adequate says European Parliament

The road to the adoption of a lasting framework for EU-U.S data transfers has been anything but smooth. Much like its predecessor, Safe Harbor, the EU-U.S Privacy Shield met its end in 2020 when the Court of Justice of the European Union ("**CJEU**") ruled that the arrangement failed to comply with the EU GDPR. The replacement EU-U.S Data Privacy Framework (the "**Framework**"), first announced by the White House in October 2022, represents the latest attempt, albeit one which is facing increased scrutiny from EU law makers as they deliberate over the award of an adequacy decision.

In a non-binding resolution adopted on 11 May 2023 (the "**Resolution**"), the European Parliament called on the European Commission not to award an adequacy decision in respect of the Framework. This follows on from concerns raised by the European Data Protection Board ("**EDPB**") in its non-binding opinion, adopted on 28 February 2023, concerning the sufficiency of the Framework.

Background
The European Commission launched the process for the adoption of an adequacy decision in respect of the United States and the Framework on 13 December 2022 (discussed in our previous insight), following U.S President Biden's signing of an Executive Order on 7 October 2022. The Executive Order established: (i) legally binding safeguards to address concerns identified by the CJEU in its *Schrems II* ruling, and (ii) a Data Protection Review Court ("**DPRC**") to protect individuals' rights of redress, where their personal data are transferred to the United States. The Framework comprises a set of privacy principles, which the European Commission's draft adequacy decision approved as offering protection to EU citizens' personal data that is 'essentially equivalent' to that received under the EU GDPR.

Concerns raised by MEPs
While the Resolution notes that the Framework contains significant improvements, compared with previous iterations (e.g. Privacy Shield), it concludes that it does not go far enough to provide 'essentially equivalent' protection to that guaranteed under the EU GDPR.

Key concerns include:

- A lack of transparency in DPRC procedures due to their decisions being classified and not made public or available to the complainant, thereby undermining data subjects' rights to access and rectify their personal

data.

- Insufficient guarantees in relation to the independence of DPRC judges, due to the U.S President's ability to dismiss them and overrule their decisions.
- The permissibility of bulk collection of personal data in certain cases and the failure to provide sufficient safeguards where bulk collection occurs. For example, the Resolution notes the lack of any requirement for independent prior authorisation to conduct bulk collection, alongside the absence of clear and strict data retention rules.

The Resolution concludes that, in order for the European Commission to satisfy its obligation to assess adequacy based on the *practical application* of legislation and guidelines in the relevant third country, it can only adopt an adequacy decision once steps have been taken by the U.S to ensure that the commitments specified in the Executive Order have been delivered. Specifically, only once (i) the U.S Intelligence Community has updated its policies and practices in line with such commitments (which it has until October 2023 to do) and (ii) the U.S Advocate General has named the EU and its Member States as qualifying countries for eligibility to access the remedies available under the DPRC.

The Resolution also underlines the need to ensure that the Framework is 'future-proof' and can withstand legal challenges, which appear inevitable. To this end, the European Parliament calls on the European Commission not to grant an adequacy decision based on the Framework and instead, to negotiate a regime that is likely to be held up in court. While the Resolution is not binding, it will be considered by the European Commission (alongside the non-binding opinion issued by the EDPB) in determining whether to formally issue an adequacy decision in respect of the Framework.
CLICK HERE.

Brazilian ANPD Publishes Statement on Youth Data Processing

Brazil's National Data Protection Authority (ANPD) has finally published its first Statement, providing legally binding guidance on the lawful bases applicable to the processing of personal data of children and adolescents.

In response to suggestions received in the public consultation, the ANPD understood that the processing may be based on any of the legal bases listed in Articles 7 and 11 of the General Data Protection Law (LGPD), as long as they observe the principle of the best interests of minors – and not only on the lawful basis of consent. According to the Statement:

"The processing of personal data of children and adolescents may be carried out based on the lawful bases foreseen in Article 7 or in Article 11 of the General Data Protection Law (LGPD), provided that their best interest is observed and prevails, to be evaluated in the each specific case, pursuant to Article 14 of the Law."

The interpretation adopted by the ANPD is the same as in Statement No. 684 of the IX Civil Law Conference, published last year:

"Statement No. 684: Article 14 of Law No. 13.709/2018 (General Data Protection Law - LGPD) does not exclude the application of other legal bases, if applicable, observing the best interests of the child."

Thus, any lawful basis may be adopted for the processing of data, taking into consideration the specific case for each processing activity. In addition, when consent is the applicable lawful basis for processing personal data of children under the age of 12, it must be granted by at least one parent or guardian.
CLICK HERE.

MISCELLEANOUS DEVELOPMENTS

Government Agencies Join Forces Against Bias and Discrimination in AI

On April 25, 2023, four federal government agencies released a joint statement announcing their resolve against bias and discrimination in automated systems and artificial intelligence (AI). Together, the Consumer Financial Protection Bureau (CFPB), the Department of Justice's Civil Rights Division (DOJ), the Equal Employment Opportunity Commission (EEOC) and the Federal Trade Commission (FTC) will jointly seek to ensure that innovation does not supplant individual rights and regulatory compliance. Specifically, these federal agencies will continue to scrutinize the implementation of new AI technology to protect civil rights, equal employment opportunity, fair competition and consumer protection.

Automated systems and AI permeate a variety of industries, including entertainment, healthcare, employment and financial services. Software and algorithmic processes can be used to streamline workflows, assist individuals in completing tasks and simplify decision-making. However, the DOJ, FTC, EEOC and CFPB are concerned that the increasing reliance on automated systems likewise will increase the risk of unlawful biases and discrimination:

- More public and private organizations are using these automated systems to make "critical decisions that can impact individuals' rights and opportunities, including fair and equal access to a job, housing, credit opportunities, and other goods and services."
- "Although many of these tools offer the promise of advancement, their use also has the potential to perpetuate unlawful bias, automate unlawful discrimination, and produce other harmful outcomes."

As noted in the joint statement, automated systems and AI depend upon large data sets to identify patterns, perform tasks and make predictions. If the underlying data set is unrepresentative, then the system could produce biased and discriminatory results. The lack of transparency in some of these automated systems may further complicate the issue, making it difficult for users to identify potential bias or discrimination in outcomes.

Practical Takeaways
The joint statement confirms the federal government's increased scrutiny of automated systems and AI-enabled technologies. As seen in the employment context, state regulators also are introducing laws and guidance aimed at enforcing responsible innovation. Employers, healthcare providers and technology developers, among others, should (1) monitor updates to federal, state and foreign regulation of automated systems; and (2) assess their organizations' intentional and inadvertent use of AI to comply with regulations and ensure best practices.
CLICK HERE.

Florida Health Information Storage Changes Taking Effect on July 1, 2023

Foreign Interests in the health care provider environment has generally meant ownership interests of persons from outside of the state in which the healthcare provider operates, rather than foreign countries. Thus, it would be easy to miss the healthcare provisions in the recent Florida legislative bill that was signed into law on May 8, 2023 entitled Interests of Foreign Countries (CS/SB 264).

Governor DeSantis signed legislation, effective on July 1, 2023, that changed Section 408.051 of the Florida Statutes to add a new Section 3 that requires that a health care provider that utilizes a certified electronic health record technology to ensure that all patient information when stored in an offsite physical or virtual environment, including third-party or subcontracted computer facilities or an entity providing cloud computing services, is physically maintained in the continental United States or its territories or Canada.

Although some states have certain data storage rules tied to Medicaid that restrict storage in foreign countries, Florida's new law would affect all payors within the State of Florida.

Additionally the new legislation adds a very broad definition of "health care provider" to include most health care practitioners licensed by the Department of Health, entities regulated by Florida's Agency for Health Care Administration (AHCA), pharmacies, continuing care facilities and more.

As health care entities look to their data storage needs, it will be increasingly important to review both Federal and State guidelines to when choosing EHR and data storage needs.

New Section 408.051(3) - SECURITY AND STORAGE OF PERSONAL MEDICAL INFORMATION. In addition to the requirements in 45 C.F.R. part 160 and 780 subparts A and C of part 164, a health care provider that utilizes certified electronic health record technology must ensure that all patient information stored in an offsite physical or virtual environment, including through a third-party or subcontracted computing facility or an entity providing cloud computing services, is physically maintained in the continental United States or its territories or Canada. This subsection applies to all qualified electronic health records that are stored using any technology that can allow information to be electronically retrieved, accessed, or transmitted.
CLICK HERE.

High Times: Marijuana Positivity in Workplace Drug Tests Reaches 25-Year Record

***Seyfarth Synopsis**: Across nationwide testing, marijuana positivity rates for 2022 reached 4.3% (up from 2.7% in 2017), with biggest gains found in states that legalized recreational marijuana.*

Impairment and related safety hazards have been disrupting the workplace resulting in lost time, absenteeism, safety hazards, and serious industrial accidents. We track annual positivity test reports from Quest Diagnostics, one of the country's largest drug testing laboratories. Quest's recently released 2023 Drug Testing Index reveals that while positivity rates for some drugs declined, the rise in positivity rates for marijuana and amphetamine continues to climb. Of the more than six million general workforce marijuana tests that Quest performed in 2022, 4.3% came back positive, up from 3.9% the prior year. Worse still, *post-accident* marijuana positivity of urine drug tests in the general U.S. workforce was 7.3%, an increase of 9% compared to 6.7% in 2021. While not entirely clear, it is possible that the widespread state legalization of marijuana has contributed to an increase in test positivity and also workplace safety hazards.

Scientific testing indicates greater likelihood of errors in judgment and workplace accidents where an employee is impaired by marijuana. A National Safety Council white paper continues to recommend a Zero Tolerance Policy for marijuana in safety-sensitive positions. Federal OSHA further advocates for post-accident drug testing as a legitimate part of a root cause analysis to determine the cause of an accident. Employers have struggled to address the hazard of marijuana impairment at work and how best to protect workplace safety.

A problem for employers is that none of the scientifically valid drug tests for marijuana definitively prove whether a person is impaired at or near the time of an accident or the time they provide a specimen for testing. Moreover, state and local marijuana laws are making it increasingly difficult for employers to even consider or act on a positive marijuana test result. Accordingly, employers looking to address drugs and alcohol in the workplace should work with outside counsel to ensure compliance with their current drug and alcohol testing programs.
CLICK HERE.