FEBRUARY 2024

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 | FEBRUARY 2024

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

Shared Applicant Pools for Agency Jobs

The Office of Personnel Management (OPM) announced an initiative for federal agencies to pursue pooled hiring with a focus on skills-based selection, evaluating needed skills versus applicants' education and past employment history. In other words, when one agency goes through the steps to recruit, interview, and select an employee, the list of prospective employees that are deemed qualified for federal employment would then be shared with other agencies hiring for a similar role.

There are clear benefits to using a pooled applicant approach including streamlining resources and capitalizing on the strengths of some agencies' selection processes to fill similar job vacancies across agencies. This may decrease time to hire and maximize effective selection processes.

However, these gains cannot shadow the need for continued efforts for equal employment opportunity and implementation of this process leads to some important questions for federal agencies, including:

- How will each agency meet record keeping requirements for job seekers and qualified applicants?
- How are agencies advised to monitor adverse impact with multiple agencies having access to the same pool?
- Which agency is responsible for validating employment tests if statistical and practical indicators for adverse impact are identified through monitoring of selection outcomes?
- If there is adverse impact, which agency is liable?
- How will each agency measure the effectiveness of outreach and recruitment towards equal employment opportunities and diversity, equity, and inclusion (DEI) programs?
- Is research available to agencies to understand how pooled hiring impacts equal employment opportunity and diversity, equity, and inclusion?
- What recommendations have been provided to agencies to maximize diversity efforts while utilizing pooled hiring practices?

Of course, the implementation of a new approach to hiring also yields many general questions, including:

- Do multiple agencies have access to the open pool of qualified candidates at the same time?
- What happens if more than one agency is interested in the same candidate?
- Can one agency decline an applicant deemed to be certified for employment? If yes, will that individual be removed from the eligibility pool for use by other agencies?
- How frequently will the qualified list be updated with newly interested and qualified candidates?

Considerations for Federal Contractors and Other Private Employers

To be clear, this initiative only affects federal agencies. However, initiatives for federal agencies can sometimes affect future obligations for federal contractors and other private employers. A pooled approach to hiring would be a sea change for private employers and would undoubtedly result in serious effects on their equal employment opportunity, affirmative action, and DEI programs, effects that regulatory agencies like the Office of Federal Contract Compliance Programs or the Equal Employment Opportunity Commission may not appreciate.
CLICK HERE.

Proposed Rule That Will Require Federal Contractors and Subcontractors to Disclose Compensation Data in Job Postings and Prohibit Compensation History Inquiries Released

Seyfarth Synopsis: *Twenty-four hours after the White House marked the 15th Anniversary of the Lilly Ledbetter Fair Pay Act, by announcing a set of actions designed to support equal pay principles for workers of federal contractors and agencies as set forth by Executive Orders 14035 and 14069, the Federal Acquisition Regulatory Council published a proposed rule that, if adopted, would prohibit federal contractors and subcontractors from seeking or considering compensation history and requiring them to disclose compensation and other benefits in job advertisements. The proposed rule includes a 60 day comment period that ends on April 1, 2024.*

Earlier this week, the Federal Acquisition Regulatory Council which consists of the US Department of Defense, General Services Administration, National Aeronautics and Space Administration, and Office of Federal Procurement Policy, published a proposed rule titled, "Prohibition on Compensation History Inquiries and Requirement for Compensation Disclosures by Contractors During Recruitment and Hiring," in the Federal Register. According to the Notice, the intended impact of the rule is to "promote pay equity by closing pay gaps, which leads to increased worker satisfaction, better job performance, and overall increased worker productivity - all factors associated with promoting economy, efficiency, and effectiveness of the Federal contractor workforce."

If adopted as proposed, the rule will have significant implications for federal contractors and subcontractors.[1] Specifically, the proposed rule has four main components: (1) a compensation history ban, (2) a compensation disclosure requirement for job advertisements, (3) an applicant notice provision, and (4) contractual flow down obligations for subcontracts.

Applicability

The prohibitions and requirements of the proposed rule are broad and would apply to contractors with federal contracts and subcontracts for commercial products (including Commercially Available Off-the-Shelf (COTS) Items) or commercial services valued in excess of $10,000, and to be performed within the United States (including its outlying areas). This means that if the rule is adopted as proposed, it would apply to most contractors, even those that *do not* meet the $50,000 threshold that triggers affirmative action program requirements.

The proposed rule is also limited to the recruitment and hiring of positions that will perform work on or in connection with a federal contract or subcontract, defining "work on or in connection with the contract" as work called for by the contract or work activities necessary to the performance of the contract. From a practical perspective, however, it will likely be exceedingly difficult for contractors to determine whether a worker may perform work on or in connection with a covered contract at the point of recruitment or hire. Perhaps for this reason, the proposed rule *encourages* (but does not *require*) contractors to apply these compensation history prohibitions and disclosure requirements to other positions, including those the contractor reasonably believes could eventually perform work on or in connection with the covered contract.

Compensation History Ban

As many states and local jurisdictions have done over the past few years, the proposed rule would prohibit federal contractors from:

1. Seeking an applicant's compensation history, either orally or in writing, directly from any person, including the applicant or the applicant's current or former employer or through an agent;
2. Requiring disclosure of compensation history as a condition of an applicant's candidacy;
3. Retaliating against or refusing to interview or otherwise consider, hire, or employ any applicant for failing to respond to an inquiry regarding their compensation history; and
4. Relying on an applicant's compensation history to screen or consider the applicant for employment or in determining the compensation for the applicant at any stage in the selection process.

As used in the proposed rule, "compensation history" means "the compensation an applicant is currently receiving or the compensation the applicant has been paid in a previous job." Further, in contrast to certain states and local jurisdictions that allow employers to consider or rely on an applicant's salary history that was voluntarily provided, the proposed rule prohibits contractors from taking the actions outlined above at *any* stage in the recruitment and hiring

process, even if the applicant volunteers their compensation history without prompting.

Notably, the proposed rule defines "applicant" as "a prospective employee or *current employee* applying for a position to perform work on or in connection with the contract." (emphasis added). Thus, unless the proposed rule is modified, employers would be prohibited from considering a current employee's salary when determining compensation for that employee's new role within the company.

Compensation Disclosure Requirements for Job Advertisements
Following state and local trends, the proposed rule also would require contractors to disclose in job advertisements the compensation to be offered for positions working on or in connection with a federal contract. Specifically, the disclosures must include the salary or wages (or range) the contractor in good faith believes that it will pay for the advertised position, as well as a general description of the benefits and other forms of compensation applicable to the job opportunity. The proposed rule defines "compensation" broadly to include "any payments made to, or on behalf of, an employee or offered to an applicant as remuneration for employment, including but not limited to salary, wages, overtime pay, shift differentials, bonuses, commissions, vacation and holiday pay, allowances, insurance and other benefits, stock options and awards, profit sharing, and retirement."

In determining the salary or wage range, contractors may use the contractor's pay scale for that position, the range of compensation for those currently working in similar jobs, or the amount budgeted for the position. Further, for positions where at least half of the expected compensation is derived from commissions, bonuses, and/or overtime pay, the contractor must specify the percentage of overall compensation or dollar amount, (or range), for each form of compensation that the contractor, in good faith, believes will be paid for the advertised position.

Notice to Applicants
Contractors must also provide written notice to applicants covered under the compensation history ban and disclosure requirements. The notice must be part of the job announcement or application process and include specific language contained in the required contract clause provisions. This language notifies applicants about the prohibitions under the proposed rule, and provides details on how to file a complaint, including how to file a discrimination complaint with the Department of Labor's Office of Federal Contract Compliance Programs ("OFCCP").

Contractual Provisions for Subcontracts
Contractors will also be required to "include the substance" of the contract clause in all solicitations and contracts, including in all subcontracts, where the principal place of performance is within the United States. The contract clause details all of the proposed rule's requirements and prohibitions including the compensation history ban, compensation disclosure requirement, applicant notice, and contract clause flow down requirements.

Complaint Process and OFCCP Involvement
In addition to the prohibitions and requirements addressed above, contractors should be aware that the proposed rule provides for an applicant complaint process whereby an applicant can allege compliance violations. Under the proposed rule, an applicant alleging violations may submit a complaint to the contracting agency point of contact as identified at http://www.dol.gov/general/labor-advisors. The complaint must be submitted within 180 days of the date the alleged violation occurred.

Further, applicants who wish to submit complaints that allege discrimination prohibited by Executive Order 11246, Section 503 of the Rehabilitation Act of 1973, and the Vietnam Era Veterans' Readjustment Assistance Act would continue to submit complaints directly to the OFCCP. If complaints alleging discrimination are submitted to an agency point of contact rather than directly with OFCCP, the complaints will be forwarded to OFCCP for review.

Next Steps for Federal Contractors and Subcontractors
While the supplemental information accompanying the proposed rule identifies several anticipated benefits including reducing the pay gaps that disadvantage certain populations, increasing the pools of qualified applicants, incentivizing applicants to invest in job-related skills and experiences, reducing turnover rates, and lowering recruiting costs, if adopted, these new requirements and prohibitions will require significant effort and planning for federal contractors.

Although the proposed rule is only at the notice and comment stage, federal contractors should begin preparing a strategy on how it will comply with these new requirements should they become final. At a minimum, contractors should inventory their current federal contracts and subcontracts and identify the jobs that perform work on or in connection with those contracts. Further, nationwide contractors who are currently juggling the patchwork of state and local laws banning salary history inquiries and requiring compensation disclosures in job advertisements, may consider adopting a nationwide approach to simplify compliance in these areas.

Opportunity to Comment
Those that wish to submit comments in response to the proposed rule may do so via the Federal eRulemaking portal at *https://www.regulations.gov* by searching for "FAR Case 2023–021." Select the link "Comment Now" that corresponds with "FAR Case 2023–021" and follow the instructions provided. Comments in response to the proposed rule must be submitted by April 1, 2024.
CLICK HERE.

Cannabis Rescheduling: HHS Findings and Legal Implications

On August 29, 2023, the U.S. Department of Health and Human Services (HHS) made a groundbreaking recommendation to the Drug Enforcement Administration (DEA) – that cannabis should be rescheduled from Schedule I to Schedule III under the Controlled Substances Act (CSA). This recommendation was made pursuant to President Biden's request that the Secretary of HHS and the Attorney General initiate a process to review how cannabis is scheduled under federal law. In recent days, the unredacted 252-page analysis supporting the August recommendation was released pursuant to a Freedom of Information Act request. While the DEA is presently reviewing HHS's recommendation and has final authority to schedule a drug under the CSA, it is ultimately bound by HHS's recommendations on scientific and medical matters.

Why does this matter? Cannabis[1] has been a Schedule I substance since the CSA was enacted in 1971. Substances are controlled under the CSA by placement on one of five lists, Schedules I through V. Schedule I controlled substances are subject to the most stringent controls and have no current accepted medical use. As a result, it is illegal under federal law to produce, dispense, or possess cannabis except in the context of federally approved scientific studies. Violations may result in large fines and imprisonment, including mandatory minimum sentences. Comparatively, Schedule III substances are considered to have less abuse potential than Schedule I and II substances, and have a currently accepted medical use in the United States.

In recent years, nearly all the states within the U.S. have revised their laws to permit medical cannabis use. And 24 states, as well as the District of Columbia, have eliminated certain criminal penalties for recreational cannabis use by adults. However, under the U.S. Constitution's Supremacy Clause, federal law takes precedence over conflicting state laws. Thus, states cannot actually legalize cannabis use without congressional or executive action, and all unauthorized activities under Schedule I involving cannabis are federal crimes *anywhere* in the United States.[2]

Notable Findings in HHS's Recommendation
For HHS to recommend that the DEA change cannabis from Schedule I to Schedule III, HHS had to make three specific findings: 1) cannabis has a lower potential for abuse than the drugs or other substances in Schedules I and II; 2) cannabis has a currently accepted medical use in treatment in the U.S.; and 3) abuse of cannabis may lead to moderate or low physical dependence or high psychological dependence. HHS considered eight factors to make those findings, some of which include: cannabis's actual or relative potential for abuse; the state of current scientific knowledge regarding the drug; the scope, duration, and significance of abuse; and what, if any, risk there is to public health. The unredacted analysis provides further insight into HHS's determination to make the forementioned findings.

Cannabis has a potential for abuse less than the drugs or other substances in Schedules I and II.
To evaluate cannabis's potential for abuse,[3] HHS compared the harms associated with cannabis abuse to the harms associated with other substances, such as heroin (Schedule I), cocaine (Schedule II), and alcohol.[4] HHS reported that evidence shows some individuals take cannabis in amounts sufficient to create a health hazard to themselves and the safety of other individuals and the community. However, HHS also reported evidence showing the vast majority of cannabis users are using cannabis in a manner that does not lead to dangerous outcomes for themselves or others. From 2015 to 2021, the utilization-adjusted rate of adverse outcomes involving cannabis was consistently lower than the respective utilization-adjusted rates of adverse outcomes involving heroin, cocaine, and other comparators. Further, cannabis was the lowest-

ranking group for serious medical outcomes, including death. Overall, the data indicated that cannabis produced fewer negative outcomes than Schedule I, Schedule II drugs, and, in some cases, alcohol.

Cannabis Has a Currently Accepted Medical Use in Treatment in the United States
To determine whether cannabis has a currently accepted medical use (CAMU) in the U.S., HHS evaluated a two-part standard: 1) whether "[t]here exists widespread, current experience with medical use of the substance by [healthcare providers] operating in accordance with implemented jurisdiction-authorized programs, where medical use is recognized by entities that regulate the practice of medicine"; and 2) whether "[t]here exists some credible scientific support for at least one of the medical uses for which Part 1 is met."

Under Part 1, HHS confirmed that more than 30,000 healthcare providers across 43 U.S. jurisdictions are authorized to recommend the medical use of cannabis for more than six million registered patients for at least 15 medical conditions. The Part 1 findings, therefore, supported an assessment under Part 2. Under Part 2, HHS reported that, based on the totality of the available data, there exists some credible scientific support for the medical use of cannabis. Specifically, credible scientific support described at least some therapeutic cannabis uses for anorexia related to a medical condition, nausea and vomiting (e.g., chemotherapy-induced), and pain.

Overall, while HHS reported that cannabis has a currently accepted medical use in the U.S., the Food and Drug Administration (FDA) underscored that such a finding does *not* mean that the FDA has approved cannabis as safe and effective for marketing as a drug in interstate commerce under the Federal Food, Drug, and Cosmetic Act.

Abuse of cannabis may lead to moderate or low physical dependence or high psychological dependence.
Lastly, HHS concluded that research indicated that chronic, but not acute, use of cannabis can produce both psychic and physical dependence in humans. However, while cannabis "can produce psychic dependence in some individuals," HHS emphasized that "the likelihood of serious outcomes is low, suggesting that high psychological dependence does not occur in most individuals who use marijuana."

Legal Ramifications of New Scheduling
Changing cannabis from Schedule I to Schedule III may potentially allow cannabis to be lawfully dispensed by prescription[5] and states' medical cannabis programs may now be able to comply with the CSA. However, it would not make state laws legalizing recreational cannabis use in compliance with federal law without other legal changes by Congress or the executive branch. Under the change, medical cannabis users may be eligible for public housing, immigrant and nonimmigrant visas, and the purchase and possession of firearms. They may also face fewer barriers to federal employment and eligibility to serve in the military. Researchers would face less regulatory controls, and the DEA would no longer set production quota limitations for cannabis. Because the prohibition on business deductions in Section 280E of the Internal Revenue Code only applies to Schedule I and II substances of the CSA, changing cannabis from Schedule I to Schedule III would allow cannabis businesses to deduct business expenses on federal tax filing.

Importantly, some criminal penalties for CSA violations depend on the schedule of the substance. Thus, if cannabis were to be reclassified as a Schedule III substance, some criminal penalties for CSA violations would no longer apply or be significantly reduced. However, CSA penalties that specifically apply to cannabis, such as quantity-based mandatory minimum sentences, would not change under a new rescheduling.

Many advocates consider HHS's findings a step in the right direction. Specifically, supporters consider the findings further evidence that cannabis should be removed from the CSA altogether and regulated akin to tobacco and alcohol (referred to as descheduling). Given the momentum of cannabis legalization across U.S. states and breakthroughs in the medical and scientific advantages of cannabis, Congressional or Executive legalization, or – at very least – descheduling of cannabis may be on the horizon.
CLICK HERE.

FTC Requires Non-Banking Financial Institutions to Report Data Security Breaches

Beginning May 11, 2024, non-banking financial institutions regulated by the Federal Trade Commission (FTC) will be required to submit notifications of data breaches or other security events that impact 500+ consumers. The FTC issued a final rule (the Rule) amending its Safeguards Rule[1] to impose this notification requirement. The FTC has indicated that such notices will be entered into a publicly available database. Below, we have outlined key requirements for non-banking financial institutions and next steps for compliance.

Key Requirements of the Revised Safeguard Rule

Who Needs to Report?
The Rule applies to all non-banking financial institutions regulated by the FTC, including exempt reporting advisers, state-registered advisers, technology companies, mortgage brokers, credit counselors, financial planners, credit reporting agencies and tax preparers, among others.

When Do You Need to Report?
The Rule requires covered entities to report a "notification event" that impacts at least 500 consumers to the FTC as soon as possible, but no later than 30 days following discovery. A "notification event" means acquisition of unencrypted "customer information" without the authorization of such customer. It is important to keep in mind that under the Safeguards Rule, "customer information" is defined broadly to mean any record containing nonpublic personal information about a customer. For example, such information may include information provided by the consumer to obtain a financial product or service and information collected through cookies on a website.[2] The scope of noticeable information as defined in the Rule is much broader than most state data breach notification statutes.

Additionally, in defining a notification event, the FTC specifies that "customer information is considered unencrypted for this purpose if the encryption key was accessed by an unauthorized person."

The Rule also specifies that a notification event is considered discovered as of the first day on which the notification event is known to any person (other than the person committing the breach) that is an employee, officer or agent of the financial institution.

How Do You Report?
Notice to the FTC must be made electronically through a form that will be made available on the FTC's website.

What Do You Need to Report?
The notice to the FTC must include:

- Name and contact information of the reporting institution.
- A description of the types of information that were involved.
- The date or date range of the notification event (if possible to determine).
- Number of consumers affected.
- A general description of the notification event.
- If applicable, whether any law enforcement official has provided the financial institution with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the FTC to contact the law enforcement official.

Notably, though not an exception to reporting requirement, the Rule provides that a law enforcement official may request a delay in the notice of up to 30 days. The delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Such additional delay may only be permitted if the FTC staff determines that public disclosure would continue to impede a criminal investigation or cause damage to national security.

When Will the Rule Go into Effect?
The Rule will take effect May 11, 2024, which is 180 days after the Rule was published the *Federal Register* (November 13, 2023).

Next Steps

Covered institutions should review existing incident response plans and related policies and procedures to ensure that notification requirements enable timely reporting under the Rule. Additionally, the Rule will likely lead to increased exposure for covered institutions and further affirms the FTC's ongoing engagement in security and privacy enforcement. Such entities should review their privacy and security programs for compliance with the Safeguards Rule and other requirements and implement any measures needed to enhance such compliance.

CLICK HERE.

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

Columbus, Ohio Bans Employers From Inquiring About Salary History

Columbus will soon join Cincinnati and Toledo as the only Ohio localities to implement a "salary history ban." As the name suggests, a salary history ban generally prohibits employers from inquiring about a job applicant's wage rates or salary history while working for a prior employer. Columbus' salary history ban will go into effect March 1, 2024.

Covered Employers and Individuals
The salary history ban applies to all employers with fifteen or more employees within the City of Columbus. The salary history ban protects all individuals applying for employment that will be performed within the City of Columbus, and whose application will be solicited, received, processed, or considered in the City of Columbus, regardless of whether the individual is ultimately interviewed by the employer.

Prohibited Conduct
Under the ordinance, employers are specifically prohibited from doing the following:

1. Inquiring about the salary history of an applicant for employment.
    a. "Inquiring" includes asking questions or making a statement to an applicant, an applicant's current or prior employer(s), or a current or former employee or agent of the applicant's current or prior employer(s) for the purpose of obtaining the applicant's salary history information. An employer is also prohibited from searching public records to obtain an applicant's salary history information.
2. Screening job applicants based on their current or prior wages, benefits, other compensation, or salary histories, including requiring that these categories satisfy minimum or maximum criteria.
3. Relying solely on the salary history of an applicant in deciding whether to offer employment, or in determining the salary, benefits, or other compensation for such applicant during the hiring process, including the negotiation of an employment contract.
4. Refusing to hire or otherwise disfavoring, injuring, or retaliating against an applicant for not disclosing their salary history.

The ordinance does, however, clarify that employers are permitted to engage in discussion with the applicant about the applicant's expectations with respect to salary, benefits, and other compensation and to inform applicants of the proposed or anticipated salary associated with the position for which they have applied.

Exceptions

The salary history ban does not apply to any of the following:

- Actions taken by an employer under any federal, state, or local law that specifically authorizes the reliance on salary history to determine an employee's compensation.
- Applicants for internal transfer or promotion.
- Voluntary and unprompted disclosures of salary history information by an applicant.
- Any attempt by an employer to verify an applicant's disclosure of non-salary related information or conduct a background check, provided that, if the verification or background check discloses the applicant's salary history, that disclosure must not be solely relied upon to determine the salary, benefits, or other compensation of the applicant.
- Applicants who are re-hired by an employer within three years of the applicant's most recent date of termination from that employer, if the employer already has past salary history data regarding the applicant from the applicant's previous employment.
- Positions for which salary, benefits, or other compensation are determined by collective bargaining.
- Federal, state, and local government employers, other than the City of Columbus.

Penalties
The ordinance provides that an aggrieved applicant may file a complaint with the Columbus Community Relations Commission (CRC). If the CRC finds that an employer has violated the salary history ban, the CRC may impose a civil fine of up to $5,000, depending on the number of violations.

Next Steps for Employers
The Columbus ordinance coincides with efforts across the country – both locally and at the state level – to enact legislative measures designed to promote pay equity and encourage fair and equitable pay practices. With the growing popularity of salary history bans both in Ohio and nationwide, employers should be aware of these new regulations and review and adjust their hiring practices accordingly.
CLICK HERE.

California Pay Data Reporting Portal Is Now Open - Employers Must Submit Pay Data Reports By May 8, 2024

California law requires employers with at least 100 employees and at least one California employee, to annually report pay, demographic, and other workforce data to the Civil Rights Department ("CRD"). This reporting is required under Government Code section 12999, and is part of the State's efforts to promote equal pay.

Remote Worker Information Now Required
A new data field added this year requires employers to report the number of employees in an employee group who worked remotely. The State's Pay Data Reporting FAQ's provides that for pay data reporting, "remote worker" refers to employees "who are entirely remote, teleworking, or home-based, and have no expectation to regularly report in person to a physical establishment to perform their work duties. Employees in hybrid roles or (partial) teleworking arrangements expected to regularly appear in person to perform work at a particular establishment for any portion of time during the Snapshot Period would not be considered remote workers for pay data reporting purposes."

Last Year's Additional Requirements Are Still In Effect
Changes implemented last year remain in effect, including the requirements to report workers hired through labor contractors, as well as reporting mean and median pay rates.

Labor Contractors
Employers must still file a separate Labor Contractor Employee Report that covers workers hired through labor contractors in the prior calendar year. Employers only submit one report that covers labor contractor workers at all of an employer's establishments.

Mean and Median Hourly Rate
Employers are also required to calculate and report the mean and median hourly rate of its payroll employees and/or labor contractor employees, by establishment, pay band, job category, race/ethnicity, and sex. Employers should calculate each employee's individual hourly rate before calculating the mean and median hourly rates. The mean hourly rate is calculated by adding the individual hourly rates for each employee in the group, then dividing that sum by the number of employees in the group. The median hourly rate is calculated by ordering the hourly wages of each employee in the group from smallest to largest and selecting the middle number.

Penalties For Failing to Report
The penalties for employers that fail to file a required report can reach $100 per employee and increase to $200 per employee for a subsequent failure to file a required report. These penalties are also assessable against a labor contractor that failed to provide required pay data to a client employer in a timely fashion. The CRD is also entitled to recover its costs in any enforcement action against an employer.

Employers may wish to review the California Pay Data Reporting: Frequently Asked Questions prior to reporting [link to https://calcivilrights.ca.gov/paydatareporting/faqs/
CLICK HERE.

New Legislation Affecting Criminal Background Screening In Pennsylvania

Pennsylvania and Philadelphia have implemented changes that impact employer practices regarding criminal background screening. House Bill Number 689 (HB 689), enacted on December 14, 2023, and effective as of February 12, 2024, introduced amendments to Pennsylvania law concerning the expungement of specific criminal record information and addresses employer immunity when hiring individuals with expunged records. Meanwhile, changes to Philadelphia's ban-the-box law expand the scope of criminal offenses that employers can consider.

Under Pennsylvania HB 689, employers are granted immunity from liability for claims associated with the effects of expunged records or the lawful utilization of criminal record history information if an applicant voluntarily discloses an expunged conviction. This provision aims to clarify potential ambiguities under existing state law regarding an employer's liability for negligent hiring when hiring an individual with an expunged criminal record who subsequently engages in misconduct.

Furthermore, the legislation extends the scope of automatic expungements to include pardoned cases. The law mandates the Pennsylvania Board of Pardons to notify the Administrative Office of Pennsylvania Courts (AOPC) quarterly of any pardons granted, prompting the AOPC to direct the relevant Court of Common Pleas to expunge the corresponding records. Private entities cannot utilize expunged criminal history record information for employment, housing, or school purposes except as required by federal law.
CLICK HERE.

COURT CASES

A Disparate Impact on a Protected Group Is Not Always Illegal

One form of discrimination is where a policy or job requirement has a disparate (i.e. negative) impact on a protected group. However, that impact is not necessarily illegal under Title VII where there is a legitimate need for the policy or requirement, as the U.S. Court of Appeals for the 7th Circuit recently reiterated.

In *Erdman v. City of Madison*, a female firefighter could not pass the City's physical abilities test, and she sued, alleging that the City's test had a disparate impact on women in violation of Title VII, and that the City could have used an alternate test with less of a disparate impact. The 7th Circuit found, however, that the City was able to demonstrate that the alternative test did not serve its unique legitimate needs.

As the 7th Circuit explained, in order to serve an employer's legitimate needs, any alternative hiring practice must be "substantially equally valid," meaning that it "would lead to a workforce that is substantially equally qualified." However, factors such as cost or other burdens imposed by the alternative may also be taken into account in determining if the alternative is "substantially as efficient as the challenged practice in serving the employer's legitimate business goals." In this case, the City argued that its test measured elements that were specifically designed to replicate tasks that its firefighters would be expected to perform with the City's equipment and in light of specific safety concerns. The City also showed that its test screened out applicants that were likely to wash out later in the training process, as it had a higher rate of hiring and retaining female applicants than other fire departments. Based on these showings, the 7th Circuit agreed that the City's test was not illegal.

This case reminds employers that not all job requirements that have a disparate impact are prohibited by Title VII. However, it is critically important that they consider whether there are alternative criteria that could accomplish essentially the same legitimate purpose with less adverse impact on the protected group – and if not, they need to be prepared to articulate why not with objective, factual support.
CLICK HERE.

First Lawsuit Under CA's Fair Chance Act Filed Against Ralph's Grocery Store: A Message for CA Employers to Comply

In December 2023, the California Civil Rights Department ("CRD") filed the first-of-its-kind lawsuit under the California Fair Chance Act ("Act") against Ralphs Grocery Store ("Ralphs") in the Los Angeles County Superior Court.

Background Re: the Act.
The Act (sometimes referred to as the "Ban the Box" law) went into effect in 2018 and aims to combat discrimination and ultimately enhance public safety by reducing undue barriers to employment for people who have been previously involved in the criminal legal system. In passing the Act, the Legislature recognized that *"employment is essential to helping formerly incarcerated people support themselves and their families"* and reduces the likelihood of an individual reoffending. In general, the Act prohibits employers with five or more employees from asking about a job applicant's conviction history before making a conditional job offer of employment; requires specific procedures for considering an applicant's criminal history after a conditional job offer is made; and limits the types of convictions an employer can consider to disqualify an individual – namely only those convictions that have a direct adverse relationship to the job responsibilities of the position applied for.

Allegations Against Ralphs.
The CRD alleges that Ralphs has ignored and continues to ignore the Act's requirements, including by screening out otherwise qualified applicants on the basis of criminal histories that do not have any adverse relationship with the duties of the job for which they were applying. The CRD claims that Ralphs repeatedly violated the Act's procedural and substantive requirements and has done so since the law's enactment. The CRD says that it obtained information during its investigation that indicates that multiple candidates lost their job offers based on convictions for a single misdemeanor count of excessive noise, and others were disqualified based on convictions from other states for simple cannabis possession. According to the CRD, these types of convictions, and hundreds more, have no adverse relationship

with the duties of working at a grocery store and were not legitimate grounds for withdrawing a conditional offer of employment. As part of the lawsuit, CRD is seeking monetary damages for the individuals who were denied jobs or lost jobs as a result of Ralphs' screening practices, and a court order to require Ralphs to come into compliance with the Act.

CRD's Other Enforcement Action.
In its announcement of the lawsuit against Ralphs (which can be obtained here), the CRD outlines other enforcement efforts it has taken since the Act went into effect in 2018. The CRD says it has investigated hundreds of complaints alleging discrimination in employment based on criminal history information, and has secured approximately 70 settlements on behalf of affected individuals.

Takeaway.
The CRD has made enforcement of the Act a priority and covered employers are advised to review their hiring policies and practices, and train their hiring managers, to ensure compliance with the Act.
CLICK HERE.

INTERNATIONAL DEVELOPMENTS

Review of international data flows: EU reports on adequacy decisions

The European Commission recently conducted a comprehensive review of the adequacy decisions granted to 11 countries or territories prior to the implementation of the General Data Protection Regulation (GDPR). This post provides an analysis and commentary on the findings of the review.

The digitisation of society and globalisation have led to an exponential increase in international data flows. To ensure the protection of individuals' rights in personal data, the EU's GDPR requires that transfers to third countries guarantee an equivalent level of protection. Adequacy decisions, granted by the European Commission, enable the free flow of personal data from the EU to countries that meet the required level of protection.

- **Scope of the review**: The review focused on developments in both the EU data protection regime and the data protection frameworks of the relevant countries and territories since the adoption of the adequacy decisions. The Commission assessed legislative and regulatory reforms, enforcement practices, case law, and changes in the data protection landscape of each country.
- **Findings**: The review found that each of the 11 countries or territories remained compliant and provided an adequate level of protection in line with the EU's evolving data protection framework. In most cases, there was further convergence with the EU's framework regarding government access to personal data and related oversight and redress mechanisms. Several countries, such as Israel and Uruguay, adopted new privacy rules, while others clarified existing privacy rules based on enforcement practice or case law.
- **Future monitoring**: While the review had positive outcomes, the Commission emphasised that adequacy decisions are not an endpoint, but a mechanism for ongoing dialogue and cooperation on data flows and digital matters. The Commission will continue to monitor developments in the protection frameworks and actual practice of the in-scope jurisdictions.

The review reaffirms that the free flow of personal data from the EU to the 11 countries or territories with adequacy decisions remains adequately protected. However, it is important to note that adequacy decisions require regular review, and organizations should stay informed about any updates or changes in the data protection landscape.
CLICK HERE.

Canada's PIPEDA remains "adequate" under the GDPR: what it means for business

On January 15th, the European Commission (the "**Commission**") published its decision (the "**Decision**") relating to the adequacy of the data protection offered by 11 countries.[1] The Commission upheld its prior adequacy decisions, which were adopted under the *Data Protection Directive* (Directive 95/46/EC), the *General Data Protection Regulation*'s ("GDPR") predecessor. As part of the decision, it was announced that Canada's *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") continues to benefit from its adequacy status under the GDPR.

What does this mean for organizations doing business in Canada?
At a high level, this means that personal information can continue to flow into Canada from European countries subject to the GDPR without the need for other data protection mechanisms. However, it is not quite that simple.
Organizations that, for their own purposes or on behalf of their customers (i.e. service providers):

1. Collect the personal information of individuals in the EU, as part of the offering of the businesses' goods or services; or
2. Are located in the EU and collect personal information, even if the processing of personal information is not within the EU,

can keep transferring personal information to Canada, without needing additional protections such as standard contractual clauses, ***as long as the recipient of the personal information is subject to PIPEDA***.

This last point is important and often overlooked. The recipient organization in Canada must be subject to PIPEDA. This means that since private sector employee information is not covered by PIPEDA, businesses which are transferring their employee personal information to recipient organizations in Canada will need additional data protection mechanism (such as standard contractual clauses).

Examples of transfers of personal information could include:

- sending personal information to a service provider with storage facilities in Canada;
- a Canadian company collecting personal information from EU customers in order to fulfill their orders; or
- transferring personal information collected in the EU to a parent company located in Canada.

Organizations must remember that any onward transfer of that personal information to another jurisdiction must be assessed according to that jurisdiction's status. For example, if an organization in Canada receives the personal information from the EU and transfers it to one of its service providers in the US, the organization must consider the adequacy standard of Canada and the protections it can implement for the transfer to the US (given only companies participating in the EU – US Data Privacy Framework have adequacy status).

Commercially, the adequacy decision is welcomed by businesses as it preserves and further encourages Canada's trade relationships with the EU, however, the Commission's decision may have other less obvious implications for Canada's privacy regime (discussed further below).

What is adequacy and why does it matter?
Article 45 of the GDPR requires that transfers of personal data to another jurisdiction can take place, without any specific authorisation, where the Commission has given that jurisdiction "adequacy status", in other words, has decided that the jurisdiction's data protection regime ensures an adequate level of protection for personal data.

Canada's adequacy status allows organizations to receive personal information governed by the GDPR without additional data protection measures such as standard contractual clauses, which are a set of standardised and pre-approved clauses that are incorporated into organizations' contractual arrangements with other parties. These clauses often require that parties comply with a standard of privacy protection that is higher than what is required by legislation in those jurisdictions, which can be considered as a disadvantage during commercial negotiations.

Why is adequacy being evaluated now?
Under Articles 45(4) and 97 of the GDPR, there is a requirement for the Commission to reassess its adequacy rulings on an on-going basis, every four years, to determine if the countries continue to provide an adequate level of protection. Canada's previous adequacy finding was issued in 2001.[2] The delay was caused in part by a requirement for the Commission to consider the implication of the Schrems II case, in which the Commission clarified the key elements to consider in the adequacy test.[3]

What is considered as part of the "adequacy" finding from the Commission?
Article 45 and Recital 104 of the GDPR list the criteria considered as part of adequacy decisions, and specifically note that these criteria are assessed with special consideration of "the fundamental values on which the Union is founded, in particular the protection of human rights". These criteria include:

- how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defense and national security as well as public order and criminal law, and the access of public authorities to personal data;
- the implementation of legislation mentioned above, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another jurisdiction;
- case law;
- whether there are effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects;
- whether there is an effective functioning of one or more independent supervisory authorities, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the EU member states;
- the international commitments the jurisdiction has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data;

- whether the jurisdiction guarantees ensuring an adequate level of protection essentially equivalent (as opposed to requiring "equivalent" protection) to that ensured within the EU, in particular where personal data is processed in one or several specific sectors.

In its Decision, the Commission assessed, in relation to Canada:

- developments in the data protection frameworks since the adoption of the previous adequacy decision, particularly amendments to PIPEDA since 2001 (e.g., valid consent and breach notification), and the ongoing PIPEDA modernization efforts under Bill C-27 (discussed below);
- PIPEDA's scope of application, noting in particular exemptions from the law, and the provincial and sectoral legislation that are considered as "substantially similar" to PIPEDA;
- The Office of the Privacy Commissioner of Canada's non-binding guidance (e.g., updates to the definition of sensitive information);
- The Office of the Privacy Commissioner of Canada's non-binding case summaries (on a variety of topics – e.g., right to deletion, international transfers of personal information);
- Oversight and redress available; and
- the rules in place relating to government access to personal information for law enforcement and national security purposes (e.g. constitutional considerations such as those under the *Canadian Charter of Rights and Freedoms*, *Privacy Act* considerations).

Impact of adequacy on substantially similar provincial legislation

Under Canada's regime, the private sector privacy statutes in Quebec, Alberta and British Columbia have been deemed "substantially similar" to PIPEDA, and therefore those laws apply instead of PIPEDA for processing of personal information that takes place within the provinces. However, the substantially similar privacy laws have not received adequacy status.[4] Interestingly, the Commission's decision indicates that "personal data transferred from the EU/EEA under the adequacy decision are considered cross-border data transfers, which are subject to PIPEDA".[5] This is a curious assertion by the EU. PIPEDA is silent on the application of the law to cross-border flows of information. The CPPA, if passed, would update the application section to clarify that the CPPA applies in respect of personal information that is collected, used or disclosed interprovincially or internationally by an organization (s. 6(2)(a)), however the CPPA is not yet in force. The OPC's non-binding *guidance* materials suggest that "all businesses that operate in Canada and handle personal information that crosses provincial or national borders are subject to PIPEDA regardless of which province or territory they are based in."[6] Provincial privacy commissioners may take a different stance. In fact, guidance from the Quebec Privacy Regulator asserts that organizations located outside of Quebec that collect personal information as part of business in Quebec are subject to the provincial law.[7]

Impacts on Canadian privacy legislation development

The decision comes at a time when the government is advancing Bill C-27, *the Digital Charter Implementation Act*, legislative reform that would update and replace PIPEDA.[8] Regulators, industry, and privacy advocates alike have long claimed that Canada's privacy laws have fallen behind, with the EU's GDPR being the cited as the gold standard. Accordingly, adequacy has been a driving force for PIPEDA's modernization. Unfortunately, PIPEDA's renewed adequacy status may result in de-prioritization of Bill C-27 (the government determines the prioritization of Bills in the House). Likely to avoid de-railing Canada's reform efforts, the European Commission explicitly called for Canada to continue to advance Bill C-27:

At the same time, the Commission recommends enshrining some of the protections that have been developed at sub-legislative level in legislation to enhance legal certainty and consolidate these requirements. The ongoing legislative reform of PIPEDA could notably offer an opportunity to codify such developments, and thereby further strengthen the Canadian privacy framework. The Commission will closely monitor future developments in this area.

Update on the Status of Bill C-27

The Commission's decision casts a spotlight on PIPEDA's reform, which provides a welcome opportunity to share an update on the status of Bill C-27. Bill C-27 was introduced and progressed through first reading on June 16, 2022. During second reading the Bill was discussed in the House of Commons on six occasions before being referred to the Standing Committee on Industry and Technology on April 24, 2023. There have been fifteen committee meetings to date, and more than 74 Privacy and AI expert witnesses have provided testimony to the Committee.

CLICK HERE.

The Norwegian Data Protection Authority is updating the strategy for data and risk-based work

The Danish Data Protection Authority has updated its strategy for the data and risk-based work of the Danish Data Protection Authority, which was first launched in 2020. As something new, the strategy also focuses on progress in supervisory cases. The updated strategy contains 12 new initiatives that in different ways must strengthen the supervisory authority's ability to target the control to the areas where there is the greatest risk to citizens' data.

"In the Danish Data Protection Authority's first strategy for a data- and risk-based effort, we focused on identifying and improving relevant data sources, testing new methods and establishing new proceedings. In the coming three years, we will focus on incorporating and optimizing the new methods and processes in the work for a more targeted control," says Cristina Angela Gulisano, director of the Norwegian Data Protection Authority.

In the updated strategy, there is continued focus on strengthening the authority's data quality, data sources, data use and documentation. At the same time, the strategy also includes a new strategic effort: **Progress in supervisory cases.** With 'supervision cases', we refer to the control activities that the Danish Data Protection Authority itself initiates annually.
"Focusing on progress in supervisory cases is crucial to maintaining momentum and legitimacy in supervisory efforts. It also ensures that the data we use in our data and risk-based efforts remain current and relevant for effective targeted control," concludes Cristina Angela Gulisano, director of the Norwegian Data Protection Authority.
CLICK HERE.

MISCELLEANOUS DEVELOPMENTS

U.S. Privacy Law Outlook: What's on the Horizon in 2024

Following an eventful 2023, we expect that many recent legislative and enforcement trends will persist, making 2024 a similarly impactful year in the development of U.S. privacy law. These trends include but are not limited to, the proliferation of comprehensive state privacy laws based on the Virginia Consumer Data Protection Act (VCDPA), increased regulatory scrutiny for businesses engaged in the processing of sensitive personal information, stalled efforts to adopt a comprehensive federal privacy law and increased federal privacy enforcement under existing sectoral privacy laws.

In addition to preparing for upcoming compliance deadlines, businesses are bracing themselves for new legislation and increased levels of regulatory enforcement at the state and federal levels. In this article, we provide an overview of recent privacy trends and provide a glimpse of what to expect in 2024.

State Activity

Legislative Activity
As of Jan. 30, 2024, fourteen U.S. states have enacted comprehensive state-level privacy laws. Of these fourteen laws, five are currently in effect: California, Connecticut, Colorado, Virginia and Utah. Laws in Montana, Oregon and Texas come into effect in 2024; laws in New Jersey, Tennessee, Iowa, Indiana and Delaware come into effect in 2025; and Indiana takes effect in 2026. More states are expected to adopt laws as legislative momentum for this trend appears to be growing at the state-level with nine states enacting privacy laws since the start of 2023 and several others, including North Carolina, having considered bills that are likely to be brought back in similar forms in future years.

Noteworthy State Privacy Laws
All three of the comprehensive state privacy laws coming into effect this year are based on the VCDPA.

The TDPSA will come into effect on July 1, 2024, and will be enforced exclusively by the Texas Attorney General. Notably, unlike the privacy laws in Colorado and Connecticut, the TDPSA includes a right to cure that does not sunset. In the near term, the TDPSA's novel approach to scoping and other substantive requirements must be evaluated by businesses to ensure compliance ahead of this summer's deadline.

The OCPA was signed into law on July 18, 2023, and goes into effect on July 1, 2024. The OCPA's definition of personal data is unique from other state privacy laws, as it encompasses data that is "derived" from an Oregon resident's personal data. Another unique element of the OCPA is the law's definition of "sensitive data," which extends to transgender or nonbinary status and victim status. The OCPA's Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) exemptions closely mirror the California Consumer Privacy Act (CCPA), in that they narrowly exempt covered data rather than covered entities.

The MCDPA was signed into law on May 19, 2023, and goes into effect on Oct. 1, 2024. Of the three enacted state privacy laws set to come into effect this year, the MCDPA conforms most closely to the VCDPA model. The MCDPA does include a right to cure; however, this right sunsets on April 1, 2026.

In addition to the aforementioned laws, noteworthy non-comprehensive privacy laws targeting specific types of data and/or data subjects will take effect in Florida, Washington and Nevada this year.

The MHMDA was signed into law on April 27, 2023, and will take effect on March 31, 2024. Many of the MHMDA's substantive requirements are somewhat similar to the aforementioned comprehensive state laws. For example, the MHMDA requires that businesses offer data subject rights and provide certain disclosures about their processing activities.

The MHMDA applies to "Consumer Health Data" which is defined as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status." In

practice, this definition encompasses data attributes that are not considered health data under other laws. For example, in some circumstances the MHMDA's definition of Consumer Health Data extends to online browsing history data and geolocation information. In the absence of an "established necessity," Consumer Health Data may only be processed with the consumer's consent.

The MHMDA applies broadly to entities that (a) conduct business in Washington or provide products or services targeting Washington consumers; and (b) alone or jointly with others, determine the purpose and means of processing consumer health data. The MHMDA includes a three-month enforcement delay for "Small Businesses" that fall below certain processing thresholds.

Violations of the MHMDA may be enforced as deceptive and/or unfair acts under Washington's existing Consumer Protection Act (CPA). In addition to AG enforcement, the CPA includes a private right of action, by which consumers have the ability to seek injunctive relief, actual damages, and treble damages (capped at $25,000). While the substantive requirements are noteworthy, the MHMDA's broad definition of Consumer Health Data and private right of action could make it one of the most impactful privacy laws in the United States.

The Nevada Consumer Health Data Privacy Law is based on Washington's MHMDA, and will come into effect on the same day. It is worth noting that the Nevada Consumer Health Data Privacy Law does not include a private right action.
On July 1, 2024, the Florida Digital Bill of Rights will take effect. The scope of this law is limited in comparison to the aforementioned comprehensive privacy laws, as many of the FDBR's requirements only apply to businesses that have an annual global revenue greater than $1 billion. Pursuant to this law, covered businesses will be required to provide consumers the ability to opt out of having their data collected through the use of voice recognition or facial recognition features. The FDBR also includes specific requirements aimed at online platforms providing services, games, or products targeted towards children.

Existing State Privacy Law Developments
This year will mark six years since the adoption of the CCPA and the fourth year of enforcement. Despite the CCPA's "old age," upcoming effective dates, new rulemakings, and growing enforcement activity should keep California top of mind for businesses in 2024.

On March 29, 2024, the final CCPA regulations will come into effect. These regulations implement the California Privacy Rights Act (CPRA) requirements. In the meantime, the amended sections of the CCPA statutory text and the corresponding 2020 regulations continue to apply. The aforementioned final regulations will be supplemented by additional waves of issue-specific regulations published by the California Privacy Protection Agency (CPPA).

The most recent round of proposed regulations were published by the CPPA on Dec. 1, 2023. Noteworthy developments in these proposed regulations include:

- *Mobile Privacy Policies*: The proposed regulations require that mobile application privacy policies be posted on an application's setting pages. Currently, posting the policy on an application's download platform is sufficient (*e.g.*, Apple App Store or Google Play Store).
- *Definition of Sensitive Information*: In addition to the existing sensitive data attributes, the proposed regulations would extend the definition of sensitive personal information to include all personal information of consumers under the age of 16.
- *Right to File Complaint*: Following the denial of a data subject request, the proposed regulations would require businesses to notify consumers of their right to file a complaint.

Thus far, the CPPA enforcement activity has been limited in scope. This activity will likely increase after the final regulations take effect on March 29. California's Attorney General also has the authority to enforce the CCPA and in 2023, brought multiple privacy-related enforcement actions under California's Unfair Competition Law. This included an enforcement action against Google in which the AG claimed that "Google misled users into believing they had control over Google's collection and use of their location data." It is worth noting that the CCPA's "right-to-cure" provision sunset on Jan. 1, 2023.

In other states, we expect that the scope and impact of enforcement will expand significantly over the next few years. This expansion can be attributed to the increased number of laws as well as the development of state-level enforcement

resources and expertise. The risks of enforcement will also become more significant as the "right-to-cure" provisions will have sunset in four states by the end of next year. We also expect that states may coordinate with one another and the Federal Trade Commission (FTC) when carrying out enforcement.

Federal Activity

Federal Legislation

The growing number of comprehensive state privacy laws has long been viewed as a possible catalyst for federal privacy legislation. While numerous federal bills have been introduced, to date, the bipartisan American Data Privacy and Protection Act (ADPPA) has achieved the most traction. The ADPPA was first introduced in 2022, and was passed with a unanimous vote by the House Energy and Commerce Committee on Oct. 16, 2023. There is speculation that this legislation may be updated by Rep. Cathy McMorris Rodgers, the chair of the House Energy and Commerce Committee, to include new provisions addressing legal issues associated with advanced artificial intelligence (AI) technology. Given the current societal focus on AI, addressing both privacy and AI in one bill may be the most propitious path forward for federal privacy legislation. That being said, broader political gridlock and this year's elections will serve as major headwinds for all federal legislation.

FTC Enforcement

In 2023, the FTC brought multiple enforcement actions related to the mishandling of sensitive health information. For example, last February the FTC alleged that GoodRx Holdings, Inc. violated Section 5 of the FTC Act by deceiving customers about their data sharing practices with advertisers and other third parties. The FTC also alleged that GoodRx's third-party disclosures constituted violations of the HIPAA Health Breach Notification Rule (HBNR). This case represented the first time that the FTC has enforced the HBNR.

Another recent point of emphasis for the FTC has been enforcement of the Children's Online Privacy Protection Act (COPPA). On July 21, 2023, the FTC and Department of Justice filed a lawsuit against Amazon for allegedly deceiving parents and users about the deletion/retention of Alexa audio data. The FTC and Microsoft also announced a settlement last year related to COPPA consent violations on Xbox gaming systems. As discussed below, the FTC is in the process of issuing updated COPPA regulations.

Federal Rulemaking Developments

On Dec. 20, 2023, the FTC issued a Notice of Proposed Rulemaking on proposed changes to COPPA. Specifically, the proposed rulemaking would (i) require a separate opt-in consent for targeted advertising, (ii) prohibit using personal information disclosures as a precondition for use/participation, (iii) institute new limits on data retention, and (iv) bolster the FTC's COPPA data security requirements. The FTC's proposed changes also include a broader definition of "Personal Information," which would include "biometric identifier[s]that can be used for the automated or semi-automated recognition of an individual." Comments on this proposed rulemaking may be submitted through March 11, 2024.

On Oct. 27, 2023, the FTC adopted amendments to the GLBA Safeguards Rule breach notification requirements. Pursuant to the amendments, non-banking financial institutions will be required to notify the FTC within 30 days of discovering a data breach involving the nonpublic personal information of at least 500 consumers. Prior to this amendment covered entities were required to implement security requirements; however, there was no specific breach notification requirement. The amendment is set to take effect on May 14, 2024.

The Impact of AI

The recent proliferation of advanced generative AI platforms may be what we remember most about the year 2023. In response to the rapid adoption of AI technology, government authorities at all levels have taken initial steps aimed at addressing the perceived risks associated with AI.

On Oct. 30, 2023, the Biden administration issued an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The 117-page order includes a range of directives, many of which are aimed at promoting the domestic development of AI technologies while also addressing the perceived risks. The order lays the groundwork for further action by requiring federal executive agencies to conduct research studies and implement other measures to prepare for the further proliferation of AI technologies. The order follows prior

government pronouncements concerning the recent proliferation of generative AI technologies. In October 2022, the Office of Science and Technology Policy published the "Blueprint for an AI Bill of Rights," and earlier this year the National Institute of Standards and Technology released the "AI Risk Management Framework."

The FTC's leadership has also indicated that AI regulation will be a major agency focus moving forward. This year the FTC has already published a blog post entitled "AI Companies: Uphold Your Privacy and Confidentiality Commitments" and has announced a Section 6(b) inquiry related to "investments and partnerships being formed between AI developers and major cloud service providers." Last year the FTC adopted a resolution pre-authorizing "compulsory process" for investigations related to AI. This pre-authorization will last for 10 years, and will make it easier for the FTC to issue discovery demands for AI-related investigations.

***

This year is poised to be another eventful one in the evolution of U.S. privacy law. While we expect existing trends will continue; new technologies and election year politics could have a significant and unexpected impact. Moving forward, taking a proactive and flexible approach to privacy compliance is more important than ever.
CLICK HERE.

Trends in AI: U.S. State Legislative Developments

U.S. policymakers have continued to express interest in legislation to regulate artificial intelligence ("AI"), particularly at the state level. Although comprehensive AI bills and frameworks in Congress have received substantial attention, state legislatures also have been moving forward with their own efforts to regulate AI. This blog post summarizes key themes in state AI bills introduced in the past year. Now that new state legislative sessions have commenced, we expect to see even more activity in the months ahead.

- ***Notice Requirements:*** A number of state AI bills focus on notice to individuals. Some bills would require covered entities to notify individuals when using automated decision-making tools for decisions that affect their rights and opportunities, such as the use of AI in employment. For example, the District of Columbia's "Stop Discrimination by Algorithms Act" (B 114) would require a notice about how the covered entity uses personal information in algorithmic eligibility determinations, including providing information about the source of information, and it would require a separate notice to an individual affected by an algorithmic eligibility determination that results in an "adverse action." Similarly, the Massachusetts "Act Preventing a Dystopian Work Environment" (HB 1873) likewise would require employers or vendors using an automated decision system to provide notice to workers prior to adopting the system and would require an additional notice if there are "significant updates or changes" made to the system. Additionally, other AI bills have focused on disclosure requirements between entities in the AI ecosystem. For example, Washington's legislature is considering a bill (HB 1951) that would require developers of automated decision tools to provide documentation of the "known limitations" of the tool, the types of data used to program or train the tool, and how the tool was evaluated for validity to deployers of the tool.
- ***Impact Assessments:*** Another key theme in state AI bills focuses on requirements for impact assessments in the development of AI tools; calls for these assessments aim to mitigate potential discrimination, privacy, and accuracy harms. For example, a Vermont bill (HB 114) would require employers using automated decision-making tools to conduct algorithmic impact assessments prior to using those tools for employment-related decisions. Additionally, the bill mentioned above under consideration in the Washington legislature (HB 1951) would require that deployers complete impact assessments for automated decision tools that include, for example, assessments of reasonably foreseeable risks of algorithmic decision making and the safeguards implemented.
- ***Individual Rights:*** State legislatures also have sought to implement requirements for consumers to exercise certain rights in AI bills. For example, several state AI bills would establish an individual right to opt-out of decisions based on automated decision-making or request a human reevaluation of such decisions. California (AB 331) and New York (AB 7859) are considering bills that would require AI deployers to allow individuals to request "alternative selection processes" where an automated decision tool is being used to make, or is a controlling factor in, a consequential decision. Similarly, New York's AI Bill of Rights (S 8209) would provide individuals with the right to opt-out of the use of automated systems in favor of a human alternative.
- ***Licensing & Registration Regimes:*** A handful of state legislatures have proposed requirements for AI licensing

and registration. For example, New York's Advanced AI Licensing Act (A 8195) would require all developers and operators of certain "high-risk advanced AI systems" to apply for a license from the state before use. Other bills require registration for certain uses of the AI system. For instance, an amendment introduced in the Illinois legislature (HB 1002) would require state certification of diagnostic algorithms used by hospitals.

- ***Generative AI & Content Labeling:*** Another prominent theme in state AI legislation has been a focus on labeling content produced by generative AI systems. For example, Rhode Island is considering a bill (H 6286) that would require a "distinctive watermark" to authenticate generative AI content.

CLICK HERE.

Pre-Hire Personality Tests Set Legal Challenges for Employers

Alston & Bird's Anna Saraie and Martha Doty analyze pre-hire personality testing, including the legal and practical considerations for employers incorporating such testing into their application processes.

Whether employees are a good personality fit within the team, department, and overall culture of a workplace is an important factor in a company's success.

Employers increasingly are requiring applicants to take personality tests as part of the recruiting process. The integration of artificial intelligence tools into personality assessments has both revitalized employer interest in using these tests for recruiting and complicated the legal landscape for their use.

But before using preemployment personality tests, employers should understand the legal and practical considerations of implementing such tests.

Legal Considerations
Employers should be aware that various laws may be implicated by using personality testing at the preemployment stage.

For starters, any preemployment testing must comply with federal anti-discrimination laws, including Title VII of the Civil Rights Act, the Americans with Disabilities Act, and the Age Discrimination in Employment Act. These laws permit certain preemployment testing if it meets statutory requirements and is nondiscriminatory.

Employee selection guidelines codified in 29 C.F.R. 1607.1 in 1978 intended to assist employers in complying with the requirements of federal law that prohibit employers from discriminating against employees based on race, color, religion, sex, and national origin.

Employers aren't strictly bound, but courts weigh the guidelines in assessing the validity of various employment tests. Any validation of preemployment personality testing should be conducted in line with these guidelines.

The Equal Employment Opportunity Commission issued two pieces of technical guidance in the past two years that build on the guidance to specifically address the use of artificial intelligence in hiring tools.

On May 18, 2023, the EEOC issued guidance on the effect of software, algorithms, and artificial intelligence used in employment selection procedures under Title VII of the Civil Rights Act. And on May 12, 2022, the EEOC issued guidance on how an employer's use of software that relies on algorithmic decision-making may violate requirements under Title I of the Americans with Disabilities Act.

The EEOC advises employers using pre-employment testing software with AI or other algorithmic decision-making tools to ensure that they know how the software was developed, as well as evaluation of whether such selection tools causes a substantially lower selection rate for individuals with a characteristic protected by Title VII.

The EEOC advises employers to consider asking the following questions about a pretesting tool when considering ADA requirements:

- If the tool requires applicants or employees to engage a user interface, did the vendor make the interface accessible to as many individuals with disabilities as possible?

- Are the materials presented to job applicants or employees in alternative formats? If so, which formats?
- Are there any kinds of disabilities for which the vendor won't be able to provide accessible formats? If so, the employer may have to provide them.
- Did the vendor attempt to determine whether the use of the algorithm disadvantages individuals with disabilities?

In addition to federal laws, employers should be cognizant of applicable state and local laws, including privacy and bias concerns. For example, New York City Local Law 144, which took effect on Jan. 1, 2023, prohibits employers and employment agencies from using an automated employment decision tool in New York City unless they ensure a bias audit was done and provide required notices.

Personality tests may be subject to this law, and other state and local governments will likely follow suit and adopt similar regulations.

Practical Considerations

Employers wishing to incorporate pre-hire personality testing will need to assess and answer the following practical questions when implementing personality tests:

- What are the company's goals in incorporating the testing in its recruiting processes?
- What personality traits will the company be testing for? Why are these traits important? Is there an alternative method for evaluating these traits?
- Which applicants will be required to take the test? Will the company require all applicants to submit, or will the company require tests for only certain positions? Will the company require tests for applicants regardless of where they're located?
- Will the test use AI tools?
- At what point in the recruitment process will applicants take the test?
- Is the company concerned with recruiting talent? Could requiring pre-hire personality tests discourage candidates from applying?
- Does the company already require other pre-hiring tests, such as drug testing or background checks? If so, would adding the additional test discourage candidates from applying?
- Which personality test will the company use? If so, which format will be used; how will this test measure the personality traits that are important to the company; and has this test been properly validated?
- How will the test results be used by hiring personnel?
- What steps will the company take to ensure tests continue to comply with applicable law, including ensuring that the tests, over time, don't disparately affect a protected group?

Outside Vendors

Employers may use outside vendors to implement pre-employment personality testing. But employers should be vigilant in asking and confirming that any testing complies with the applicable laws, because the EEOC has clearly indicated that employers can be liable for violations of federal anti-discrimination laws even if an outside vendor developed the software.

At a minimum, employers must ensure that the personality testing has been properly validated. Further, employers should ask the vendors to provide the actual test questions and review these questions with employment counsel to ensure the questions don't infringe on an employee's rights under applicable anti-discrimination and privacy laws.
Finally, employers should work with the vendor to monitor and assess test results while the pre-employment personality tests are required. This will ensure the testing doesn't disparately affect a protected class.
CLICK HERE.