JULY 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

TABLE OF CONTENTS

SCREENING COMPLIANCE UPDATE | JULY 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

Significant Improvements for International Transfers of Personal Data - Adequacy Decision for the New EU-U.S. Data Privacy Framework Adopted by the European Commission

On July 10, 2023, the European Commission adopted its long-awaited adequacy decision for the EU-U.S. Data Privacy Framework ("Adequacy Decision"). This ends a three-year journey to set up a successor to the EU-U.S. Privacy Shield mechanism, which the Court of Justice of the European Union ("CJEU") deemed invalid on July 16, 2020. U.S. President Joe Biden welcomed the Adequacy Decision, stating that it "*will provide greater data privacy protections and economic opportunities*."

The Adequacy Decision concludes that the U.S. provides for an adequate level of protection under the EU's General Data Protection Regulation ("GDPR") when personal data of individuals in the European Economic Area ("EEA") is transferred to U.S. companies certified under the new EU-U.S. Data Privacy Framework.
Along with the Adequacy Decision, the European Commission published a fact sheet and a Q&A document.

Background: Changes in U.S. Law

The Adequacy Decision follows certain changes in U.S. law, in particular Executive Order 14086 ("Enhancing Safeguards for United States Signals Intelligence Activities") dated October 7, 2022. The Executive Order and accompanying regulations:

- provide additional safeguards to ensure that U.S. signals intelligence activities are necessary and proportionate to the pursuit of defined national security objectives;
- enhance rigorous oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities; and
- create a new independent redress mechanism for complaints about access to data by U.S. national security authorities with binding authority to direct remedial measures. This new independent redress mechanism set up by the U.S. government has two levels and aims at investigating and resolving complaints from any individual whose data has been transferred from the EEA about the collection and use of their data by U.S. intelligence agencies access to their data by U.S. national security authorities. At a first level, complaints are investigated by the Civil Liberties Protection Officer of the U.S. intelligence community. At the second level, individuals can appeal the decision of the Civil Liberties Protection Officer before the newly established Data Protection Review Court ("DPRC").

The U.S. Attorney General also allowed access to the redress mechanism in Section 3 of Executive Order 14086 by designating the EU and Iceland, Liechtenstein and Norway as "Qualifying States," following an analysis of the legal protections for U.S. data in these countries.

The EU-U.S. Data Privacy Framework is administered by the U.S. Department of Commerce and enforced by the U.S. Federal Trade Commission.

Certification of companies in the U.S. under the EU-U.S. Data Privacy Framework

The Adequacy Decision directly addresses transfers from the EU to recipients in the U.S. who have self-certified under the EU-U.S. Data Privacy Framework. Companies will have to agree to comply with a detailed set of privacy principles ("DPF Principles") such as purpose limitation, data minimization and data retention, as well as specific commitments on data security and sharing with third parties. The Adequacy Decision provides that the DPF Principles apply immediately on certification. Participating organizations are required to recertify their adherence to the DPF Principles on an annual basis.

This certification process can be started immediately, as soon as the framework's website at www.dataprivacyframework.gov is fully operational.

Companies currently registered under the former EU-U.S. Privacy Shield framework are likely to be transferred more or less automatically to the EU-U.S. Data Privacy Framework, although updates to privacy policies and other documents referencing the EU-U.S. Privacy Shield framework should be made in the next three months, but additional details on implementation have not been announced yet.

Indirect effects of the Adequacy Decision on other GDPR transfer mechanisms

According to a Q&A document published by the European Commission on July 10, 2023, all the safeguards implemented under Executive Order 14086 apply to all data transfers from the EEA to companies in the U.S., regardless of the transfer mechanism relied upon in each case. Therefore, these safeguards also facilitate using other tools, such as the Standard Contractual Clauses and Binding Corporate Rules.

In practice, the general obligation to carry out a transfer impact assessment ("TIA") under the Standard Contractual Clauses will remain, but there should not be any doubt regarding the overall result of the assessment in light of the Adequacy Decision.

Upcoming legal challenges of the Adequacy Decision before the CJEU

It is widely expected that the Adequacy Decision will be challenged in court. Austrian activist *Max Schrems*, founder of the privacy organization *noyb*, has already announced such a challenge, aiming at invalidating the new transfer mechanism. There could be a "Schrems III" judgment by the CJEU following *Schrems I* (regarding Safe Harbor) and *Schrems II* (regarding the EU-U.S. Privacy Shield).

The European Commission is confident that the Adequacy Decision will survive a legal challenge. A member of EU Justice Chief *Didier Reynders'* cabinet recently said that the European Commission is convinced that *"this arrangement is stable and meets the requirements of our European Court of Justice."* In the press release on the Adequacy Decision, EU Justice Commissioner *Reynders* explained that "[the Commission] *is very confident to try to, not only implement such an agreement, but also to defend* [it] *in all procedures that* [it will] *have to face."*

Regular reviews

The Adequacy Decision in practice will be subject to regular review. To this end, the European Commission will continuously monitor developments in the U.S. to verify that all relevant elements have been fully implemented in the U.S. legal framework and are working effectively. In the event of developments affecting the "adequacy" of the level of protection in the U.S., the Adequacy Decision may be adapted or even withdrawn by the European Commission. The first periodic review will take place within one year of the entry into force of the Adequacy Decision.

Conclusion

For the time being, companies finally have a robust legal basis for transferring data from the EEA to the U.S. It remains to be seen whether the Adequacy Decision will be invalidated by the CJEU in another potential *Schrems III* decision.

CLICK HERE.

European Commission Adopts EU-U.S. Data Privacy Framework Adequacy Decision

On July 10, 2023, the European Commission adopted an adequacy decision regarding the EU-U.S. Data Privacy Framework (Framework). The adequacy decision procedure was established by the European Union's (EU) General Data Protection Regulation (GDPR) to create a legal mechanism by which to permit the transfer of personal data from the EU to non-EU countries. In essence, an adequacy decision means that the European Commission has determined that a country—in this case the U.S.—offers an adequate level of protection to personal data comparable to that of the EU.

Going forward, U.S. companies that self-certify to the Framework, which will be administered by the U.S. Department of Commerce, will be able to freely transfer personal data to and from the EU. In order to self-certify to the Framework,

U.S. companies will be required to commit to comply with a detailed set of privacy obligations and make the required certifications to the U.S. Department of Commerce. The privacy obligations are expected to include requirements around purpose limitation, data minimization, data retention, as well as specific obligations concerning data security and the sharing of data with third parties. Further, like its predecessor the U.S. Privacy Shield, compliance with these requirements will be enforced by the U.S. Federal Trade Commission.

Although the adequacy decision is now in effect, the European Commission will continuously monitor relevant developments in the U.S. and regularly review the adequacy decision. The first review will take place by July 10, 2024. Now that the adequacy decision has been finalized, the U.S. Department of Commerce will (i) provide information on how U.S. businesses that currently are not covered under the Privacy Shield can self-certify to the new Framework, and (ii) provide guidance to those companies that continued to adhere to the Privacy Shield Principles during the past three years. More information, as well as the certification, can be found on the recently created Data Privacy Framework website, which will likely be fully functional in the coming days.

CLICK HERE.

The FTC Sets Its Sights on Biometric Information

Does your business collect or use fingerprints? Do your building access points use retina, finger, or palm scans? Does your security office use facial recognition technology to identify repeated trespassers? Do your phone systems use voice recognition technology? If you answered yes to any of these questions, your organization collects and uses biometric information. It is also important to think about your business' own products and services, and specifically, whether those products and services collect, use, or rely on biometric information.

These questions are not typically top of mind for legal and compliance teams, however, based on a recent Federal Trade Commission ("FTC") policy statement, they soon should be. The recent policy statement focuses on how use of emerging technologies that use biometric information might harm consumers and violate the FTC Act. The guidance is useful for both business that use biometric technologies in their own products and services, as well as for businesses that use biometric technologies provided by third party vendors.

In its statement, the FTC cites "*The increasing use of consumers' biometric information and related marketing of technologies that use or purport to use biometric information raise significant concerns with respect to consumer privacy, data security, and the potential for bias and discrimination.*" Similarly, Samuel Levine, Director of the FTC's Bureau of Consumer Protection, noted "*In recent years, biometric surveillance has grown more sophisticated and pervasive, posing new threats to privacy and civil rights.*"

Technological advancements in recent years has vastly increased the proliferation of biometric information technologies. If you have had your fingerprints taken, used voice or facial recognition technology, or used DNA ancestry testing, your biometric information was collected. However, your biometric information may also be collected and used in ways that are not always apparent. Many retail stores, airports, and other physical establishments use facial recognition technologies that collect and rely on use of biometric information. The FTC has taken note of all of this, and its recent policy statement may be a shot across the bow.

What is "biometric information?"

The FTC defines "biometric information" as "*data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body.*" This includes, but is not limited to, the following: depictions, images, descriptions, or recordings of an individual's facial features, iris or retina, finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern), as well as data derived from such depictions, images, descriptions, or recordings, to the extent that it would be reasonably possible to identify the person from whose information the data was derived. For example, 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 depicted in the photograph are considered "biometric information."

Current Legal Landscape

Biometric information has been regulated for several years under state law in Illinois, Texas, and Washington. Additionally, biometric information is regulated under general state privacy laws such as the California Consumer Privacy Act. However, there is no federal law that specifically regulates biometric information. The FTC, in its typical fashion as of late, signals that it is willing to fill that perceived gap by utilizing Section 5 of the FTC Act – which broadly prohibits unfair or deceptive acts or practices in or affecting commerce - as a means to regulate biometric information.

Notably, the fines for non-compliance with current state biometric information laws can be quite significant. For example, violation of Illinois' Biometric Information Protection Act (BIPA) carries fines up to $1,000 per violation for negligent violations, and $5,000 for intention or reckless violations. If that was not a deterrent enough, the Illinois Supreme Court in Cothron v. White Castle recently clarified that separate BIPA violations accrue ***each and every*** time an organization scans or transmits an individual's biometric information – which can easily result in astronomical penalties. For example, if a business scans an employee's fingerprint each day in order to allow facility access, ***a separate claim accrues each and every time that the employee's fingerprint is scanned to enter the facility.*** Start doing the math…

And, a recent US Court of Appeals ruling in the Seventh Circuit marked the first time that an appellate court provided a roadmap to insurance carriers regarding policy language that the Court said was too vague to exclude coverage for a policyholder that allegedly violated BIPA. The ruling obligates an insurance carrier to pay an IT vendor's legal bills in two proposed BIPA class actions. The Court's ruling gives carriers a strong message about the type of specificity courts expect to see in policy language if the carriers want to exclude coverage for BIPA. If your company potentially has BIPA exposure, read your policy carefully (or contact our Mintz experts to assist).

How Biometric Technologies intersect with The FTC Act

The policy statement includes a non-exhaustive list of examples of practices that the FTC will scrutinize in determining whether companies that collect and use biometric information are comply with Section 5 of the FTC Act.

Deceptive Practices

The policy statement draws attention to "false or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information." The FTC specifically warns against making claims without a reasonable basis, including claims that biometric technologies will deliver particular results or outcomes.

The FTC notes that false or misleading statements about the collection and use of biometric information constitute deceptive acts in violation of Section 5 of the FTC Act, as does failing to disclose any material information needed to make a representation non-misleading. Additionally, the policy statement guides businesses not to make false statements about the extent to which they collect or use biometric information or whether or how they implement technologies using biometric information.

Unfair Acts

The policy statement makes clear that the use of biometric information or biometric information technology may be an unfair practice within the meaning of the FTC Act.

The FTC draws upon its previous enforcement actions, noting that "collecting, retaining, or using consumers' personal information in ways that cause or are likely to cause substantial injury, or disseminating technology that enables others to do so without taking reasonable measures to prevent harm to consumers can be an unfair practice in violation of Section 5 of the FTC Act."

How to Avoid Liability under the FTC Act

Reasonable Privacy and Information Security

According to the policy statement, "in order to avoid liability under the FTC Act, businesses should implement reasonable privacy and data security measures to ensure that any biometric information that they collect or maintain is protected from unauthorized access."

Factors in the FTC's Assessment

The FTC notes that determining whether a business's use of biometric information or biometric information technology violates Section 5 "requires a holistic assessment of the business's relevant practices."
There are several factors that the FTC will use in its analysis (though the list is not exhaustive) of whether a business is violating Section 5 in connection with its use of biometric technologies:

- ***Failing to assess foreseeable harms to consumers before collecting biometric information*** - (Prior to collecting biometric information or using biometric information technology, businesses should conduct a holistic assessment of the potential risks to consumers)
- ***Failing to promptly address known or foreseeable risks*** – (this includes failing to identify and implement readily available tools for reducing or eliminating risks)
- ***Engaging in surreptitious and unexpected collection or use of biometric information.*** (In some situations, use of biometric technologies may be unfair in and of itself, such as, for example, using biometric technology to surreptitiously identify or track a consumer in a manner that exposes the consumer to risks such as stalking, exposure to stigma, reputational harm, or extreme emotional distress)
- ***Failing to evaluate the practices and capabilities of third parties*** - (this includes due diligence, assurances, contractual obligations, and ongoing oversight to ensure that third parties, including affiliates and vendors, that will have access to biometric information or will use biometric technologies are meeting appropriate requirements)
- ***Failing to provide appropriate training for employees and contractors*** – (this includes all personnel that interact with biometric information or related technologies)
- ***Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale, or use in connection with biometric information*** (this is meant 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)

A Bridge Too Far

According to the FTC, in some situations, the adoption of a contemplated practice that uses biometric information may be unjustifiable when weighing the potential risks to consumers against the anticipated benefits of the practice. For example, if more accurate, less risky alternatives are available, using a technology that is proven to have high error rates may present an unjustifiable risk to consumers, even if the technology is more convenient, more efficient, or more profitable for the business considering implementing the technology.

Takeaways

Do you know whether your organization collects or uses biometric information, or more directly, does your company's products or services collect, use, or rely on biometric information? Now is a good time to find out. As organizations grow, it is quite common for technology to roll out across various departments that is not always flagged as carrying privacy or data protection risks, and this can easily include biometric information technology. Also, keep your third party vendors and service providers in mind when conducting this review, as they may be collecting or using biometric information as part of the products and services that they are providing to your organization – and your organization may be on the hook for it.

CLICK HERE.

The U.S. Equal Employment Opportunity Commission Has Confirmed That Employers Face Potential Liability If They Use AI Tools To Screen Applicants. Employers Should Listen.

The U.S. Equal Employment Opportunity Commission ("EEOC") has released guidance confirming that employers face potential liability if they use AI tools to screen applicants in a way that disproportionately impacts employees on the

basis of a protected class such as race, color, religion, sex, or national origin.

While ChatGPT and its competitors are new, the legal framework used to assess other applicant screening tools has been around for quite some time. Employers and the legal system have struggled for years over whether and to what extent employers should be allowed to take a person's credit scores or even their criminal record into account when making hiring decisions. Indeed, the system by which a person's credit score is calculated is via an algorithm which is applied to large body of data to make predictions about a person's future behavior. There is a well-developed body of case law addressing situations where facially neutral hiring criteria end up having a disparate negative impact upon particular group of historically marginalized people. This so called "disparate impact" analysis requires that employers show that their facially neutral hiring criteria are job related and consistent with business necessity if those hiring criteria disproportionally disadvantage individuals of a particular race, sex, national origin, or other legally protected class.

As the EEOC has confirmed, this disparate impact analysis definitively applies to employers' use of AI in the hiring process. Employers may not use AI to select applicants in way that adversely impacts individuals on the basis of race, sex, national origin, or other legally protected classes unless the selection criteria are "job related for the position in question and consistent with business necessity." For example, screening on the basis of physical strength would not be allowed for an office job where physical strength is not necessary because such a requirement would disproportionately exclude female applicants and not be job related. Similarly, Employers cannot use AI in a way that adversely impacts a protected class, without also showing that they are selecting for job related criteria.

The conventional wisdom is that it would be hard to sue an employer for using AI, which was not explicitly programmed to exclude members of a protected class, when making hiring decisions. While a plaintiff might be able to show that an algorithm is disproportionately disadvantaging people of a certain race, gender, or other protected class, the employer has a legal defense if the employer can show that the selection criteria are job related and consistent with business necessity. In other words, even if the algorithm is disproportionately screening out people in a certain protected class, if the algorithm is selecting for goals such as decreased turnover or high sales potential, the law favors the employer. Since any selection algorithm anyone would use would almost always be programmed to select for traits or capabilities that are job related and consistent with business necessity, such as skill at sales, low likelihood of turnover, etc., the employer will prevail.

There is a further step in the legal analysis, however, that is going to increasingly come into play as the potential for bias with such algorithms becomes better understood. Even if a defendant can show that their selection criteria are job related and consistent with business necessity, a plaintiff can still prevail by showing that the employer could have used different selection criteria that creates less of a disadvantage for minority applicants, but still achieves the employer's job-related selection goals. Indeed, the EEOC addresses this very point in its most recent guidance, explaining that failure to adopt a less discriminatory algorithm may give rise to liability. As tools that have been vetted for bias on the basis of race, gender, and national origin become available, and as those tools are proven to be at least as effective as other tools that have not been vetted for bias, employers will be obligated to select the vetted tools, or face potential liability.

In the meantime, employers should avoid using unvetted AI tools to make important screening or hiring decisions that could improperly impact applicants on the basis of protected classes such as race or sex. Regulatory bodies such as the Equal Employment Opportunity Commission have already begun the process of regulating AI hiring tools. Just as several states have banned or limited the use of credit scores when making hiring decisions, agencies and legislatures will likely begin to pass legislation and adopt rules for how and when AI tools may be used how they ought to be vetted. Until the legal dust settles, employers would be wise to exercise caution.

CLICK HERE.

August 1st – New Form I-9 Version and Permanent Option for Remote Verification of Employees for Employers Using E-Verify

On August 1st, United States Citizenship and Immigration Services (USCIS) will publish the new Form I-9 for employers to use to confirm a new employee's authorization to work in the United States. Employers are encouraged to begin using the new form on August 1st for all new hires, but may use the current form (version 10/21/19) through

October 31st. Starting November 1, only the new Form I-9 may be used for newly hired employees and reverifications. The new Form I-9 will be a single page and will include a checkbox for employers to indicate they examined Form I-9 documentation remotely under a new Department of Homeland Security (DHS)-authorized alternative procedure (see further information below). USCIS is moving the Preparer/Translator Certification and the Reverification/Rehire sections to stand alone documents. Thus, if either of those situations apply, employers must complete a separate document and maintain it with the Form I-9.

E-Verify Employers

Additionally, DHS has issued a final rule which provides an alternative to the in-person physical review of an employee's Form I-9 documents. E-Verify participants will be allowed to remotely verify any new employee's Form I-9 work authorization document(s) hired at an E-Verify hiring site. This alternative can only be utilized by E-Verify employers in good standing at their E-Verify participating hiring sites. Employers utilizing this "remote verification" option must retain clear and legible copies of all documents presented by the employee which establish identity and work authorization.

Practically, the "remote verification" will first require the employee to submit copies of their Form I-9 work authorization document(s) (front and back) to the employer. Then the employee must participate in a live video interaction (i.e. zoom, facetime call, etc.) with the employer where the employer can examine the documents "live" and see the employee to ensure the documents reasonably relate to the employee. Next, the employer will complete Section 2 of the Form I-9 indicating that they utilized the alternative verification procedure. Finally, the employer must then complete E-Verify for the employee. This process (Form I-9 completions and E-Verify completion) must be done within three (3) business days of the employee's first day of work for pay.

In addition, this new rule has an additional benefit for E-Verify employers regarding their remote working authorization verifications during COVID-19. DHS is allowing employers who are in good standing, participated in E-Verify between March 20, 2020 and July 31, 2023 and utilized it to verify new hires, to use this new alternative to comply with their "in-person" verification requirements that must be met by August 30th. Such employers will not complete E-Verify again for this COVID reverification process.

Employers should take this opportunity to review their Form I-9 compliance procedures, record retention procedures and policies and ensure they are prepared to comply with the new Form I-9.

CLICK HERE.

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

Hawaii Enacts Pay Transparency Law and Expands Equal Pay Law

Seyfarth Synopsis: On July 3, 2023, Hawaii Governor Josh Green signed into law a pay transparency bill that will require employers to disclose in job listings an hourly rate or salary range that reasonably reflects the actual expected compensation for the job. The bill will also expand Hawaii's equal pay law to (1) prohibit pay discrimination based on *any protected category* under Hawaii law, not just sex; and (2) compare employees who are performing "substantially similar work," rather than "equal work." The law will become effective January 1, 2024.

Required Pay Disclosure in Job Listings

Hawaii has become the latest jurisdiction to enact a law that will require pay transparency in job postings. Effective January 1, 2024, Hawaii employers with fifty or more employees will be required to disclose in job listings an hourly rate or salary range that reasonably reflects the actual expected compensation for the role. The law does not define "hourly rate" or "salary range."

Employers should note, the Hawaii law will not require employers to disclose pay information in job listings for positions that are internal transfers or promotions within the company. This is a departure from several other jurisdictions' pay transparency laws, which require internal job postings to follow the same pay transparency requirements as external job postings.

The law also explicitly excludes job listings for positions with employers that have fewer than fifty employees and for public employee positions for which salary, benefits or other compensation are determined pursuant to collective bargaining. The law does not specify whether the fifty employee threshold refers to employees within Hawaii or to a company's total employee count.

Expansion of Equal Pay Law

The newly signed bill will also amend Hawaii's equal pay law in two ways.

First, the law will now prohibit pay discrimination based on *any protected category* under Hawaii law, not just sex. Accordingly, employees may now bring claims of discrimination in pay based on race, sex including gender identity or expression, sexual orientation, age, religion, color, ancestry, disability, marital status, arrest and court record, reproductive health decision, or domestic or sexual violence victim status.

Second, the law adopts a different standard for comparing employees. Hawaii's equal pay law previously tracked the federal Equal Pay Act's "equal work" standard and required an employee to establish that they were paid less than another employee for "equal work on jobs the performance of which requires equal skill, effort, and responsibility, and that are performed under similar working conditions." This "equal work" standard has now been replaced with a "substantially similar work" standard such that employees may now be compared if they are performing "substantially similar work." This tracks recent development in several other jurisdictions, like California and New York, that have adopted this "substantially similar work" standard.

Enforcement and Potential Remedies

While the newly enacted bill does not contain separate provisions on enforcement or remedies, Hawaii law generally allows individuals claiming to be aggrieved by an alleged unlawful discriminatory practice to file a complaint with the Hawaii Civil Rights Commission. Individuals also have a private right of action under Hawaii law.

Next Steps for Employers

Hawaii employers should take steps to ensure that they are ready to comply with the new law on January 1, 2024. Employers should evaluate the practical implications of adding appropriate pay ranges to Hawaii postings and train hiring managers, talent acquisition professionals, and human resources employees on the requirements of the law.

As always, Seyfarth's Pay Equity Group is available to assist employers in navigating these new requirements and ensuring that they are ready for the ongoing trend towards greater pay transparency generally.

CLICK HERE.

Colorado's New Job Application Law Prohibits Age-Related Inquiries

Colorado employers should take heed to update their initial job applications, including online forms, to comply with Colorado's new "Job Application Fairness Act," codified at C.R.S Section 8-2-131. The new requirements went into effect on July 1, 2024, and apply not only to employers based in Colorado but also to multi-jurisdictional companies who advertise and hire within the state.

As of the effective date, Colorado employers are prohibited from inquiring about a prospective employee's age, date of birth or dates of attendance at or date of graduation from educational institutions on any initial employment applications. Employers may still ask the applicant to provide copies of certifications and transcripts, but only if they first notify the applicant they can redact information that would identify their age, date of birth or dates of study from those materials. While the Job Application Fairness Act does not create a private right of action for aggrieved workers, employers who violate this law do face penalties enforced by the Colorado Department of Labor and Employment (CDLE). The first violation may result in a warning and an order requiring compliance within 15 business days. The second violation may result in an order requiring compliance within 15 business days and a fine of up to $1,000. A third violation may result in an order requiring compliance within 15 business days and a fine of up to $2,500. Each distinct job application containing age-related inquiries constitutes a separate violation under this law.

There are some notable exceptions to the birthdate ban. Employers may verify an applicant's compliance with age requirements for a job at the initial interview stage when required for a bona fide occupational qualification pertaining to public or occupational safety, and to comply with federal laws or regulations or state or local laws or regulations based on a bona fide occupational qualification. However, such requests may not require disclosure of the worker's age, date of birth, or dates of study by the applicant or a third party.

While most employers don't ask direct age-related questions, such as the candidate's age or date of birth, unless otherwise needed for the reasons outlined above, job applications often do seek information that can reveal the applicant's age. Employers who operate within Colorado should review application forms and remove questions that can indirectly reveal age, such as dates of attendance or graduation from school. In addition, employers would be well-advised to provide training to their interviewers to ensure they understand not to ask age-related questions during applicant interviews.

CLICK HERE.

Enforcement of California's CPRA Regulations Delayed Until March 2024

In a last-minute ruling, a California judge just delayed enforcement of the California Privacy Rights Act (CPRA) regulations until March 29, 2024. Enforcement of the regulations was otherwise set to commence on July 1. This delay is a nice reprieve for businesses subject to the California Consumer Privacy Act (CCPA), but it is not a wholesale carveout from any enforcement of the CPRA. Below is a discussion of the implications on businesses and the next steps you should take.

How We Got Here

For a detailed flashback on the passage of the CPRA and CPRA Regulations, check out the Fisher Phillips Insights from November 2020 and February 2023.

The overview: In 2020, the California voters passed the CPRA by ballot initiative. While agency officials originally promulgated regulations based on the original version of the CCPA, the new statute called for further regulations to flesh out the new requirements of the law. They were to be completed no later than July 1, 2022, with enforcement starting July 1, 2023.

The California Privacy Protection Agency (CPPA), which is responsible for drafting the regulations, was unable to complete its rulemaking process by the July 1, 2022, deadline and finalized the regulations on March 29, 2023 – nine months late. This gave businesses a scant three months to get into compliance with the regulations.

The very next day, the California Chamber of Commerce filed a lawsuit seeking to delay enforcement of the regulations. The Chamber sought to delay enforcement of the entire CPRA until one year after all regulations were completed, noting that the agency was still working on rules related to cybersecurity audits, risk assessments, and automated decision-making. In other words, businesses would have been looking on at least a one-year reprieve if the Chamber's request had been granted.

Friday afternoon, a Sacramento Superior Court granted the Chamber's request for an injunction and delayed enforcement of the CPRA regulations until March 29, 2024. The Court further ruled that any future regulations passed by the CPPA would likewise have a one-year delay from when they were enacted. However, it did not go quite as far as the Chamber requested and delay enforcement until all rulemaking was completed.

What This Ruling Means for Businesses Subject to the CCPA

The good news: there is another nine months to get fully compliant with the March 29, 2023 regulations. Until the new regulations go into effect, the prior version of the regulations – which interpret the CCPA prior to the CPRA – remain in effect.

Now, the bad news: this is not a wholesale delay of enforcement of the CPRA. Businesses still need to comply with the CPRA provisions which were in the ballot initiative, even if they have a reprieve from the more detailed requirements under the regulations.

Next Steps for Businesses

Given this recent ruling and new timeline, businesses are no doubt asking what they should do now and what to prioritize. Here are the key takeaways:

- The employee, job applicant, independent contractor, and business-to-business exemption are still expired as of January 1 of this year. That was NOT affected by this Court ruling. As such, if you have not already done so, your business needs to update its CCPA notices and privacy policies to fully address these groups of California residents and their CCPA rights.
- The CPPA can still enforce the CCPA and the CPRA – it just cannot enforce the March 29, 2023 CPRA regulations. If you are still working on compliance with the CCPA, the original CCPA regulations from 2020, and the CPRA, you need to get into compliance immediately.
- Businesses should take a look at how they are prioritizing various components of CPRA compliance. With the delay of enforcement of the regulations, priority should to:
    - Focus on ensuring compliance with the requirements that are enforceable today;
    - Review the March 29, 2023 regulations and understand how they will affect your current practices;
    - Finalize an approach and the action items you will take towards compliance with the regulations;
    - Ensure the business and those involved with CCPA compliance understand the obligations and what's ahead.

There are several components to compliance with the CCPA – affecting multiple business units with operational considerations to make. Becoming compliant can be a lengthy process so businesses should make sure to take advantage of this time to get fully compliant without delay.

CLICK HERE.

New Florida Immigration Law and E-Verify Requirements for Employers

SB 1718 E-Verify Requirements

On May 10, 2023, Gov. Ron DeSantis signed a new immigration bill into law, which, among other immigration enforcement measures, requires employers with more than 25 employees to use the federal E-Verify system to verify the employment eligibility of new employees. The requirement takes effect July 1, 2023. Florida law has required public employers, contractors, and subcontractors to participate in E-Verify since 2021. The new law expands the participation requirement to private employers with more than 25 employees.

What Is E-Verify?

E-Verify is an internet-based system operated by the U.S. Department of Homeland Security that electronically verifies employment eligibility information provided by new employees. The E-Verify system supplements, but does not replace, existing I-9 employment authorization requirements. Employer I-9 requirements remain in effect.

The system compares information provided by the employee to federal databases. Generally, E-Verify provides confirmation that the Social Security number provided by the employee matches Social Security Administration records. E-Verify procedures allow employees to correct or challenge initial E-Verify determinations.

Notably, E-Verify can be used only for new hires. Employees hired before July 1, 2023, remain subject to the existing Form I-9 documentation requirements, but their information does not have to be entered into the E-Verify system.

Enforcement and Compliance

The E-Verify provisions may be enforced by state agencies, including the Florida Department of Economic Opportunity, the attorney general, and the Florida Department of Law Enforcement. Employers must provide documentation of employment eligibility to these agencies upon request.

Beginning July 1, 2024, if the Florida Department of Economic Opportunity determines that an employer has failed to comply with the E-Verify requirements, the employer will be given 30 days to correct the noncompliance. A fine of $1,000 per day may be imposed if three violations occur in any 24-month period. Violations may also result in suspension or revocation of state licenses, permits, registrations, and other forms of authorization required by law.

The new law imposes separate civil and criminal penalties on employers that hire individuals without work authorization, in addition to existing federal civil and criminal penalties. So employers may be penalized by the state of Florida for failure to participate in E-Verify and for employment of unauthorized individuals, and may also be penalized by the federal government for the unauthorized employment.

Challenges to E-Verify Provisions

Florida joins eight other states — Alabama, Arizona, Georgia, Mississippi, North Carolina, South Carolina, Tennessee, and Utah — that currently require private employers to use E-Verify.

State E-Verify participation requirements have withstood challenges arguing that federal immigration law preempts state enforcement measures. In 2011, in *Chamber of Commerce v. Whiting*, the U.S. Supreme Court upheld Arizona's E-Verify requirement for private employers on the ground that state licensing laws are exempt from preemption.

Other provisions of the new law, in particular those relating to the validity of driver's licenses issued by other states, immigration status data collection requirements for hospitals, and criminalization of interstate travel with noncitizens, may be challenged on federal preemption grounds, but the E-Verify provisions are expected to stand.

How to Enroll in E-Verify

Florida employers with more than 25 employees are required to enroll in E-Verify and to use the system for new

employees beginning July 1, 2023. Employers can enroll online and learn more on the E-Verify website, including free webinars on E-Verify and I-9 requirements and procedures.

CLICK HERE.

Texas Data Privacy and Security Act – An Overview

Texas is the second-largest state to enact a comprehensive consumer data privacy law. The Texas Data Privacy and Security Act (TDPSA) became law on June 16, 2023. Texas becomes the 11th state to enact a comprehensive consumer data privacy law, joining California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Montana, and Florida (with Oregon soon to be the 12th). Having a total population in excess of 30 million people, Texas will be the second-largest state, after California, to enact such legislation. Considering the number of residents in the 11 states with comprehensive privacy laws so far, close to 40 percent of the entire U.S. population will have access to new state consumer rights regarding their personal data. Companies need to be aware of the applicable state resident, data, and revenue thresholds and be ready to respond to a potential wave of data subject requests, while also effectively navigating the web of complex compliance and reporting obligations.

The TDPSA, which takes effect on July 1, 2024, except for global opt-out technology provisions that take effect on January 1, 2025,[1] is similar to the state privacy laws in Virginia, Utah, and Iowa (among others) that are generally more "business-friendly" relative to laws such as those in California and Colorado. Businesses that have prepared to comply with these other state privacy laws should be well-positioned to comply with the TDPSA. Even so, the TDPSA contains several notable provisions that companies should consider when developing their privacy compliance programs.

Notable Provisions

- **"Small Business" Carveout**: The TDPSA adopts a first-of-its-kind carveout for "small businesses" as defined by the U.S. Small Business Administration (SBA). As discussed in more detail below, whether a small business meets the SBA definition can be a complicated, fact-specific question. Even with a "small business" carveout, the lack of a revenue threshold or data processing threshold as found in other state privacy laws may mean that the TDPSA will apply broadly and impact a significant percentage of companies doing business in the state. Also, the TDPSA is unique among state privacy laws in prohibiting otherwise-exempt small businesses from selling sensitive personal data without consent.
- **Consent Necessary to Process Sensitive Data**: The law requires all covered businesses to obtain consent before processing "sensitive" personal data.[2] As noted above, even entities otherwise exempt from the TDPSA as a "small business" are prohibited from *selling* sensitive personal data without consumer consent.
- **Notices for Sale of Sensitive Personal Data**: As with Florida's privacy law, if a controller engages in the sale of sensitive personal data, the TDPSA requires the controller to include the following notice: ***"NOTICE: We may sell your sensitive personal data."*** Similarly, if a controller engages in the sale of biometric personal data, they must include the following notice: ***"NOTICE: We may sell your biometric personal data."*** These notices must be posted in the same location and in the same manner as a covered business's privacy notice. Exempt "small businesses" do not need to comply with these notice requirements.
- **Requirement to Recognize Universal Opt-Out Mechanism**: Like the laws in Colorado, Connecticut, California, and Montana, the TDPSA will require covered businesses to recognize universal opt-out mechanisms for the sale of personal data and targeted advertising in 2025.[3] Covered businesses will be obligated to process opt-out requests submitted by consumers via universal opt-out mechanisms that are "consumer-friendly and easy to use" and that "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."
  Cure Period with No Sunset: Following the Virginia law, the TDPSA provides covered businesses with 30 days to cure any violation of the law before the Texas attorney general can bring an enforcement action. Also like the Virginia law, this cure period does not "sunset" after a period of time.

Application Thresholds

The TDPSA applies to persons that:

1. conduct business in Texas or produce products or services consumed by Texas residents;
2. process or engage in the sale of personal data; and
3. are not "small businesses" as defined by the SBA.

Unlike the privacy laws in Virginia, Utah, Iowa, and elsewhere, the TDPSA has no specific thresholds based on annual revenue or volume of personal data processed.

Companies may find that determining whether they qualify as a "small business" under SBA regulations is surprisingly complicated. The SBA does not have a single definition for a "small business." Instead, definitions of "small business" by the SBA vary widely from one industry vertical to the next.[4]

Controller Obligations

Similar to other state privacy laws, the TDPSA imposes specific obligations on data "controllers"—those that determine the purposes and means of processing personal data—including:

- **Data minimization** – Controllers must limit collection of personal data to what is "adequate, relevant, and reasonably necessary" to achieve the purposes of collection as disclosed to the consumer.
- **Non-discrimination** – Controllers may not process personal data in violation of state and federal antidiscrimination laws or discriminate against a consumer for exercising any of the consumer's rights under the Act, including by denying goods or services, charging different prices or rates, or providing a different level of quality of goods or services.
- **Opt-out right for sales, targeted advertising, and profiling** – A controller that sells personal data to third parties or processes data for purposes of targeted advertising[5] or "profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer"[6] must clearly and conspicuously disclose consumers' right to opt out.
- **Protections for sensitive personal data** – Controllers may not process sensitive personal data without obtaining prior consent from the consumer. If a controller processes the sensitive personal data of a known child, the consumer must process that data in accordance with the Children's Online Privacy Protection Act of 1998 (COPPA).
- **Privacy notice** – A controller is required to provide consumers with a reasonably accessible and clear privacy notice containing the following information:
    - The categories of personal data processed by the controller, including the processing of any sensitive data;
    - The purpose for processing personal data;
    - The categories of personal data the controller shares with third parties (if applicable);
    - The categories of third parties with whom the controller shares personal data (if applicable); and
    - A description of the methods required for a consumer to submit a request to exercise their rights under the TDPSA, and how consumers may exercise their rights, including their appeal rights.
- **Data security safeguards** – Controllers must "establish, implement, and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue."

Exemptions

Consistent with most other state data privacy laws, the TDPSA contains entity-level, data-specific, and employment-related exemptions. Additionally, the TDPSA only protects consumers acting in an individual or household capacity, meaning it is also not applicable in business-to-business (B2B) contexts. Other exempted entities and data types are summarized below.

***Entity-level exemptions*:**

- Electric utilities, power generation companies, and retail electric providers;[7]
- Financial institutions subject to Title V of the Gramm-Leach-Bliley Act;
- Covered entities and business associates governed by HIPAA (which would include many professional services

firms and cloud service providers);
- State agencies and political subdivisions;
- Nonprofit organizations; and
- Institutions of higher education.

***Data-specific exemptions*:**
- Protected Health Information subject to HIPAA, health records, patient identifying information for the purposes of 42 U.S.C. § 290dd–2, information and documents created for purposes of the Health Care Quality Improvement Act of 1986, patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005, or identifiable private information used in connection with human clinical trials and research.
- Information originating from, and "intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this section" that is maintained by a HIPAA-covered entity or HIPAA-defined business associate.
- Personal information covered by and/or processed in accordance with the Fair Credit Reporting Act, Driver's Privacy Protection Act, Family Educational Rights and Privacy Act of 1974, the Farm Credit Act of 1971, and several others.
- Personal data processed by a person in the course of a purely personal or household activity.
- Emergency contact information.

***Employment-related exemption*:**
- Data processed or maintained in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent such data is collected and used within the context of that role.

***Processing-related exemptions*:**

The TDPSA does not restrict a controller's or processor's ability to:
- Comply with federal, state, or local laws, rules, or regulations;
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons, by federal, state, municipal, or other governmental authorities;
- Protect an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis;
- Investigate, establish, exercise, prepare for, or defend legal claims;
- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, and to preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security;
- Provide a product or service specifically requested by a consumer;
- Fulfill 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, or are compatible with the provision of a requested product or service or the performance of a consumer contract.

Additionally, the statutory requirements imposed on a controller or processor under the TDPSA do not apply if compliance would require violating an evidentiary privilege under Texas law or the disclosure of a trade secret, or "adversely affect[ ] the rights or freedoms of any person, including the right of free speech."

Consent Defined

The TDPSA narrowly defines "consent" as a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written

statement, including a statement written by electronic means, or any other unambiguous affirmative action. The Texas law expressly does not recognize the following as viable forms of consent:

- Acceptance of a general terms of use or similar document containing descriptions of personal data processing in combination with other, unrelated information;
- Hovering over, muting, pausing or closing a given piece of content; or
- Any agreement obtained via "dark patterns."[8]

Biometric Data

Like other state privacy laws, the TDPSA defines the term "biometric data" as data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retina or iris, or other unique biological patterns or characteristics (perhaps including "faceprints," although they are not mentioned explicitly). The term expressly excludes physical and digital photographs as well as video or audio recordings, and any data generated therefrom. This exclusion is similar to ones found in other state privacy laws' definitions of biometric data. However, this exclusion distinguishes the TDPSA from the Illinois biometrics law,[9] which, while generally exempting photographs and video and audio recordings, applies to scans of facial geometry created from photographs.[10] Biometric data is characterized as "sensitive data" under the TDPSA (see below) only when "processed for the purpose of uniquely identifying an individual."

Sensitive Data

Like most other state privacy laws, the TDPSA prohibits businesses from collecting and processing "sensitive data" without obtaining the consumer's consent (or the parent's consent if under 13). The TDPSA 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;

And also includes:

- Genetic and biometric data that is processed to uniquely identify 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).

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

Definition of "Sale"

The TDPSA defines "sale of personal data" as the "sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party." As a result, the Texas definition tracks with California's broader definition of "sale," as compared to the narrower definition under Virginia's privacy law, which only applies to disclosures of personal data "for monetary consideration" and not "other valuable" consideration.

TDPSA's definition of a "sale" excludes any disclosure to an affiliate of the controller, the controller's processor, for the purpose of providing a requested product or service, in a merger or acquisition of the controller's business or assets, or of information that the consumer intentionally made public via mass media.

Consumer Rights

As with other state privacy laws, the TDPSA provides consumers the right to confirm the processing of and obtain access to the consumer's personal data; request that a controller correct inaccuracies in the consumer's personal data; delete personal data about the consumer; and if available in digital format, obtain a copy of the data "the consumer

previously provided to the controller" in a portable and readily usable format "that allows the consumer to transmit the data to another controller without hindrance."

The TDPSA requires covered businesses to establish two or more secure and accessible methods (through the website or by email in specified circumstances) for consumers to submit authenticated requests to exercise their rights with respect to their personal data. Responses to consumer requests are due within 45 days of receipt, subject to a 45-day extension, when reasonably necessary. Controllers must provide information in response to a consumer's request "at least twice annually per consumer" and free of charge, unless the request is "manifestly unfounded, excessive, or repetitive."

The TDPSA also provides that any provision of a contract or agreement that waives or limits consumer rights is void and unenforceable.

Data Protection Assessments

The TDPSA requires controllers to conduct and document data protection assessments for certain types of processing that pose heightened risks to consumers. The assessments must identify and weigh the benefits of the processing to the controller, consumer, other stakeholders, and the public, against the potential risks to the consumer (while also taking into consideration any mitigating safeguards that could reduce those risks).[11] The categories that require assessments are identical to those required by Connecticut's privacy law, including:

- Processing personal data for targeted advertising;
- The sale of personal data;
- Processing personal data for profiling consumers, if such profiling presents a reasonably foreseeable risk to consumers of unfair or deceptive treatment, disparate impact, financial, physical or reputational injury, physical or other intrusion upon seclusion of private affairs, or "other substantial injury";
- Processing of sensitive data; and
- Any processing activities involving personal data that present a "heightened risk of harm to consumers."

Data protection assessments conducted to comply with comparable requirements of other laws or regulations (such as other states' privacy laws) will satisfy the requirements of the TDPSA. Data protection assessments must cover processing activities occurring only after the law's effective date and do not need to be retroactive (some state privacy laws require such assessments to cover processing activities occurring for a period prior to the law's effective date).

Data Governance Principles

The TDPSA incorporates data governance principles, including purpose limitation and reasonable security practices. Furthermore, controllers are prohibited from collecting additional categories of personal information or using collected information for additional purposes, unless they've obtained a consumer's consent.

Processor Contracts

The TDPSA uses a controller-processor framework and requires that controllers and processors—those that process personal data on a controller's behalf—enter into agreements that include terms that are standard under other state privacy laws, including clear instructions for processing data, the nature and purpose of processing, the type of data processed, the duration of processing, and the rights and obligations of both parties, including confidentiality of personal information, contracts with sub-processors, deletion or return of personal data upon termination of the agreement, and cooperation with reasonable assessments by the controller.

Enforcement – Private Right of Action?

The Texas attorney general has exclusive authority to enforce the TDPSA, though – in contrast to California, Colorado, and Florida – Texas does not provide any rulemaking authority. The Texas attorney general may levy civil penalties of up to $7,500 per violation and seek injunctive relief as well as attorney's fees and other expenses incurred in investigating and bringing an action for violations.

There is no private right of action afforded to consumers for violations under the TDPSA or "any other law."

Cure Period

Before commencing an action to enforce the TDPSA, the Texas attorney general must notify the person of the specific provisions alleged to have been violated. Following that notice, there will be a 30-day "cure" period within which the person can correct the violation. If the violation is cured, no enforcement action can be brought.

To properly "cure" under the TDPSA, the person must provide the attorney general a written statement within the 30-day period that the person: cured the alleged violation; notified the consumer that the consumer's privacy violation was addressed, if the consumer's contact information has been made available to the person; provided supporting documentation to show how the privacy violation was cured; and made changes to internal policies, if necessary, to ensure that no such further violations will occur.

The right to cure has no sunset provision and would remain a permanent part of the law, which is in contrast to states such as Colorado, Connecticut, Montana, and others where the cure period sunsets after a number of years.
Looking Ahead

The TDPSA will go into effect the same time as the recently enacted Florida Digital Bill of Rights (which is actually prior to four other states that recently passed consumer data privacy laws earlier in 2023).

The seven state privacy laws enacted so far in 2023 are slated to go into effect as follows:

- July 1, 2024 – Texas
- July 1, 2024 – Florida
- October 1, 2024 – Montana
- January 1, 2025 – Iowa
- July 1, 2025 – Tennessee
- January 1, 2026 – Indiana

Laws in Oregon and Delaware, if signed as currently presented to their governors, would be effective July 1, 2024, and January 1, 2025, respectively.

CLICK HERE.

Oregon to Become Next State to Enact Comprehensive Data Privacy Law

Oregon will soon join Iowa, Indiana, Florida, Montana, Texas, and Tennessee in passing a comprehensive data privacy law. On June 25, the Oregon legislature passed the Oregon Consumer Privacy Act. The OCPA has moved to the desk of Gov. Tina Kotek (D), who is expected to sign it into law. Assuming she does, the law will take effect on July 1, 2024. Oregon's law applies to any entity ("controller") that conducts business in the state of Oregon, or that provides products or services to Oregon residents, and that, during a calendar year, controls or processes the personal data of

- 100,000 or more consumers, not including personal data controlled or processed solely for the purpose of completing a payment transaction; or
- 25,000 or more consumers, while deriving 25 percent or more of its annual gross revenue from the sale of personal data.

"Consumer" is defined by the OCPA as a person residing in Oregon and "acting in any capacity other than in a commercial or employment context." Similar to the other laws passed this year, Oregon's definition excludes employment-related data.

Oregon's privacy law is similar to Washington State's Privacy Act; however, the Oregon law does include some unique provisions. Below are some of the highlights from the OCPA:

Applicability

Unlike some state privacy laws, the OCPA lacks some of the relatively common entity-level exemptions. For example, the OCPA does not exempt covered entities within the meaning of the Health Insurance Portability and Accountability Act or entities covered by the Gramm-Leach-Bliley Act. However, it does permit numerous data-level exemptions for data covered by federal law.

Like Colorado's law, the OCPA does not generally exempt non-profits. However, there is a limited non-profit exemption for organizations that (1) are established to detect and prevent fraudulent acts associated with insurance, or (2) provide programming to radio or television networks. Moreover, the OCPA has a one-year exemption for all non-profits until July 1, 2025.

"***Personal data" definition***

Under the OCPA, "personal data" is defined as "data, derived data or any unique identifier that is linked to or is reasonably linkable to a consumer or to a device that identifies, is linked to or is reasonably linkable to one or more consumers in a household." The definition excludes de-identified data. Covered entities will need to review their data collection and processing procedures, as well as public-facing disclosures related to data collection, use, and disclosure.

Consumer rights

The OCPA provides consumers with a right of access to obtain from a controller the following:

- Confirmation that the controller is processing or has processed the consumer's personal data and the categories of personal data that has been or is being processed.
- A list of the specific third parties, other than natural persons, to which the controller has disclosed the consumer's personal data.
- A copy of the personal data that the controller has processed or is processing.

Additionally, out of concerns that doing so would not afford consumers adequate protection, the Oregon legislature does not exclude pseudonymous data from the scope of the OCPA. As a result, controllers must include pseudonymous data when assessing and complying with consumer requests to exercise their access, deletion, correction, or portability rights.

The OCPA also provides the following consumer rights, similar to legislation in other states:

- Correction: to require the controller to correct inaccuracies in personal data about the consumer.
- Deletion: to delete personal data about the consumer.
- Opt out: to opt out of personal data processing for purposes of
    - targeted advertising,
    - the sale of personal data, or
    - profiling in furtherance of decisions producing legal effects or similar effects.
- Data Portability: to provide a copy of personal data in a portable and readily usable format.

Similar to California, Colorado, Connecticut, and Montana, Oregon will require data controllers to recognize universal opt-out mechanisms beginning on January 1, 2026.

Data protection assessments

Joining a number of other states, Oregon will require a controller to conduct a data protection assessment for all processing activities that present a heightened risk of harm to consumers, including processing of the following:

- Sensitive personal data.
- Personal data for targeted advertising, selling, or profiling, where certain foreseeable risks exist.

These data protection assessments must be retained by controllers for at least five years.

Enforcement

The OCPA provides authority to the Oregon Attorney General to enforce the OCPA and to levy civil penalties of up to

$7,500 for each violation, or to enjoin the business from certain activities, or to seek other equitable relief. The OCPA has a five-year statute of limitations.

Right to cure

The Oregon Attorney General must provide controllers with a 30-day period to cure violations of the OCPA. However, this right to cure will sunset on January 1, 2026.

Private right of action

Although the initial drafts of the OCPA contained a private right of action for consumers, that provision was ultimately removed. Thus, California is still the only state whose privacy law includes a private right of action for consumers.

CLICK HERE.

Connecticut Expands Regulation of Consumer Data Privacy

Amendments to the Connecticut Data Privacy Act add significant new requirements for processing consumer health and minors' personal data

The Connecticut legislature passed and the governor recently signed amendments to the Connecticut Data Privacy Act (CTDPA), the state's comprehensive consumer data privacy law, which goes into effect July 1, 2023. Some provisions in the new legislation – An Act Concerning Online Privacy, Data and Safety Protections (CT Online Privacy Law) – go into effect July 1, 2023, while other provisions will become effective next July 1 and October 1, 2024. The new law gives minors (and in some cases minors' parents) more control over their personal data and accounts on social media platforms and introduces new protections for minors' personal data and health-related data of Connecticut residents.

We highlight key provisions of the CT Online Privacy Law below.

Enhanced Privacy Protections for Consumer Health Data

Effective July 1, 2023

The new law amends the CTDPA to protect "consumer health data," which includes any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, including gender-affirming health data and reproductive or sexual health data. The law amends the existing definition of "sensitive data" to include "consumer health data," thereby requiring controllers to obtain consent from consumers before processing such data. It also prohibits any person from selling or offering to sell "consumer health data" without consumers' consent or allowing employees or contractors access to "consumer health data" unless they are subject to contractual or statutory duties of confidentiality.

The law also prohibits the use of "geofences" (i.e., virtual boundaries using GPS, cellular, Wi-Fi, or similar technology within 1,750 feet of any mental health or reproductive or sexual health facility) for the purpose of identifying, tracking, or collecting data from or sending notifications to a consumer "regarding the consumer's consumer health data."

Ability to "Unpublish" and Delete Accounts on Social Media Platforms

Effective July 1, 2024

The CT Online Privacy Law requires social media platforms to give minors – defined as consumers under 18 years of age – the right to "unpublish" (i.e., remove from public visibility) and delete their accounts. Social media platforms will have to describe and provide in their privacy notices mechanisms to exercise these rights. Platforms will have 15 business days to "unpublish" accounts and 45 business days (with a 45-day extension, when necessary, with notice) after receiving a request to delete accounts and cease processing that minor's personal data. Social media platforms are

not required to delete accounts when preserving the account or personal data is otherwise permitted or required by applicable law, including as required or permitted under the CTDPA. While minors who are 16 and older must exercise this right themselves, parents may make requests on behalf of minors under 16 years of age.

The CT Online Privacy Law defines "social media platforms" narrowly to include public or semi-public Internet-based services or apps that:

- Are used by consumers in Connecticut,
- Are *primarily intended* to connect and allow users to socially interact with such service or app, and
- Enable a user to: (a) construct a public (or semi-public) profile for the purpose of signing into the service or app; (b) populate a public list of other users with whom the user shares a social connection through the service or app; and (c) create or post content that is visible by other users (including but not limited to message boards, chat rooms, or through a landing page or main feed that shows the user content that is generated by other users).

The law expressly excludes public (or semi-public) Internet-based services or apps that:

- Exclusively provide email or direct messaging services;
- Primarily consist of news, sports, entertainment, interactive video games, electronic commerce, or content that is preselected by the provider *or* for which any chat, comments, or interactive functionality is incidental to, directly related to, or dependent on the provision of such content; or
- Is used by and under the direction of an educational entity, including but not limited to learning management systems or student engagement programs.

Unlike other laws that impose obligations regarding minors, the CT Online Privacy Law does not require that the social media platforms have "actual knowledge" or willfully disregard that the consumer is a minor. It does require, however, that the social media platform "authenticate" the request, meaning that the social media platform will not have to comply if it cannot – using reasonable means and making a commercially reasonable effort – determine that the request has been submitted by or on behalf of the minor who is entitled to exercise the right. As part of the authentication process, the individual making the request will need to provide information showing that the account or personal data belongs to a minor, as defined under the law, and this will undoubtedly require some proof of age of the minor account holder. Violations of this section of the law are unfair or deceptive acts or practices under the Connecticut consumer protection statute and are enforceable by the Connecticut attorney general.

Children's Online Safety Protections

Effective October 1, 2024

The CT Online Privacy Law also creates new obligations for controllers that provide an "online service, product, or feature" to "minors" (here, again, minors are consumers who are under 18 years of age). An "online service, product, or feature" is defined broadly to include *any* service, product, or feature that is provided online, *except for*: (1) any telecommunications service, as defined in 47 U.S.C. § 153; (2) broadband Internet access service, as defined in 47 C.F.R. § 54.400; or (3) delivery or use of a physical product.

Controllers that provide an online service, product, or feature to consumers whom the controller has actual knowledge, or willfully disregards, are minors must: (1) use "reasonable care" to avoid any "heightened risk of harm" to minors caused by the online service, product, or feature; and (2) conduct a data protection assessment of such online service, product, or feature to, among other things, address any "heightened risk of harm" to minors. A "heightened risk of harm" occurs when a controller processes minors' personal data in a way that creates a reasonably foreseeable risk of: (1) unfair or deceptive treatment of or unlawful disparate impact on minors; (2) any financial, physical, or reputational injury to minors; or (3) any physical or other intrusion upon the solitude or seclusion – or the private affairs or concerns – of minors, if such intrusion would be offensive to a reasonable person. Controllers that comply with the requirement to conduct a data protection assessment will be entitled to a rebuttable presumption that they have complied with the duty to use reasonable care in an enforcement action brought by the Connecticut attorney general.

Certain Activities Prohibited Without Consent: Controllers that offer an online service, product, or feature and have actual knowledge or willfully disregard that consumers are minors are prohibited from doing the following without the

minor's consent (or consent of the minor's parent, if the minor is under 13 years of age):

- Processing a minor's personal data for: (1) targeted advertising; (2) sales; or (3) profiling in furtherance of any fully automated decisions that produce legal or similarly significant effects;
- Processing a minor's personal data *except* as – or for longer than – reasonably necessary to provide the online service, product, or feature;
- Processing a minor's personal data for any processing purpose other than what the controller disclosed at the time of collection (or is reasonably necessary for and compatible with the processing purpose disclosed);
- Using any system design feature to "significantly increase, sustain, or extend" any minor's use of such online service, product, or feature; or
- Collecting a minor's precise geolocation data, unless – in addition to obtaining the required consent – such precise geolocation data is necessary for the controller to provide such online service, product, or feature (and then only for the time necessary to do so) *and* the controller provides to the minor a signal – available for the duration of collection – that the controller is collecting such data.

Consent mechanisms provided may not be designed to substantially subvert or impair or manipulate with the effect of substantially subverting or impairing user autonomy, decision-making, or choice.

Direct Messaging Services: Controllers may not offer any direct messaging "apparatus" for use by minors without providing easily accessible safeguards that limit the ability of adults to send unsolicited communications to minors with whom they are not connected. This provision will not apply to services whose predominant or exclusive function is: (1) email; or (2) direct messaging consisting of text, photos, or videos sent between devices when such messages are shared between – and only visible to – sender and recipient and not posted publicly.

Enforcement and Cure Period: The Connecticut attorney general has exclusive enforcement authority and from October 1, 2024, through December 31, 2025, must give controllers or processors 30 days to cure any alleged violations of these provisions that the attorney general determines (in his or her discretion) the controller may cure. Beginning January 1, 2026, the attorney general will have discretion to provide an opportunity to cure and will consider the following factors in doing so: (1) the number of violations that the controller or processor is alleged to have committed; (2) the size and complexity of the controller or processor; (3) the nature and extent of the controller's or processor's processing activities; (4) whether there exists a substantial likelihood that the alleged violation has caused or will cause public injury; (5) the safety of persons or property; (6) whether the alleged violation was likely caused by a human or technical error; and (7) the sensitivity of the data.

CLICK HERE.

District of Columbia Cannabis Employment Protections Amendment Act Goes Live July 13

The District of Columbia is joining the increasing number of jurisdictions providing greater protections for private employees who use marijuana off-duty, during non-work hours. Such development remains in contrast with federal law, which still classifies marijuana as a controlled substance, prohibiting both possession and use of marijuana.

In addition to protections for private employees, the D.C. Cannabis Employment Protections Amendment Act of 2022 (C.E.P.A.A.) imposes new obligations on private employers to inform employees of the new laws. D.C. Law 24-190 §§ 100 et seq.; tentatively D.C. Code §§ 32-921.01 through .08. The C.E.P.A.A. goes into effect July 13, 2023.

Highlights for D.C. Employers

Under C.E.P.A.A., employers will be prohibited from taking personnel actions against an individual for cannabis or marijuana use off-premises during non-work hours.

Employers are permitted to take action related to such use, however, if the employee is designated as safety sensitive, a federal contract or statute prohibits marijuana use, or the employee used or possessed marijuana at the employer's premises or during work hours.

Drug-Testing

The presence of cannabinoid metabolites in an employer-required or requested drug test may be used to justify adverse action if the employee is impaired by the use of cannabis at the place of employment or during work hours.

Cannabis impairment is exemplified by the employee manifesting specific, articulable symptoms that substantially decreases or lessens the employee's performance of duties or such symptoms interfere with the employer's ability to maintain a safe and healthy workplace. This will alter the availability of pre-employment drug testing for many private employers in the District of Columbia.

Safety Sensitive-Designated Positions

Employers must provide notice to their employees of the new protections within 60 days of July 13 or upon hire.

The notice requirement includes informing employees if their position has been designated as safety sensitive, among other requirements. Safety-sensitive positions are those reasonably foreseeable that, if the employee performs the position under the influence of drugs or alcohol, the person could cause actual, immediate, and serious bodily injury or loss of life to themself or others. The following are statutory examples of safety sensitive positions:

(A) Security services such as police or security that involves the custody, handling, or use of weapons;
(B) Regular or frequent operation of a motor vehicle or other heavy or dangerous machinery;
(C) Regular or frequent work on an active construction site;
(D) Regular or frequent work near gas or utility lines;
(E) Regular or frequent work involving hazardous material;
(F) Supervision of those who reside in an institutional or custodial environment; or
(G) Administration of medication, performance or supervision of surgeries, or other medical treatment requiring professional credentials.

Notice of Reporting Requirements

Employees may report alleged noncompliance with the C.E.P.A.A. within one year to the D.C. Office of Human Rights. Administrative requirements for recreational and medical marijuana users differ under the new law. Recreational marijuana users are required to exhaust their administrative remedies under the C.E.P.A.A. before bringing private cause of action. Medical marijuana patients are not required to exhaust administrative remedies, but they cannot bring a private cause of action directly to the court if they have initiated an administrative complaint with the D.C. Office of Human Rights alleging the same noncompliance.

Employer Penalties for Noncompliance

If the employer if found to have violated the C.E.P.A.A., the director of the D.C. Office of Human Rights may order the employer to do any of the following:

- Pay civil penalties, half of which awarded to complainant and half deposited to the General Fund of D.C.;
    - 1–30 employees: up to $1,000 per violation o 31–99 employees: up to $2,500 per violation o 100+ employees: up to $5,000 per violation
- Pay double the civil penalties listed above if the employer is found to be noncompliant in the past year;
- Pay the employee's lost wages;
- Undergo training or any other equitable relief to undo the adverse employment action; and
- Pay reasonable attorneys' fees and costs.

In a private cause of action, a court may institute the civil penalties above and:

- Payment of lost wages;
- Payment of compensatory damages;
- Equitable relief as appropriate; and
- Payment of reasonable attorneys' fees and costs.

D.C. employers should amend their workplace designations and policies in accordance with the changes mandated by the

D.C. Cannabis Employment Protections Amendment Act. Jackson Lewis attorneys are happy to assist in navigating the changes required to remain compliant with new laws in the District of Columbia.

CLICK HERE.

New NYC Law Restricting Artificial Intelligence-Driven Employment Tools Reveals What's to Come

Up until now, employers have been able to use artificial intelligence (AI)-powered hiring and promotional tools without worry about compliance with AI-specific laws. On July 5, 2023, that changed. New York City passed **Local Law 144**, legislation restricting employers' use of artificial intelligence-driven employment tools.

Local Law 144 prohibits employers from using an automated employment decision tool ("AEDT") in hiring, promotion, and other employment decisions, unless the employer first ensures that the tool has been audited for bias within the preceding year. These AI-powered tools—ranging from programs that screen resumes for qualifications to those that assign scores to candidates based on mannerisms and responses in video interviews—are increasingly used by employers. However, AEDTs have generated controversy due to the potential for bias. Now, New York City employers are required to independently audit their AEDT systems for bias and publish the results on their company websites, or face fines. Local Law 144 also requires employers to provide job candidates with notice about the use of an AEDT system and offer them an opportunity to opt out. Employers found in violation of Local Law 144 face a $500 fine on the first offense and a $1,500 fine on each subsequent one.

New York City Local Law 144 comes amid a global push to regulate the use of AI and may provide a model for auditing rules that can be adopted in other jurisdictions. However, it does not provide any legal threshold for when AI-based hiring or recruiting should be considered biased or to have a disparate impact on protected groups. The EEOC, which has publicized its intent to review AEDTs with scrutiny, has provided limited endorsement for a "**rule of thumb**," which states that if a hiring test has a selection rate of less than 80% for a protected group, compared to others, then such a gap likely indicates bias.

Notably, other states and jurisdictions have also enacted AI-based legislation:

- In 2020, Illinois enacted the Artificial Intelligence Video Interview Act, **820 ILCS 42,** to govern the use of AI to assess video interviewees for jobs. Employers recruiting in Illinois must (1) obtain consent from applicants before using AI, after explaining how the AI works and its evaluation standards; and (2) ensure proper control of video recordings and deletion upon request. Unlike New York City's law, however, the Illinois law does not include civil penalties.
- Maryland passed an AI-employment law in 2020, **B. 1202**, which prohibits employers from using facial recognition technology during an interview for employment without consent. Consent requires a signed waiver that states: (1) the applicant's name; (2) the date of the interview; (3) that the applicant consents to the use of facial recognition; and (4) confirmation that the applicant read the consent waiver. H.B. 1202 does not include a specific penalty or fine.
- Many states are creating councils to oversee AI and new regulations, including Alabama, Colorado, Illinois, Maryland, Vermont and Washington with pending legislation to create similar entities in many more states.
- On May 24, 2022, Vermont created the Artificial Intelligence Commission to support the ethical use and development of artificial intelligence in the state, relating to the use and oversight of artificial intelligence in state government. **VT H.B. 410**.
- Similar to Vermont, Colorado passed **CO S.B. 113**, which created a task force for consideration of facial recognition services. This task force is directed to, among other issues, recommend whether the scope of the task force should be expanded to include consideration of artificial intelligence.

Since 2018, states have ramped up legislation directly related to artificial intelligence and the predicted advances in technology. Local Law 144 is the most comprehensive regulation to date of the use of artificial intelligence and machine learning applications in human resources. But it is certainly not the first piece of legislation on the books governing the use of AI in the workplace. Other jurisdictions are expected to quickly follow suit given the recent media attention to ChatGPT and other AI applications. Employers that use automated decision-making for hiring and promotional decisions should start considering now whether they need to modify these tools to ensure that they do not contain bias.

CLICK HERE.

Illinois Poised To Require Pay Transparency In Job Postings

Illinois is poised to become the latest state to require employers to provide salary information in job postings. Governor J.B. Pritzker is expected to sign House Bill 3129, which amends the Illinois Equal Pay Act (IEPA) and requires employers to include pay scale and benefits information in job postings. If the Bill is enacted, its requirements will go into effect on January 1, 2025, and will apply to employers with 15 or more employees and to positions that are (i) physically performed, in whole or in part, in Illinois or (ii) physically performed outside of Illinois where the employee reports to a supervisor, office or other work site in Illinois.

The bill defines "pay scale and benefits" broadly to mean the wage or salary, or the wage or salary range, for the position and a general description of the benefits and other compensation, including, but not limited to, bonuses, stock options or other incentives the employer reasonably expects to offer. The bill's posting requirements can be satisfied by including a hyperlink in the job posting to a publicly viewable webpage that outlines the pay scale and benefits for the position. Further, an employer may satisfy the bill's benefits posting requirement by posting a relevant and up-to-date general benefits description in an easily accessible, central and public location on the employer's website, and providing this location in the job posting. The law also applies to internal promotions: if a job is posted publicly, but internal candidates may also apply for the position as a promotion, the employer must announce, post or otherwise make known to current employees that promotion opportunity within 14 days of externally posting the position.

Notably, if an employer does not use job postings, the bill clarifies that it does not create any new requirement to do so. Use of a third-party posting service does not allow employers to circumvent the posting requirements; any third party that fails to provide the pay scale and benefits in job postings published on behalf of an employer is subject to liability, unless it can show that the employer failed to provide the necessary information. Accordingly, Illinois employers should work closely with any third party they use to assist with job postings and recruitment to ensure that posting requirements are satisfied. The law includes record-keeping requirements, including the obligation 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 law, until their destruction is authorized by the Illinois Department of Labor (IDOL) or court order.

An employer that does not make pay scale and benefits information available to an applicant, through public or internal postings for the job, "shall disclose … the pay scale and benefits to be offered for the position prior to any offer or discussion of compensation and at the applicant's request." Additionally, the law includes an anti-retaliation provision: employers "shall not refuse to interview, hire, promote, or employ, and shall not otherwise retaliate against, an applicant for employment or an employee for exercising any rights" thereunder.

The IDOL may initiate investigations regarding compliance with the amendments under HB3129 at its discretion or upon receiving a complaint from any individual (within one year of the violation). If the IDOL determines that a violation occurred, an employer may cure the violation within seven days; otherwise, the employer will be subject to civil penalties. Excluding duplicative posts, each job posting not in compliance with the law will be considered a separate violation that could incur civil penalties. Employers found to be in violation of the bill's posting requirements face fines ranging from $250 to $10,000, depending on the number of prior violations, whether postings are duplicative, and whether the job posting is active or inactive at the time the notice of violation is issued. The law does not provide for a private right of action.

This law is just the latest in a series of actions that Illinois lawmakers have taken regarding pay transparency issues. In 2019, Illinois amended the IEPA to prohibit employers from requesting or requiring that job applicants disclose wage or salary history as a condition of employment. In 2021, Illinois further amended the IEPA to require certain employers to obtain an equal pay registration certificate every two years and provide EEO-1 type diversity data in annual reports filed with the State. When the law becomes effective, Illinois will join a number of other states, including California, Colorado and Washington, in requiring the disclosure of salary information in job postings.

CLICK HERE.

Delaware Could Become the 13th State to Enact a Comprehensive State Privacy Law

On June 30, 2023, the Delaware House of Representatives passed the Delaware Personal Data Privacy Act (H.B. 154) (the "DPDPA"), a day after the Delaware Senate passed the legislation. The DPDPA heads to Governor John Carney for a final signature. This could make Delaware the 13th U.S. state to enact comprehensive privacy legislation.

Applicability

The DPDPA would apply to persons that conduct business in Delaware or persons that produce products or services that are targeted to Delaware residents and that during the preceding calendar year did any of the following: (1) controlled or processed the personal data of not less than 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) controlled or processed the personal data of not less than 10,000 consumers and derived more than 20 percent of their gross revenue from the sale of personal data.

The DPDPA's protections would apply to Delaware residents who act for a personal or household purpose, with express exemption for individuals acting in a commercial or employment context. The DPDPA also contains a number of exemptions, including exceptions for financial institutions, affiliates and data subject to Title V of the Gramm-Leach-Bliley Act, covered entities and business associates under the Health Insurance Portability and Accountability Act of 1996 and nonprofit organizations.

Controller Obligations

Similar to other comprehensive state privacy laws, the DPDPA would require controllers to limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. In addition, controllers would need consumer's consent to process sensitive data or to process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer. The DPDPA also requires controllers to establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

The DPDPA also would require controllers to provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes, among other requirements: (1) the categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (4) the categories of personal data that the controller shares with third parties, if any; (5) the categories of third parties with which the controller shares personal data, if any; and (6) an active electronic mail address or other online mechanism that the consumer may use to contact the controller.

The DPDPA also would require controllers that control or process the data of not less than 100,000 consumers (excluding data controlled or processed solely for the purpose of completing a payment transaction) to conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to the consumer. For the purposes of the DPDPA's data protection assessment requirement, processing that presents a heightened risk of harm to a consumer includes: (1) the processing of personal data for the purposes of targeted advertising; (2) the sale of personal data; (3) the processing of sensitive data; and (4) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of any of the following: (a) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (b) financial, physical, or reputational injury to consumers, (c) a physical or other intrusion upon the solitude or seclusion, or private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (d) other substantial injury to consumers.

Consumer Rights

The DPDPA provides consumers with the following rights: (1) to confirm whether a controller is processing the consumer's personal data and access such personal data; (2) to correct inaccuracies in the consumer's personal data; (3) to delete personal data provided by, or obtained about, the consumer; (4) to obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; (5) to obtain a list of the categories of third parties to which the

controller has disclosed the consumer's personal data; (6) to opt out of the processing of the personal data for purposes of (a) targeted advertising, (b) the sale of personal data and (c) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Controllers would have 45 days to respond to consumer rights requests, with a potential 45-day extension in certain circumstances.

Enforcement

The DPDPA does not contain a private right of action and would be enforced exclusively by the Delaware Department of Justice. The DPDPA provides a 60-day cure period for violations until December 31, 2025. If a violation is not cured, the Department of Justice may bring an enforcement proceeding.

Effective Date

If the DPDPA is enacted before or on January 1, 2024, the DPDPA would take effect on January 1, 2025. If the DPDPA is enacted after January 1, 2024, however, the DPDPA would take effect on January 1, 2026.

CLICK HERE.

COURT CASES

California FCRA Ruling Boosts Technical Claim Defense

A significant decision from a California state appeals court has shifted the legal landscape for technical Fair Credit Reporting Act claims brought in California state court in favor of defendants.

In October, the Fifth Appellate District held the FCRA does not confer standing on plaintiffs to sue in California state court, absent any allegation of concrete injury. The case is styled *Limon v. Circle K Stores Inc.*

In January, the California Supreme Court denied both the plaintiff's petition for review and several requests for depublication of the opinion, meaning that the court of appeal's opinion will stand for now.

In Limon, the plaintiff alleged the defendant violated the "standalone disclosure" and "clear and conspicuous" requirements of the FCRA by including extraneous information in a background check disclosure.

Under the FCRA, a prospective employer that intends to use a background check on a candidate must first disclose to the candidate the employer's intention to procure such a report and obtain the candidate's authorization in writing.

The disclosure must be clear and conspicuous and appear in a document that consists solely of the disclosure.

The allegedly extraneous information in the Limon disclosure included both a liability release and state disclosures. Limon also alleged he "was confused regarding the nature of his rights under the FCRA."

Limon had initially been filed in the U.S. District Court for the Eastern District of California in 2018, but was dismissed in 2020 without prejudice for lack of Article III standing.

The case was subsequently refiled in California state court, where the defendant demurred on the grounds that the plaintiff lacked standing because he suffered no concrete injury or harm.

The trial court sustained the demurrer without leave to amend and entered judgment in favor of the defendant. The Fifth Appellate District affirmed the trial court's ruling.

The Fifth Appellate District decision provided a detailed analysis of the framework for standing in California. The court first acknowledged the California Legislature does have the "power to confer standing on a class of persons irrespective of whether they suffered injury." However, if that right is not provided by statute, then concrete injury may be required. The court explained while California courts are not constrained by the case or controversy provisions of Article III of the U.S. Constitution, they have equated the "beneficially interested" test for standing in California to the Article III requirement.

As a general matter, to have standing to pursue a claim for damages in California state court, a plaintiff must be beneficially interested in the claims they are pursuing.

Accordingly, a plaintiff lacks standing if she does not have a real interest in the ultimate adjudication of a case because she has neither suffered, nor is about to suffer, an injury of sufficient magnitude reasonable to assure that all the relevant facts and issues will be adequately presented.

Thus, the purpose of a standing requirement is to ensure California courts will decide only actual controversies between parties with a sufficient interest in the subject matter of the dispute to press a case with vigor.

Next, the Fifth Appellate District explained the FCRA does not eliminate the requirement that a plaintiff be beneficially interested — suffer an injury-in-fact — to have standing because the FCRA's statutory damages provision is intended to compensate a plaintiff for actual injury. It is designed to provide redress where damages are "difficult or impossible to quantify or prove," according to the decision.

It is not intended to penalize a company for violation of the FCRA. Additionally, the FCRA does not confer public interest standing on a plaintiff.

Instead, the FCRA expressly confers authority upon federal and state agencies and officials — not private litigants — to vindicate the public's interest in ensuring compliance with the FCRA. As such, to have standing to pursue his claims, a plaintiff must allege a concrete injury.

Under this framework, the court held Limon had not suffered a sufficient injury to sue based on the alleged technical violations of the FCRA's background check disclosure requirements.

The Fifth Appellate District explained Limon did not allege:

- He did not receive a copy of the consumer report that the defendant obtained;
- The consumer report obtained by the defendant contained any defamatory content or other per se injurious content;
- The consumer report contained false or inaccurate information; and
- Any exposure to a material risk of future harm, imminent or substantial.

Accordingly, the court held there was no injury to Limon's protected interest in ensuring fair and accurate credit reporting, nor was there any injury associated with any adverse employment decision based on false or inaccurate reporting.

The court also explained the alleged "extraneous language" was not extensive and the disclosure notices otherwise appeared to comply with the FCRA.

Further, Limon undoubtedly understood he was willing to have a background check conducted on him prior to being hired and knew he could withhold his consent.

In light of the above facts, the court held that Limon had not alleged a concrete or particularized injury to his privacy interests in connection with his claim of informational injury. Thus, Limon did not have standing to pursue his claim in California state court.

The court's ultimate conclusion was that, under California law, an informational injury that causes no adverse effect is insufficient to confer standing upon a private litigant to sue under the FCRA.

This decision is important because, for decades, plaintiffs have pursued technical FCRA cases in certain state courts, given their lack of Article III standing requirement.

This is particularly true following the U.S. Supreme Court's 2021 TransUnion LLC v. Ramirez decision on standing, which held a concrete injury requires more than the existence of a risk of harm, and which led to a substantial increase in state court filings.

California has been a particularly popular forum for these types of cases, given the generally pro-consumer mindset of California courts, the traditionally broad justiciability requirements for standing, and the sheer number of individuals that reside in the state.

However, the Fifth Appellate District has now foreclosed plaintiffs from pursuing such claims in California state courts under its interpretation of California's standing doctrine, and the California Supreme Court has decided not to accept the petition for review and to decline requests for de-publication.

Accordingly, for now, and this interpretation of legal standing in California will drastically limit FCRA plaintiffs' ability to bring lawsuits alleging technical, no-harm violations in any forum.

At least one federal district court has already said as much. The U.S. District Court for the Northern District of California explained last month in Aguilar v. Laboratory Corp. of America that, normally, a lack of subject matter jurisdiction over a removed claim would result in remand, but in the Ninth Circuit there is an exception when it is an

'absolute certainty' that the state court would immediately dismiss the case on remand ... While it is theoretically possible that there could be standing to pursue the FCRA claim in state court even if no federal standing exists, California courts also require a 'concrete injury' for standing to pursue a FCRA claim.

Undoubtedly, the Limon decision will bolster FCRA defendants' ability to assert lack of standing as a defense in FCRA cases filed in California state court, where plaintiffs have not suffered any concrete harm.

And, for now, this opinion will likely drive down settlement values for these kinds of technical FCRA cases, given the risk that the litigation stands to be dismissed based on lack of standing, perhaps even at the pleading stage.

Ultimately, however, plaintiffs will surely look for ways to fight and/or distinguish this decision. Also, given the lack of horizontal stare decisis among sister appellate districts in California, plaintiffs attorneys will likely work to have other California appellate courts examine the standing issue under FCRA.

Accordingly, while this decision will offer a short-term boost to defendants, the long-term impact of Limon remains to be determined.

CLICK HERE.

INTERNATIONAL DEVELOPMENTS

UK Information Commissioner's Office Publishes New Guidance on Data Subject Access Requests

On May 24, 2023 the UK's data protection body, the Information Commissioner's Office (the ICO), published a new guide for employers on responding to data subject access requests (DSARs).

When publishing the guidance, the ICO noted that it received over 15,000 complaints regarding subject access in the last year and failure to comply with a DSAR was the most frequent reason that people complained to the ICO, making up around a third of all of the complaints.

Failing to comply with a DSAR can result in fines or reprimands as well as reputational damage, so it is important that organizations get it right. We are also increasingly seeing failure to comply with DSARs being cited as a complaint in employment litigation.

What are DSARs?

The right of access gives individuals the right to request a copy of their personal information from organizations. Organizations must respond to a DSAR within one month of receipt of the request although this timeframe can be extended by up to a further two months if the DSAR is complex or if the employee has sent a number of requests.

DSARs have become a strategic tool for employees attempting to gain information, often during a dispute or grievance process. Employers must strike a balance between upholding employees' right of access, protecting sensitive corporate information, protecting other individuals' data and applying legal exemptions in an appropriate way. As many employers have learned the hard way, DSARs can be time-consuming and resource intensive.

What does the guidance include?

Although the new guide doesn't tell us anything new, it includes some practical guidance for employers on some common tricky areas, for example:

- disclosure of witness statements used in internal disciplinaries or investigations;
- disclosure of whistleblowing reports;
- the application of the existing legal exemptions (*e.g.*, confidential references, privilege, management information and negotiations with the requester);
- when a request is manifestly excessive (and can therefore be refused);
- whether you still need to comply with a DSAR if the worker has signed an NDA or settlement agreement;
- whether you need to comply with a DSAR if the individual is going through an employment tribunal or grievance process (spoiler alert: yes, you do);
- how to deal with emails that the worker is copied on;
- searches of social media used in the workplace (*e.g.*, Facebook, WhatsApp, Twitter); and
- how to deal with requests for CCTV footage.

CLICK HERE.

MISCELLEANOUS DEVELOPMENTS

Data Privacy and AI Regulation in Europe, the UK, and US

Artificial intelligence (AI) magnifies the ability to analyze personal information in ways that may intrude on privacy interests, which can give rise to legal issues. Generally, there are two types of concerns with AI and privacy: input concerns, including the use of large datasets that can include personal information, and output concerns (a newer phenomenon with the rise of AI), such as whether AI is being used to arrive at certain conclusions.

Although they do not always expressly speak to AI, there are regulations and guidance throughout the United Kingdom, Europe and United States that cover the privacy principles.

European Union

In Europe, there is one comprehensive privacy law in the European Union and United Kingdom: the General Data Protection Regulation (GDPR). It is relevant to all industries and applies to all personal data, regardless of type or context, including automated processing of data, which is tightly regulated. It contains a robust requirement to inform people how their data going to be used and what will happen with it. Notably, it includes a requirement to conduct a data protection impact assessment, which could lead to further investigation by regulators.

The GDPR also covers "automated individual decision-making, include profiling" requiring explicit consent from a data subject for the processing of data, with certain exemptions. For AI tools, lawfulness, fairness, and transparency are key requirements under the GDPR.

AI Ethics Framework Proposal

In 2021, the European Commission proposed new rules and actions in an effort to turn Europe into a global hub for "trustworthy" AI, the AI Act, and coordinated plan, which is an outline that goes hand in hand with the AI Act. Certain AI systems are prohibited under the AI Act, including a number that are sometimes highlighted as issues in the context of social media.

The UK

The AI Act no longer applies to the UK, yet it is still relevant to UK businesses as a result of its extraterritorial reach, as in the US. From a privacy perspective, the UK needs to maintain data protection equivalence with the EU to maintain its adequacy status—which is up for review by December 2024.

In 2022, the UK government announced a 10-year plan to make the UK an "AI Superpower" in its National AI Strategy and in March 2023 published its white paper setting out the UK government's framework and approach to the regulation of AI, providing a principles-based approach. UK regulators are expected to publish non-statutory guidance in the next 12 months demonstrating divergence from the EU's approach.

UK White paper

The Department for Science, Innovation, and Technology (DSIT) also published a long-awaited AI white paper in March 2023 setting out five principles which regulators must consider to build trust and provide clarity for innovation. The UK regulators will incorporate these principles into guidance to be issued over the next 12 months. Following its 2022 toolkit, the ICO has published its own detailed guidance and a practical toolkit on AI and data protection, updated in March 2023.

The United States

The US comprises a myriad of privacy laws based on jurisdiction and sector which contain principles relating to AI;

however, specific AI guidance is expected. The White House announced a blueprint for an AI Bill of Rights, with recommended principles to deploy AI, particularly privacy provisions.

The National Institute of Standards and Technology's cyber security guidance has been widely adopted. The AI Risk Management Framework released in January 2023 specifically identifies privacy as significant for input and output risk.

FTC Enforcement Actions

The Federal Trade Commission (FTC) is the enforcement authority that regulates data privacy issues and has issued a series of reports on AI and related consumer and privacy issues, most recently in April 2021. There have been a series of enforcement actions relating to algorithms, particularly algorithmic disgorgement where underlying data was found to be unlawfully used to target individuals for advertising.

California Consumer Privacy Act

The California Consumer Privacy Act (CCPA), effective July 1, 2020, is similar to the principles under the GDPR and entails a broad definition of personal information, intended to include robust consumer profile and preference data collected by social media companies and online advertisers.

The CCPA has been amended in a way that starts to speak directly to AI, including a definition of "profiling" and rules about "automated decision-making." It requires a data privacy impact assessment for processing activities, including profiling, and requires the new California Privacy Protection Agency to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology, which contains a broad mandate. The draft regulation is expected within the next few months.

In 2023, similar rules were enacted through the Virginia Consumer Data Protection Act, the Colorado Privacy Act, and Connecticut Data Privacy Act.

The Way Forward

New regulations and guidance are on the way in the UK, EU, and US requiring AI projects to safeguard the often-large datasets at hand. There are ways to potentially navigate risks through anonymization and de-identification, the use of privacy policies, and contractual provisions; however, close attention should be paid to whether AI has the right to use data in an AI system and how the system uses and discloses information.

CLICK HERE.