ILLINOIS STATE BAR ASSOCIATION

OCTOBER 2024 VOL 3 NO. 1

Privacy & Information Security Law

The newsletter of the Illinois State Bar Association's Privacy & Information Security Law Section

BIPA Update: Illinois Adopts Reform Limiting Potential Claims (And Damages) in Litigation

BY BRITTNEY MOLLMAN, DREMAIN MOORE, SUSAN LORENC, AND ELIZABETH CASALE

ON AUGUST 2, 2024, ILLINOIS GOV. J.B. PRITZKER signed S.B. 2979 into law. S.B. 2979 amends the Illinois Biometric Information Privacy Act (BIPA) to more clearly specify the scope of liability where multiple violations are alleged.

What is BIPA?

BIPA, enacted in 2008, regulates how private entities collect, use, share, and store biometric data. BIPA's expansive definition of biometrics includes retinal or iris scans, fingerprints, voice prints, and facial geometric scans. Under BIPA, private entities could be liable for liquidated damages ranging from $1,000 to $5,000 per violation.

White Castle v. Cothron broadens BIPA claim accrual

In February 2023, the Illinois Supreme Court issued a significant holding

Continued on next page

Discrimination Based on Conviction Records: What Are Employees' Rights and Employers' Responsibilities in Illinois?

BY MARA BALTABOLS, HANNAH MOSER, AND PATRICK COWLIN

IN MARCH 2021, GOVERNOR PRITZKER signed an amendment to the Illinois Human Rights Act (IHRA or the Act) that expanded protections for individuals with a conviction record. Prior to the amendment, the Act only protected people with arrests that had not resulted convictions from discrimination or retaliation at their job or when applying for jobs.

The Act now protects a person from being discharged, disciplined, denied employment, or denied promotions because of a conviction record without notice and an interactive assessment of whether there is a substantial relationship between the conviction and the job.[1, 2] Under the IHRA,

Continued on next page

BIPA Update

CONTINUED FROM PAGE 1

addressing the accrual of BIPA claims. See *Cothron v. White Castle System, Inc.,* 216 N.E.3d 918 (Ill. 2023). In *Cothron,* a plaintiff filed a class action alleging that his employer violated BIPA by failing to obtain a written release before implementing a policy requiring its employees to scan their fingerprints to clock in and out of their shifts. White Castle moved to dismiss the plaintiff's claims as time-barred under the statute, arguing the plaintiff's claims accrued in 2013, five years after BIPA was enacted into law, and when the plaintiff's first actionable biometric scan would have occurred.

The Illinois Supreme Court, however, sided with the plaintiff, who argued that a BIPA violation occurred each and every time employee biometrics were scanned and transmitted to third-party data processors. The Court reasoned that because BIPA contained no text limiting accrual to the first scan, each subsequent scan embodied a separate violation, thus extending the limitations period and significantly increasing the possible liability of employers and private entities defending against BIPA claims. The Court's ruling acknowledged the potential for ruinous outcomes for defendants facing BIPA liability under this holding but called upon the legislature to implement necessary changes to the statutory language. In the meantime, courts had discretion to tailor damage awards to provide fair compensation to class members while preserving BIPA's deterrent effect without destroying defendants with heavy penalties.

Illinois Legislature Responds to *Cothron* with S.B. 2979

S.B. 2979 effectively overrules the Illinois Supreme Court's ruling in *Cothron.* The amendment specifies that BIPA damages accrue just once, regardless of how many scans were collected in a single case.

The amendment also permits entities to collect consent using digital technology rather than written releases, an issue not previously addressed under BIPA.

However, it is important to note that the amendment does not address retroactivity. S.B. 2979's prohibition on per-scan damages arguably should apply to pending BIPA claims since the amendment evidences legislative intent to curtail multiplicative damages on a per-scan basis. However, the issue is not yet settled. We will monitor how Illinois courts address this question in the amendment's aftermath.

Conclusion

The BIPA amendment is an important development in Illinois law protecting employers from extreme legal outcomes. It still remains, however, that the statutory damages imposed under BIPA are harsh and have the potential for significant impact on employers and other private entities that collect and use biometric data. ■

Susan Lorenc is a Thompson Coburn Partner serving as Vice-Chair of Thompson Coburn's Labor and Employment Department and leading Thompson Coburn's Labor and Employment Practice Group in Chicago. Susan also serves on Chicago Innovation's Board of Advisors.

Dremain Moore is an associate in Thompson Coburn's Business Litigation practice group specializing in breach of contract, products liability, and class action claims involving BIPA and similar statutes.

Brittney Mollman is a counsel in Thompson Coburn's Business Litigation practice group specializing in litigating cybersecurity, privacy, and data governance claims and emerging artificial intelligence issues.

Elizabeth Casale is an associate in Thompson Coburn's Business Litigation practice group specializing in antitrust, corporate governance, and cybersecurity, privacy, and data governance issues.

Originally published: https://www.thompsoncoburn.com/insights/publications/item/2024-08-16/bipa-update-illinois-adopts-reform-limiting-potential-claims-(and-damages)-in-litigation

Privacy & Information Security Law

This is the newsletter of the ISBA's Privacy & Information Security Law Section. Section newsletters are free to section members and published at least four times per year. Section membership dues are $35 per year.

To subscribe, visit www.isba.org/sections or call 217-525-1760.

OFFICE
ILLINOIS BAR CENTER
424 S. SECOND STREET
SPRINGFIELD, IL 62701
PHONES: 217-525-1760 OR 800-252-8908
WWW.ISBA.ORG

EDITOR
Michelle R. Ratledge

COMMUNICATIONS MANAGER
Celeste Niemann
cniemann@isba.org

ART DIRECTOR
Ticara Turley
tturley@isba.org

PRIVACY & INFORMATION SECURITY LAW SECTION COUNCIL
Tatyana L. Ruderman, Chair
Rita W. Garry, Vice-Chair
Aaron W. Brooks, Ex-Officio
Monique A. Anawis
Elizabeth R. Bacon
Mara A. Baltabols
Jason S. Bartell
Daniel M. Bronke
Fariz Mohammed Burhanuddin, Esq
Jo Ann Dominguez
Brian Eaton
Keith E. Emmons
John M. Fitzgerald
Gabrielle Nicole Ganze
Jennifer L. Gordon
David P. Hennessy
Rick L. Hindmand
Neil Patrick Johnson
Nicole E. Kopinski
Ambrose V. McCall
Dremain Taylor Moore
Jeremy Oehmen
Clayton Read Pasley
Michelle R. Ratledge, Newsletter Editor
David P. Saunders
Rachel Schaller
Ari J. Scharg
Bryan Paul Thompson
Sofia M. Zneimer
Mark C. Palmer, Board Liaison
Alonzo Alexander, Staff Liaison
Kelly L. Garrett-Hicks, CLE Committee Liaison

DISCLAIMER: This newsletter is for subscribers' personal use only; redistribution is prohibited. Copyright Illinois State Bar Association. Statements or expressions of opinion appearing herein are those of the authors and not necessarily those of the Association or Editors, and likewise the publication of any advertisement is not to be construed as an endorsement of the product or service offered unless it is specifically stated in the ad that there is such approval or endorsement.

Articles are prepared as an educational service to members of ISBA. They should not be relied upon as a substitute for individual legal research.

The articles in this newsletter are not intended to be used and may not be relied on for penalty avoidance.

Discrimination Based on Conviction Records

CONTINUED FROM PAGE 1

a "conviction record" includes information showing that a person has been convicted of a felony, misdemeanor, or other crime, placed on probation, fined, imprisoned, or paroled by any law enforcement agency or military authority.

Background checks raise privacy and security concerns. Once an employee is offered employment, with the employee's permission, their employer may request a copy of the conviction history report. The report is generated through various background check companies that compile background check information for employers. Although these companies must comply with the requirements of the Fair Credit Reporting Act (FCRA), requirements that have been in place for years, complying with the FCRA does not equal compliance with IHRA. The IHRA's protections for disclosure and consideration of conviction record information by employers add another layer employers must be aware of. Yet, despite the IHRA's expanded and publicized protections from discrimination based upon conviction records, many employers do not know or are wholly dependent upon the background check companies to provide disclosures to applicants.

Having a conviction record can significantly inhibit an individual's opportunities for employment, and the Act now aims to curb unfair practices employers may have used to exclude people with conviction records from the workforce. Being unable to get or keep a good job negatively impacts individuals who may be returning from prison or other restrictions. Studies have shown that securing employment after a conviction leads to many benefits for the individual, including an increase in self-esteem, a positive sense of identity, and ultimately, a more stable lifestyle.[3] Unemployment can significantly contribute to re-offending, while stable jobs for incarcerated individuals decreases recidivism rates.[4]

Communities also benefit when people with a criminal record find good jobs. Poverty rates decrease, taxes are collected on earned income, and families are strengthened as the collateral effects of incarceration and crime are minimized.[5]

Further, the poor job prospects for people with conviction records are a genuine economic concern, as an estimated 70 million people, or one in three adults in the United States, have a prior arrest or conviction record.[6] Employing individuals with conviction records also has benefits for employers. It provides employers with evidence of nondiscriminatory hiring practices, potentially qualifies employers for tax credits and free bonding services, expands small applicant pools, and reduces training costs, especially when hiring candidates who have completed specialized job training while incarcerated.[7]

Even though Illinois has taken tangible steps to address this problem by restricting an employer's utilization of criminal backgrounds, many companies do not comply with this important law. Often, employers will automatically deny or disqualify a candidate based on a conviction record without proper interactive process or notice. More on that below.

Any lawyer representing employers, employees, or in any practice intersecting with the criminal justice system should be aware of what the IHRA requires when an employee or prospective employee has a conviction record.

First off, people with convictions are often turned down from jobs because of their background checks or prior conviction records. Under Illinois law, an automatic rejection or termination based on a job applicant or employee's criminal history can violate the Illinois Human Rights Act. The employer must show a substantial relationship between the conviction and employment, such as a job provides an opportunity to the applicant to commit the same crime. Simply having a conviction record is not enough to deny employment.

Also, the new protections have been in place for quite some time. The Illinois Human Rights Act provides protections beginning March 23, 2021, for individuals who were denied employment or a promotion or discharged from employment because of a "conviction record" without notice or a complete "interactive assessment" as required by law.

A "conviction record: under the IHRA is limited to actual dispositions, and not arrests (which should not appear on an individual's conviction history report). A conviction includes but is not limited to, a felony, misdemeanor, probation, imprisonment, or parole. It may include guilty pleas or information that a person has been convicted of a felony, misdemeanor, or other criminal offense.[8]

An employer can only use a conviction record as a basis for an employment decision if there is either:

- a substantial relationship between one or more of the previous criminal offenses and the employment sought or held or
- the granting or continuation of the employment would involve an unreasonable risk to property or to the safety or welfare of specific individuals or the general public.

Additionally, the employer must have engaged in the interactive process to make this determination **and** properly given notice to the individual.[9]

For conviction record to be "substantially related" to the employment means that an employer can demonstrate that the position creates an opportunity for the employee to engage in the same or a similar criminal offense. Or that the circumstances leading to the conduct for which the person was convicted will also occur in the employment position. Showing that a conviction record poses an "unreasonable risk" means that before making a decision to bar employment, an employer must assess the risk that the employee poses to the workplace in the particular position and determine whether the risk is unreasonable under the circumstances.

The employer must engage in an "interactive assessment" to determine if there is a "substantial relationship" between

the conviction and the employment. One of the first and mandatory steps is for the employer to provide a preliminary decision with consideration of several mitigating factors. The mitigating factors include:

(1) the length of time since the conviction;
(2) the number of convictions that appear on the conviction record;
(3) the nature and severity of the conviction and its relationship to the safety and security of others;
(4) the facts or circumstances surrounding the conviction;
(5) the age of the employee at the time of the conviction; and
(6) evidence of rehabilitation efforts.[10]

The mitigating factors are typically considered after the employer as provided the preliminary decision to the applicant of the denial or withdrawal of employment. The employer or employment agency must provide notice of the decision and the reason for the denial. Then, the employee has five business days to respond. The applicant/employee as the opportunity to respond with mitigating factors. The employer must provide the employee with a notice of the decision, a copy of the conviction, the report relied upon, and an explanation of rights. Then, the employer may make a final decision.[11] The final decision must in writing and include:

(a) notice of the disqualifying conviction or convictions that are the basis for the final decision and the employer's reasoning for the disqualification;
(b) any existing procedure the employer has for the employee to challenge the decision or request reconsideration; and
(c) the right to file a charge with the IDHR.

Discrimination may result where the employer has failed to comply with the Act's requirements. Aggrieved employees may, on their own or with the assistance of an attorney, file a charge of discrimination with the Illinois Department of Human Rights. They should also consider seeing whether their criminal conviction can be expunged so that it may not appear on background checks in the future.

As a result of a violation, the employer or employment agency may be liable for damages directly resulting from the violation, including actual damages, emotional distress damages, injunctive relief, and attorney fees, and costs.

The IHRA also prohibits employers from taking any adverse action against an employee or prospective employee because of a pending arrest.[12] The analysis about whether there is a "substantial relationship" between the arrest and the job will not save an employer from potential liability. However, employers may obtain or use "other information which indicates that a person actually engaged in the conduct for which he or she was arrested."[13]

Employees and employers in Chicago and/or Cook County should be aware that local ordinances similar to the IHRA protect against discrimination based on employees' conviction record. Statutes of limitations and deadlines may be different under Illinois law. In Chicago, for example, employees have 365 days to file a complaint with the Chicago Commission on Human Relations (not just the 300 days under the IHRA).

Certain employer practices that exclude employees or applicants due to arrests or convictions may constitute intentional or unintentional, but still illegal, race discrimination. Due to historical and continuing systemic race discrimination and segregation in the United States, minority citizens are disproportionately more likely to have an arrest or conviction record. Therefore, an employer's purported neutral policy that, for example, excludes applicants from employment based on certain crimes being on their record may disproportionately impact protected classes and violate Title VII and the IHRA if the neutral policy is not job related and consistent with business necessity.[14] National data supports a finding that policies excluding applicants and/or employees with criminal records from employment have a disparate impact based on race and national origin.[15] This is otherwise known as "disparate impact" discrimination.

Hopefully, with continued outreach and education about the conviction record amendment and its implications, compliance with the law will become more consistent. Quality, stable employment is an unmatched factor in rehabilitating individuals with conviction records and decreasing recidivism. The benefits of increasing employment opportunities for individuals with conviction records are seen on an individual and community level. As mentioned previously, employers also stand to benefit from continued and expanded compliance with this section of the IHRA.

Illinois attorneys can do their clients and their communities a great service by helping enforce, or comply, with the conviction record protections in the IHRA. Feel free to send any questions to the authors. ■

Authors Mara Baltabols (mara@fishlawfirm.com) and Hannah Moser (hmoser@fishlawfirm.com) are attorneys with Workplace Law Partners, P.C. based out of Chicago and Naperville. Their practices focus on complex litigation primarily representing employees in discrimination, wage and hour, and privacy issues in the workplace – including those related to employees' arrest or conviction records.

Author Patrick Cowlin (pcolwlin@hq-law.com) is a shareholder at Hawks Quindel, S.C., based out of Chicago. Patrick Cowlin is a Shareholder at Hawks Quindel, S.C., and recently helped open the firm's first Chicago office. He exclusively represents employees and whistleblowers in class action and individual cases, including those involving discrimination, retaliation, wage and hour issues, and individuals discriminated against because of their arrest or conviction records.

---

1. 775 Ill. Comp. Stat. Ann. 5/2-103.1
2. Illinois Department of Human Rights, "Conviction Record Protection – Frequently Asked Questions" https://dhr.illinois.gov/content/dam/soi/en/web/dhr/filingacharge/documents/il-sb1480-conviction-record-protections-faq-from-idhr.pdf
3. Parker, Kelly, "Employment after Prison: The Importance of Supporting Workers Who are Seeking Work after Incarceration" https://www.ncda.org/aws/NCDA/pt/sd/news_article/476831/_PARENT/CC_layout_details/false
4. Office of Justice Programs, Bureau of Justice Statistics, "Employment And Expenditure." Available at: https://www.bjs.gov/index.cfm?ty=tp&tid=5
5. Parker, Kelly, "Employment after Prison: The Importance of Supporting Workers Who are Seeking Work after Incarceration" https://www.ncda.org/aws/NCDA/pt/sd/news_article/476831/_PARENT/CC_layout_details/false
6. National Employment Law Project, "Ensuring People With Convictions Have A Fair Chance to Work" https://www.nelp.org/campaign/ensuring-fair-chance-to-work/
7. Parker, Kelly, "Employment after Prison: The Importance of Supporting Workers Who are Seeking Work after Incarceration" https://www.ncda.org/aws/NCDA/pt/sd/news_article/476831/_PARENT/CC_layout_details/false
8. 775 Ill. Comp. Stat. Ann. 5/1-103 (G-5)
9. 775 Ill. Comp. Stat. Ann. 5/2-103.1(A)(1)-(2)
10. 775 Ill. Comp. Stat. Ann. 5/2-103.1(B)(1)-(6)
11. 775 Ill. Comp. Stat. Ann. 5/2-103.1(C)
12. 775 ILCS 5/2-103.
13. 775 ILCS 5/203(B).
14. https://www.eeoc.gov/laws/guidance/enforcement-guidance-consideration-arrest-and-conviction-records-employment-decisions
15. *Id.*

7 Questions to Ask Before Giving a Vendor Access to Your Data Set in an Artificially Intelligent World

BY TATYANA RUDERMAN

IN 2024 WE HAVE SEEN MANY VOICES enter the chat on how to approach AI governance, globally and locally. One thing is clear: the time to begin addressing AI compliance is yesterday, and the considerations below are a good place to start.

To start thinking about what more you may need to do, we present you with 7 questions to ask before handing over access to your data set.

Question 1. What Are My Legal Obligations?

Regulations that specifically target artificial intelligence/machine-learning or certain automated decision-making technologies are quickly evolving, but use of these Big Data technologies is nothing new – and already regulated under existing laws. AI/ML technologies, including discriminatory AI, have long been used in analytics or similar internal business tools to help study and analyze data, make predictions, automate processes, provide fraud detection, and help overall improve a company's products and services. There is no doubt that use of such AI tools provides great value to businesses.

However, under recent and new guidance and legal frameworks, certain tools/vendors may require more compliance before implementation, particularly for use of emerging AI/ML technologies like generative AI (genAI), including large language models (LLMs), and now large vision models (LVMs). As a very distilled list, ongoing, specific regulation of AI/ML focuses on requirements for AI governance (programs and documentations, risk assessments, training), transparency (notice to end users, labeling, documentation), accountability (registration, third party review), and individual rights (opt out/appeal, nondiscrimination).

Recent regulation includes:

- The EU AI Act;
- US state AI Acts (such as in Colorado and Utah); and
- Massachusetts' AI Advisory.

Use of AI tools to process personal data will trigger requirements under US and international comprehensive privacy laws, including transparency requirements, data minimization/retention standards, data access/deletion rights, etc. US state privacy laws already specifically govern certain aspects of AI. These state privacy laws currently exist in California, Colorado, Connecticut, Virginia, Utah, and Florida. And soon in Texas, Oregon, and Montana. Among other requirements, they require proper disclosures, consents, and opt-out rights for users when making AI-powered decisions that grant or deny financial or lending services, insurance, housing, health care services, employment, educational opportunities, or basic necessities. Certain states also impose additional requirements. For example, Colorado requires disclosure of: (1) the logic and training used to create the AI tool; (2) whether the AI tool has been evaluated for accuracy, fairness, and bias; and (3) why the AI tool must be used. California is proposing additional regulations that will likely place similar transparency requirements on businesses.

Examples of other official statements, advisories, and industry guidance include:

- NIST's AI Risk Management Framework (AI RMF);
- A joint statement by US federal agencies (the CFPB, DOJ, EEOC, and FTC) emphasizing that aspects of AI systems are governed by existing laws (such as laws governing discrimination, deception, and privacy);
- President Biden's Advisory on AI; and
- Legal/industry group frameworks (such as from the World Economic Forum and CARU's guidelines on AI-generated children's advertisements and data collection).

Taking advantage of the hottest/most exciting vendor solutions is very difficult to navigate as technologies evolve far more quickly than laws and few truly have knowledge of and understand exactly how each tool is built/how it works, and there is a lack of clear, cohesive legal guidance. Yet, companies that deploy AI tools are responsible not only for their own compliance, but also for ensuring their use of AI is ethical.

Question 2. Have I Double Checked Whether the Data Processing Involves Use Of AI/ML/Automated Decision-Making Technology?

Guidance around use of artificial intelligence/machine-learning or automated decision-making tools remains quite murky and in-flux. There is even a lack of consensus around the definitions of what is AI/ML. Because of how many nuances there are to this question, evaluating vendor tools must be done on a case-by-case basis.

As mentioned above, you may be surprised to find that many of your vendors do indeed use technologies or sub processors that integrate some degree of AI/ML or automated decision-making technology, based on how these are defined across various laws and guidance (such as tools that involve basic automation or analytics). Use of such AI tools is also growing in areas where automated decision-making allows for more efficiency, such as entering or analyzing data, providing customer service, and managing inventory.

In evaluating a vendor, it will be very important to consider how the vendor views themselves and their services – and

bear in mind that a vendor's silence on the topic speaks volumes. To evaluate this, ask:

- Does the vendor represent to have a robust compliance program in place? Certain vendors acknowledge and address their use of AI tools on their websites, in technical documentation, FAQs, contractual terms, etc., which may help assure you they are well aware of the legal and regulatory frameworks governing their services and compliance obligations.
- Are references to AI/ML or automated technologies buried in the contract or technical documentation, or not acknowledged at all? For others, it may take more digging to understand how their solution works and whether it involves use of AI/ML/automated decision learning, and even more work to get on the same page about how to delineate contractual obligations.

Question 3. Is the Vendor's Tool Subject to Special Regulation?

Depending on the specific context, the use of AI/ML or automated decision-making tools alone may not rise to the level where they now require additional compliance beyond what is required for your privacy and data security compliance – this very much depends on the very specific context of how the tool is used.

At a very high level, additional AI-specific regulation will mostly impact AI solutions that do more than simply automate – you will want to pay extra attention whenever individual data is involved to train AI, particularly that which is "sensitive" (such as health data, biometrics, precise location), where there is a type of processing considered more "high risk", or where the tool makes consequential/significant decisions (such as making employment or financial decisions).

Different rules and degree of regulation will apply depending on: whether you are a developer (*e.g.* vendor or business building the AI/ML tool), deployer (*e.g.* the business implementing a tool in its product), or user of AI (*e.g.* personnel), what industry you are in (for example, several state bar associations (such as California and Florida) have issued guidance to attorneys on how to reasonably use AI in accordance with professional responsibility requirements), and of course, what jurisdictions you are in.

Question 4. What Data Is Being Inputted Into The AI/ML System and How Much of It?

Personal Data & Consent. Data used to train AI systems must be collected and processed in compliance with all laws. To ensure this, you'll need to understand exactly what data types will be input to the AI tool. Depending on the context, direct consent from users may be needed. If sensitive data (including certain demographic data, biometrics, health data, children's data, or precise geolocation), or potentially sensitive (like photos/videos) is used this will require a higher level of notice and consent as there is a focus on enforcement surrounding "high risk processing activities" (and you may also need to consider compliance under other existing frameworks, such as for biometrics or children's data). If only "anonymous" data is being used, make sure that means it is truly anonymous, subject to the strictest applicable standards and that it would not otherwise be possible for the AI tool to re-identify an individual based on patterns gleaned from other data types.

Data Minimization/Retention Requirements. The amount of data processed within the tool must align with data minimization and limitation principles and must be deleted in accordance with retention schedules and policies. This requires a careful and critical inquiry, and documentation, to assess the minimum amount of data reasonably necessary to provide the service (to avoid other potential harms associated with AI like bias, this will require a lot of data) – note data minimization standards are becoming even stricter under certain forthcoming US states laws such as Maryland.

Question 5. What Data Comes Out of the AI/ML Process?

Consequential/Significant Decisions. It will be key to understand at a baseline how the tool produces outputs – in particular where the output involves consequential/significant decisions impacting an individual – in order to transparently explain this to end users (for example, if required, to explain the logic behind how the AI system arrives at its conclusion), to feel confident that the tool works as intended (for example, that it accurately makes its predictions), among many other considerations.

Privacy Exposing Inferences. AI-powered outputs become data you hold and will be subject to your existing privacy and data security obligations. You will want to understand what data you can expect to receive from the AI tool. Is the output data more sensitive than the input data (for example, inferences drawn about a person's movements or activities that reveal health or mental status)? Is the data adequately protected from unauthorized access? Would you want your customers to know you hold this kind of data (for example, if you are required to produce it in response to an access request)?

Question 6. Can the Vendor Provide Proper Assistance to Help You Comply with Existing and Coming Laws and Regulatory Compliance Requirements That Govern Your Business?

Depending on the specific context, you'll need to make sure yours (or the vendors') standard contractual terms and privacy/data security attachments adequately address use of the tool, including any applicable privacy or data security requirements or AI-specific regulations.

It will be essential to evaluate exactly how the vendor will provide assistance in meeting your privacy and data security compliance obligations, for example, to handle a downstream consumer deletion request or to opt out of automated decision-making. The very nature of AI is at odds with certain privacy requirements and poses novel issues (for example, the

requirement to minimize data is at tension with AI's insatiable need for data to train its algorithms, and properly deleting data presents a challenge when that data has already been used to train AI).

You'll want assurance that your vendor will be a helpful and forthcoming partner in helping you navigate these complicated issues.

Question 7. What Are the Potential Harms to Your Business and End Users? Does the Use of This Technology Align with Business Branding and Strategy?

Deploying certain new technologies that involve AI/ML or automated decision-making can pose fairly significant risks to your business, or potential harm to end users and/or society. Before engaging a vendor, you'll want to generally assess whether the benefit of the tool is worth the potential risks, and consider what steps need to be taken to protect against core AI risks and harms, such as to avoid algorithmic bias and discriminatory impact in the AI outputs. Mitigate some of these risks by seeking input from multiple stakeholders to ensure use of the tool aligns with business goals, strategy, and branding. This should include product owners, procurement, IT/security, information systems, legal, marketing, and any other key roles – and be sure to document this input and how it was addressed.

As a few examples of potential enforcement, the FTC has pursued several cases against companies for alleged unlawful use of AI, with penalties including algorithmic disgorgement (such as this settlement with Rite Aid, and AI has been the subject of various class actions (for example, a proposed class action against Home Depot and Google). Texas has released a statement indicating it will aggressively enforce its consumer protection laws (including its privacy law that governs AI). Maintaining documentation of the involvement of key stakeholders will help offset some of these risks – to avoid or mitigate such investigation or enforcement by being able to demonstrate due diligence and responsible practices around use of these AI/ML and automated decision-making tools. ■

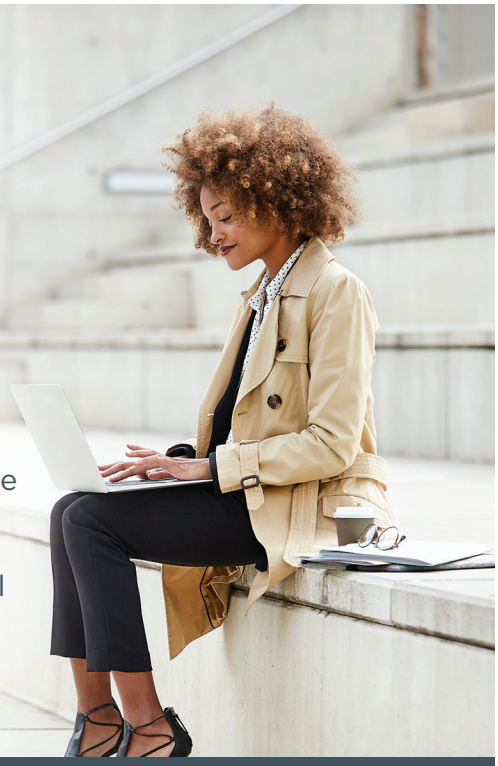
Originally published on: https://www.infolawgroup.com/insights/2024/6/27/7-questions-to-ask-before-giving-a-vendor-access-to-your-data-set-in-an-artificially-intelligent-world

ILLINOIS LAWYER NOW
Presented by the Illinois State Bar Association

CALLING ALL LEGAL BLOGGERS!

Are you an ISBA member with a legal blog? The ISBA wants to help elevate your content and make it available to a wider audience through Illinois Lawyer Now.

Be a part of one of the **FIRST** state bar-sponsored legal blog aggregation sites!



Joining is easy and **FREE**, simply fill out the quick form at **IllinoisLawyerNow.com/join**

Business Data Privacy Standards and the Impact of Artificial Intelligence

BY RITA W. GARRY

IN AN ERA WHERE DATA IS OFTEN likened to the new oil, its management, protection, and ethical use have become paramount concerns for businesses worldwide. As businesses harness the power of artificial intelligence (AI) to derive insights and streamline operations, the need for robust data privacy standards and effective governance frameworks has never been more critical.

The Importance of Data Privacy Standards

Data privacy standards are regulatory frameworks that govern how organizations collect, store, use, and share personal and sensitive information. These standards vary globally, with regulations such as the General Data Protection Regulation (GDPR) in Europe, the amended California Consumer Privacy Act (CCPA), and 18 other U.S. States' consumer data protection and rights legislation, it is clear laws and regulations worldwide are setting stringent guidelines for data handling practices.

Businesses adhering to these standards not only mitigate legal risks but also build trust with their customers. Trust is increasingly becoming a competitive differentiator in today's digital landscape where data breaches and misuse incidents dominate headlines. Implementing robust data privacy measures ensures that businesses protect sensitive information, maintain customer confidence, and avoid costly penalties associated with non-compliance.

Artificial Intelligence and Data Governance

Artificial intelligence technologies, including machine learning and natural language processing, have revolutionized how businesses analyze and utilize data. AI systems can process vast amounts of information at unprecedented speeds, uncovering patterns and generating insights that drive strategic decisions and operational efficiencies.

However, the use of AI introduces complexities to data governance. Traditional data governance practices focused on managing structured data within defined schemas. AI, on the other hand, thrives on vast swaths of information and can generate entirely new data. This surge in AI sophistication and the growth of transformational technologies creates unique challenges for governance frameworks.

Challenges in AI-driven Data Governance

- Data Quality and Bias: AI models are only as good as the data they are trained on. Biases inherent in training data can perpetuate inequalities or produce inaccurate results, undermining the reliability and fairness of AI applications.
- Interpretability and Transparency: AI algorithms often operate as "black boxes," making it challenging to understand how decisions are made. Lack of transparency can hinder accountability and compliance with regulatory requirements for data usage.
- Security and Privacy Risks: AI systems require access to large datasets, raising concerns about data security and privacy. Ensuring data protection throughout the AI lifecycle—from collection and processing to storage and disposal—is crucial to mitigate risks.

Integrating Data Privacy with AI

To address these challenges, businesses must integrate data privacy principles into their AI strategies from the outset. These involve:

- Privacy by Design: Embedding privacy considerations into the design and development of AI systems ensures that data protection measures are built-in rather than retrofitted.
- Ethical AI Frameworks: Establishing guidelines for ethical AI usage promotes responsible data stewardship and mitigates risks associated with bias, discrimination, and privacy violations.
- Compliance Monitoring: Implementing mechanisms to monitor AI systems for compliance with data privacy regulations and ethical standards ensures ongoing adherence to best practices.

The Future of Data Governance in AI

As AI continues to evolve, so too must data governance frameworks. Future advancements in AI technologies, such as federated learning and differential privacy, hold promise for enhancing data privacy while preserving the utility of AI applications. Collaborative efforts between businesses, policymakers, and technology experts are essential to navigate these complexities and ensure that AI-driven innovation benefits society responsibly. Prominent AI governance efforts are happening now and on a worldwide scale. These efforts are reflected in baseline use principles, AI laws and regulations, AI governance frameworks, declarations and voluntary commitments, and standards efforts.

Conclusion

In conclusion, while artificial intelligence offers unprecedented opportunities for business innovation and growth, its adoption necessitates a reevaluation of data privacy standards and governance practices. Businesses that prioritize data privacy, transparency, and ethical AI usage not only safeguard against regulatory scrutiny and reputational damage but also foster trust and loyalty among customers. By embracing a proactive approach to data governance in the age of AI, businesses can unlock the full potential of their data assets while upholding principles of privacy and accountability in a rapidly evolving digital landscape. ■

Author Rita W. Garry is an Attorney with Howard & Howard Attorneys PLLC. Ms. Garry is a seasoned corporate, transactional, artificial intelligence and data privacy attorney, the trusted legal advisor to a wide variety of business enterprises across industries, and a Certified Information Privacy Professional (CIPP/US).

Originally published in CPO Magazine at: https://www.cpomagazine.com/data-privacy/business-data-privacy-standards-and-the-impact-of-artificial-intelligence-on-data-governance/