```
e($repo_path."/config");if ($parse_ini['bare']) {$this->repo_path = $repo_
_path = $repo_path;if ($_init) {$this->run('init');}} else {throw new Excep
ow new Exception('"'.$repo_path.'" is not a directory');}} else {if ($creat
h))) {mkdir($repo_path);$this->repo_path = $repo_path;if ($_init) $this->ru
xistent directory');}} else {throw new Exception('"'.$repo_path.'" does not
git" directory) * * @access public * @return string */public function git_d
repo_path."/.git";}/** * Tests if git is installed * * @access public * @ret
=> array('pipe', 'w'),2 => array('pipe', 'w'),);$pipes = array();$resource
et_contents($pipes[1]);$stderr = stream_get_contents($pipes[2]);foreach ($pi
);return ($status != 127);}/** * Run a command in the git repository * * Acc
ommand to run * @return string */protected function run_command($command) {$
),);$pipes = array();/* Depending on the value of variables_order, $_ENV may
ables with * putenv, and call proc_open with env=null to inherit the reset *
store just those * variables afterwards. * * If $_ENV is not empty, then we
env = NULL;foreach($this->envopts as $k => $v) {putenv(sprintf("%s=%s",$k,$v
po_path;$resource = proc_open($command, $descriptorspec, $pipes, $cwd, $env);
1]);$stderr = stream_get_contents($pipes[2]);foreach (
;if ($status) throw new E
```

# REGULATING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

BY
HEATHER EGAN
SUSSMAN

&
IAN
ADAMS

&
NUR
LALJI

Heather Egan Sussman is a partner at Orrick, Herrington & Sutcliffe LLP, and head of the firm's Strategic Advisory and Government Enforcement Business Unit.  Ian Adams is a public policy attorney at Orrick, advising clients on matters at the intersection of law, business and public policy. Nur Lalji is an associate in ORrick's Cyber, Privacy & Data innovation Practice Group.

TechREG CHRONICLE
FEBRUARY 2023

## REGULATING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

By Heather Egan Sussman, Ian Adams & Nur Lalji

Artificial Intelligence ("AI") and machine learning ("ML") have the potential to create breakthrough advances in a range of industries, but they also raise novel legal, ethical, and privacy questions that will likely define the next era of technological advancement. Over the last several years, there has been a flurry of AI- and ML-related regulations and guidance issued by international bodies, governments, and regulators seeking to mitigate the risks posed by AI and ML, especially when these technologies are used to make important decisions related to employment or healthcare. Given the proliferation of these technologies across various industries, more regulation is likely to come. Organizations with AI and ML-based products and services should understand and consider how existing laws apply to them, as well as how the changing regulatory landscape may impact their business plans going forward. In this article, we discuss the differing approaches to regulating AI and ML in Europe and at the federal and state levels in the United States and the best practices for building compliance.

# 01 INTRODUCTION

AI and ML are considered some of the most important technological developments in recent years, and their use across a myriad of industries has exploded over the past decade. A 2022 survey by NewVantage Partners found that nearly 92 percent of executives said their organizations were increasing investments in data and AI systems and 26 percent of companies already have AI systems in widespread production.

Perhaps what is most compelling about AI and ML from a business perspective is its potential to make organizations more efficient and data driven in their decision-making. Specifically, the use of ML algorithms makes it possible for organizations to ingest huge amounts of data, identify patterns, and create rules that enable the machine learning model to make automated decisions and provide an output to the organization that otherwise may have been either too time or capital intensive. However, there is real risk that the power of AI and ML may be misused. In order to mitigate the potential for harm at the hands of AI and ML systems, there is increasing pressure for regulatory oversight. Over the last two years, policymakers and regulators, from international bodies to municipal governments, have begun to focus on the potential for AI applications to cause harm. The increasing drum beat of regulation of AI and ML on both sides of the Atlantic makes clear that the global race to regulate AI and ML has begun in earnest.

Compliance (and noncompliance) with these regulations may have a steep cost for businesses. AI and ML touch on many aspects of the regulatory tapestry in the U.S. and abroad — privacy, security, employment, civil rights, regulation of BigTech, and beyond. The potential for large fines, lawsuits, and regulatory investigations makes it essential for organizations to build a risk and governance strategy that explicitly accounts for AL and ML-related activities. In fact, it may be necessary to consider structural modifications within firms to identify an individual or cross-functional committee to take responsibility over AI and ML compliance.

In this article, we (i) identify some of the novel legal, ethical, and privacy issues that AI and ML present; (ii) evaluate the differing approaches to regulating AI and ML in Europe and at the federal and state levels in the United States; and (iii) discuss considerations for building an effective risk management and governance strategy.

# 02 LEGAL, ETHICAL, AND PRIVACY CONCERNS

AI and ML systems present novel legal, ethical, and privacy challenges. For example, these systems can produce unintentionally biased outputs based on bias inherent in the data they ingest or the algorithms that processes the underlying data. This can produce discriminatory or otherwise negative outcomes. Additionally, due to the large troves of data these systems require, the use of AI and ML is also often at odds with privacy and consumer protection principles. We discuss each of these in turn.

### *A. Bias in AI*

In 2018, researchers Joy Buolumwini and Timnit Gebru exposed the inherent biases in the facial recognition models across several major technology companies. According to their study, *Gender Shades*, these companies' facial recognition technologies were significantly more likely to misidentify women and individuals with darker skin tones.[2] These disproportionate error rates were reportedly produced, in part, because of the training data fed to the model — which was predominantly white and male.[3] This study, and others like it, show the often unintended but discriminatory consequences of AI and ML systems that are not carefully reviewed by diverse and cross-disciplinary teams of engineers, data scientists, compliance professionals, and lawyers that are tasked with considering the ethical use of AI and ML.

Moreover, although AI and ML has often been touted as a neutral solution, often, the inverse is true — without human intervention, these models may reflect back historic biases that had previously gone undetected. Amazon, for example found that the algorithms it developed for hiring were disproportionately disadvantaging women. This was reportedly because the algorithms were trained on resumes submitted to Amazon in the previous ten years, which disproportionately "came from men, a reflection of male dominance across the tech industry."[4] One can easily see how companies utilizing AI and ML in their hiring processes may unintentionally produce similar effects if there are not adequate safeguards in place to review the underlying data and the algorithm and remove inherent biases.

[2] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81:1–15 (2018).

[3] *Id.* at 3.

[4] Jeffrey Dastin, Amazon scraps secret AI recruiting tool that showed bias against women, Reuters (October 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

These examples showcase how important it is for organizations to audit their training set data and algorithmic outputs to account for unintentional results, such as the incomplete or inaccurate representation of a particular group or a legally protected class. It is worth noting that mitigating biases of this type has been the impetus for several regulatory proposals, many of which center around audit requirements that would result in the proliferation of disparate impact tests — an outcome many companies are likely to find problematic.[5] However, companies that pro-actively endeavor to address such issues and seek to promote transparency at a high level in how their AI and ML systems operate, may inoculate themselves from the worst scrutiny.

### *B. Privacy and AI*

There is an inherent tension between privacy and AI. Privacy laws generally promote the concept of "data minimization," which stands on the principle that organizations should limit their collection of personal information to only that which is directly relevant and necessary to accomplish the purpose for which the personal information was collected for in the first place. From a consumer protection standpoint, principles of lawfulness, fairness, and transparency are also key, meaning that individuals should be provided with information and afforded meaningful choices with regards to how their personal information is collected and used. AI and ML systems, however, need to be trained with large amounts of data, and they improve as more data is fed to them. This friction has led some business to obfuscate how they use personal information to train their AI and ML models, with consumers only learning about this data usage after the fact.[6]

Despite these inherent challenges, only 44% of executives said their organizations have well-established policies and practices to support data responsibility and AI ethics.[7] Nonetheless, the legal landscape surrounding AI and ML has changed dramatically in recent years, and new laws seek to protect consumers from these legal and ethical harms.

## 03
## LEGAL LANDSCAPE

In the spring of 2021, the European Commission (the "Commission") published its highly anticipated communication and "Proposal for a Regulation laying down harmonized rules on artificial intelligence" (the "EU AI Regulation").[8] The EU AI Regulation was released just days after the Federal Trade Commission (the "FTC") published a blog post entitled "Aiming for truth, fairness, and equity in your company's use of AI" (the "2021 FTC Memo").[9] Additionally, there have been a flurry of AI and ML-related action from U.S. regulatory agencies, state governments vis-à-vis privacy laws, and U.S. city governments relating to the use of AI and ML for employment decisions.[10]

### *A. Europe*

The European Commission proposed the EU AI Regulation in the spring of 2021 to harmonize AI rules across the continent. The EU AI Regulation takes a risk-based approach to controls on using AI and ML systems, depending on the intended purpose of the system. The EU AI Act proposes a sliding scale of rules based on risk that would classify different AI and ML applications as unacceptable, high, limited, or minimal risks.[11]

[5] See, e.g. U.S. EEOC, Artificial Intelligence and Algorithmic Fairness Initiative, https://www.eeoc.gov/ai (Last accessed Jan. 23, 2023); New York City Council, Automated Employment Decision Legislation, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9&Options=Advanced&Search; Algorithmic Accountability Act of 2022, congress.gov/bill/117th-congress/house-bill/6580/text; American Data Privacy and Protection Act of 2022, https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[6] See, e.g. Alex Hern, TechScape: Clearview AI was fined £7.5m for brazenly harvesting your data – does it care?, The Guardian (May 25, 2022), https://www.theguardian.com/technology/2022/may/25/techscape-clearview-ai-facial-recognition-fine.

[7] Tam Habert, *Regulations Ahead on AI*, SHRM (April 2, 2022), https://www.shrm.org/hr-today/news/all-things-work/pages/regulations-ahead-on-artificial-intelligence.aspx.

[8] European Commission, *Proposal for a Regulation laying down harmonized rules on artificial intelligence (April 21, 2021)*, digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

[9] Press Release, Federal Trade Commission, Aiming for truth, fairness, and equity in your company's use of AI (April 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

[10] AI and ML are dependent on huge data sets which can include personal information, including sensitive personal information. Consequently, privacy laws have become a primary means to address the risks inherent in relying on AI to make decisions that have legal and social consequences such as loan approvals or employment decisions.

[11] Press Release, Orrick, The New EU Approach to the Regulation of Artificial Intelligence (May 7, 2021), https://www.orrick.com/en/Insights/2021/05/The-New-EU-Approach-to-the-Regulation-of-Artificial-Intelligence.

The EU AI Regulation is intended to have extraterritorial effect and establishes the European Artificial Intelligence Board that will have significant authority to levy "dissuasive" fines for noncompliance of up to 6% of annual global turnover for certain breaches, as well as the power to order AI and ML systems to be withdrawn from the market. The inclusion of these GDPR-like penalties shows that the EU is serious about regulating the burgeoning AI and ML industry. The EU AI Regulation applies across all sectors (public and private) to "ensure a level playing field." On December 6, 2022, the European Council adopted its common position on the Artificial Intelligence Act.[12] The adoption of this approach enables the Council to enter negotiations with the European Parliament once the European Parliament adopts a position on the proposed regulation. Negotiations are expected to be complex with thousands of amendments already proposed by political groups in the European Parliament.

The EU AI Regulation will become law once both the European Commission and the European Parliament agree on a common version of the text and will enter into force 24 months after that date, though some provisions may apply sooner. If enacted, the regulation would have significant consequences for organizations that develop, sell, or use AI or ML systems. Those consequences include the introduction of legal obligations and a monitoring and enforcement regime with hefty penalties for non-compliance. Specifically, organizations will be required to register standalone high-risk AI or ML systems, such as remote biometric identification systems, in an EU database. Potential fines for noncompliance range from 2-6% of a company's annual revenue. The regulation has striking similarities to the General Data Protection Regulation, or GDPR, which already carries implications for AI as Article 22[13] prohibits decisions based on solely automated processes that produce legal consequences or similar effects for individuals unless the user has explicitly consented, or the AI or ML system meets other requirements.

The proposed EU AI Regulation will have a significant impact on any organization that operates anywhere in Europe or targets the European market. It is likely that the regulation of AI will follow a path similar to the evolution of data privacy regulations where the sweeping regulations that start in the EU cause other jurisdictions to follow that lead. In the United States, a patchwork of local, state, and federal regulations, guidance, and frameworks have already emerged in the wake of the EU AI Regulation and do not appear to be losing steam.

> *"The proposed EU AI Regulation will have a significant impact on any organization that operates anywhere in Europe or targets the European market*

***B. United States***

Unlike the comprehensive framework proposed in Europe, regulatory guidelines have generally been proposed on an agency-by-agency basis in the United States, as well as regulation at the state and local levels.

1. National AI Initiative Act

In January 2021, the National AI Initiative Act (the "U.S. AI Act")[14] became law creating the National AI Initiative that provides "an overarching framework to strengthen and coordinate AI research, development, demonstration, and education activities across all U.S. Departments and Agencies." The U.S. AI Act created new offices and task forces aimed at implementing a national AI strategy, implicating a multitude of U.S. administrative agencies including the FTC, Department of Defense, Department of Agriculture, Department of Education, and the Department of Health and Human Services.

2. Algorithmic Accountability Act of 2022

The Algorithmic Accountability Act (the "AAA")[15] of 2022 was introduced on February 3, 2022, by Sen. Ron Wyden, Sen. Cory Booker, and Rep. Yvette Clark. The bill is likely to be reintroduced in a substantially similar form in the new Congress and would require large technology companies across the states to perform a bias impact assessment of any

[12] Press Release, Council of the EU, Artificial Intelligence Act: Council Calls for Promoting Safe AI that Respects Fundamental Rights (December 6, 2022), https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/#:~:text=The%20Council%20has%20adopted%20its,fundamental%20rights%20and%20Union%20values.

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal information and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) GDPR Article 22, https://gdpr-info.eu/art-22-gdpr/.

[14] National AI Initiative Act of 2020, https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210.

[15] Algorithmic Accountability Act of 2022, congress.gov/bill/117th-congress/house-bill/6580/text.

automated decision-making system that makes critical decisions in a variety of sectors, including employment, financial services, healthcare, housing, and legal services. The Act's scope is potentially far reaching as it defines "automated decision system" to include "any system, software, or process (including one derived from ML, statistics, or other data processing or artificial intelligence techniques and excluding passive computing infrastructure) that uses computation, the result of which serves as a basis for a decision or judgment." Notably, significant sections of the Act as introduced in 2022 were incorporated into the "three corners" privacy bill (known as the ADPPA) that will function as the basis for future efforts to develop a national digital privacy standard.[16]

3. <u>Department of Commerce</u>

A flurry of AI-related activity has emanated from the Department of Commerce, including a move towards a risk-management framework. Congress has directed the National Institute of Standards and Technology, part of the Commerce Department, to develop "a voluntary risk management framework for trustworthy AI systems." That framework may greatly influence how organizations approach AI-related risks, including avoiding bias and promoting accuracy, privacy, and security.

In September 2021, the Department of Commerce established the National Artificial Intelligence Advisory Committee[17] to advise the president and federal agencies. It will offer recommendations on the "state of U.S. AI competitiveness, the state of science around AI, issues related to the AI workforce" and how AI can enhance opportunities for underrepresented populations, among other topics. Given its responsibilities and engagement with AI, the Department of Commerce appears poised to play a central role in the federal approach to AI regulation.

4. <u>Federal Trade Commission</u>

The FTC has also made it clear that it will use its power under Section 5 of the FTC Act, the Fair Credit Reporting Act, and the Equal Credit Opportunity Act to help ensure AI is used truthfully, fairly, and equitably in the United States.

> *"In September 2021, the Department of Commerce established the National Artificial Intelligence Advisory Committee to advise the president and federal agencies*

The 2021 FTC Memo discussed above made clear that the FTC will marshal its resources to pursue the use of biased algorithms. The FTC provided a roadmap for its compliance expectations and organizations should "keep in mind that if you don't hold yourself accountable, the FTC may do it." Among other things, organizations should:

· Rely on inclusive data sets: "Companies should think about ways to improve their data set, design their model to account for data gaps, and — in light of any shortcomings — limit where or how they use the model."
· Test an algorithm before use and periodically afterwards "to make sure that it doesn't discriminate based on race, gender, or other protected class."
· Be truthful about how they use customers' data and don't exaggerate an algorithm's abilities.
· Embrace transparency and independence.[18]

In June 2022, the FTC indicated that it plans to submit an Advanced Notice of Preliminary Rulemaking to "ensure that algorithmic decision-making does not result in harmful discrimination."[19] Also in June 2022, the FTC issued a report to Congress discussing how AI may be used to combat online harms, ranging from scams, deep fakes, and opioid sales.[20] However, the report sought to strike a balance and noted that AI is also susceptible to producing biased and discriminatory outcomes.

[16] American Data Privacy and Protection Act of 2022, https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[17] Press Release, Department of Commerce Establishes National Artificial Intelligence Advisory Committee (September 8, 2021), https://www.commerce.gov/news/press-releases/2021/09/department-commerce-establishes-national-artificial-intelligence.

[18] Press Release, Federal Trade Commission, Aiming for truth, fairness, and equity in your company's use of AI (April 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

[19] FTC Plans to Submit an Advanced Notice of Preliminary Rulemaking ("ANPRM") "under section 18 of the FTC Act to curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination." https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=3084-AB69.

[20] Federal Trade Commission Report to Congress, *Combatting Online Harms Through Innovation* (June 16, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf.

5. <u>The White House</u>

The E.U.-U.S. Trade and Technology Council has committed[21] to develop "AI systems that are innovative and trustworthy and that respect universal human rights and shared democratic values." The council also plans to discuss "measurement and evaluation tools. . . to assess the technical requirements for trustworthy AI" and study the technology's impact on the labor market.

In November 2021, the White House Office of Science and Technology Policy solicited engagement[22] from stakeholders across industries in an effort to develop a "Bill of Rights for an Automated Society." Such a Bill of Rights could cover topics like AI's role in the criminal justice system, equal opportunities, consumer rights, and the healthcare system.

6. <u>Food and Drug Administration</u>

The Food and Drug Administration (the "FDA") issued Artificial Intelligence/Machine Learning Based Software as a Medical Device ("SaMD") Action Plan to outline its proposed steps for creating a regulatory framework "that would allow for modifications to be made from real-world learning and adaptation, while ensuring that the safety and effectiveness of the software as a medical device are maintained."[23] The Action Plan outlines how the agency intends to oversee development and use of the software in the SaMD context.

7. <u>National Security Commission and Government Accountability Office ("GAO")</u>

The National Security Commission on Artificial Intelligence submitted its final report to Congress in 2021. It recommends the government take domestic actions to protect privacy, civil rights, and civil liberties in its AI deployment. It notes that a lack of public trust in AI from a privacy or civil rights/civil liberties standpoint will undermine the deployment of AI to promote U.S. intelligence, homeland security, and law enforcement. The report advocates for public sector leadership to promote trustworthy AI, which will likely affect how AI is deployed and regulated in the private sector.

Also in 2021, the GAO identified practices to help ensure accountability and responsible AI use by federal agencies. The report identified four key focus areas:

- Organization and algorithmic governance
- System performance
- Documenting and analyzing data to develop and operate an AI system
- Continuous monitoring and assessment to ensure reliability and relevance over time.

> ***Also in 2021, the GAO identified practices to help ensure accountability and responsible AI use by federal agencies***

8. <u>EEOC</u>

In May 2022, the U.S. Equal Employment Opportunity Commission (the "EEOC") released a guidance[24] warning to U.S. companies that their use of algorithmic decision-making tools to assess job applicants and employees could violate the Americans with Disabilities Act by intentionally or unintentionally screening out individuals with disabilities when utilizing algorithms in the hiring process.

9. <u>NIST</u>

The National Institute of Standards and Technology ("NIST"), which falls under the U.S. Department of Commerce, is currently engaging with stakeholders to develop "a voluntary risk management framework for trustworthy AI systems."[25] Additionally, in September 2021, NIST released a paper describing its Principles on Explainable AI.[26] Under these non-binding principles, AI algorithms should:

[21] Press Release, U.S.-EU Trade and Technology Council Inaugural Joint Statement (September 29, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/.

[22] Press Release, Join the Effort to Create A Bill of Rights for an Automated Society (November 10, 2021), whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/.

[23] Press Release, Artificial Intelligence and Machine Learning in Software as a Medical Device (January 2021), https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.

[24] Press Release, The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees (May 12, 2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.

[25] NIST AI RISK MANAGEMENT FRAMEWORK (August 18, 2021), https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf.

[26] NIST Four Principles of Explainable Artificial Intelligence (September 29, 2021), https://www.nist.gov/publications/four-principles-explainable-artificial-intelligence.

· Have accompanying evidence or reason(s) for all outputs;
· Be understandable to individual users;
· Correctly represent how system generates the output;
· Have confidence in output and only operate in the conditions for which it was designed.

10. State Privacy Laws

Because AI and ML are dependent on huge data sets which may include personal information, U.S. state privacy laws have become one of the means to mitigate risk. These laws, which include the California Privacy Rights Act (the "CPRA"), the Colorado Privacy Act (the "CPA"), the Virginia Consumer Data Protection Act (the "VCDPA"), and the Connecticut Data Privacy Act (the "CTDPA"), seek to put the consumer in control of their personal information and ensure that AI is used in a responsible manner. However, they also create new obligations for organizations to assess and potentially comply with, and also are structured in a way that poses unique challenges in the AI and ML context.

(i) Obligations for AI and ML Systems Use

Each of the state privacy laws grant consumers rights regarding opting out of the processing of their personal information for purposes of profiling and create requirements that impact automated decision-making. Though the definitions of automated decision-making and profiling differ slightly across the state privacy laws, profiling generally refers to an organization attempting to evaluate personal aspects of a data subject via the processing of their personal information. Relatedly, automated decision-making refers to an organization either (i) acting upon profiling to make a decision by automated means without human intervention or with limited human intervention or (ii) establishing an automated system that renders a decision based directly on information provided by a data subject (such as an age gate that would prevent anyone under a certain age from being able to participate in a program or apply for a position). Several of the state privacy laws also require data controllers to conduct a data protection impact assessment (a "DPIA") for processing activities that present a "heightened risk of harm" to a consumer.

(ii) Challenges with the privacy law framework

The state privacy laws generally split businesses up into two categories: entities that control the ways in which consumers' personal information is collected, used, and disclosed (i.e. that act as a "controller") and entities that assist these businesses and act as a "service provider" or "processor" on their behalf. Acting as a controller or service provider/processor come with varying obligations, risks, and benefits that organizations must consider. While conventional businesses may more naturally fit into one category or the other, businesses that use AI and ML systems may have a difficult time classifying themselves in accordance with these definitions.

> “*Because AI and ML are dependent on huge data sets which may include personal information, U.S. state privacy laws have become one of the means to mitigate risk*

For example, a SaaS-based vendor that uses AI and ML systems as part of their product offerings may generally consider themselves to be a service provider, but want to use the data they collect from their customers to improve their machine learning model. Where the data they receive from customers includes personal information, this provides a challenge under the state privacy law frameworks, as service providers are generally prohibited from using personal information for their own purposes.[27] Although certain privacy laws include exceptions to this requirement, such as permitting service providers to use personal information purely for their own internal purposes, use of personal information to train and improve a machine learning model does not clearly fit within this exception, as that data may be combined with other datasets and used for the benefit of other customers.[28] Practices such as deidentifying and aggregating personal information may solve part of this problem, it may not provide a workable solution for all vendors, such as where their model may be predicated on the use of the personal information to provide the service. In addition, customers themselves may be hesitant to allow the personal information they provide to a vendor to be used to enhance the vendor's machine learning model, even where such information is deidentified. As such, businesses that use AI and ML will need to think carefully about how they classify themselves under the privacy law framework and develop their compliance strategy with this classification in mind.

All of the state privacy laws come into effect at varying points in 2023. Accordingly, the compliance obligations and the potential for increased regulatory scrutiny in the U.S. will increase significantly in the coming year. For more infor-

[27] See, e.g. CCPA Draft Regulations, § 7051(a).

[28] CCPA Draft Regulations, § 7050(a)(3).

mation about how state privacy laws will affect AI, see our Orrick's Insight, "New State Privacy Laws Zero in on AI."[29]

11. New York City's Biometric Data Protection Law

On July 9, 2021, the New York City Biometric Identifier Information Law (the "NY Biometric Act")[30] went into effect. The NY Biometric Act applies to the collection and processing of "biometric identifier information," which is defined as "physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual." The NY Biometric Act identifies a retina or iris scan, a fingerprint or voiceprint, and a scan of hand or face geometry as examples of biometric identifier information. The NY Biometric Act only applies to a "commercial establishment," defined as a place of entertainment, a retail store, or a food and drink establishment.

There are two primary legal requirements: (i) commercial establishments that collect, retain, or share a customer's biometric identifier information must disclose these activities "by placing a clear and conspicuous sign near all…customer entrances notifying customers in plain, simple language." The NY Biometric Act does not require commercial establishments to obtain any type of written consent from consumers either before or even after their biometric data is collected; and (ii) commercial establishments cannot "sell, lease, trade, share in exchange for anything of value or otherwise profit from the transaction of biometric identifier information."

The NY Biometric Act includes a private right of action under which individuals can recover damages of $500 per violation for an establishment's failure to post a conspicuous notice, $500 for each negligent violation of the ban on the sale or sharing of biometric data, and $5,000 for each intentional or reckless violation of the ban on selling or sharing biometric identifier information.

Additionally, New York City has passed the first law[31] in the United States that will require employers to conduct audits of automated decision-making tools used to evaluate job candidates or employees (the "New York City Automated Employment Decision Law"). The law, which took effect in January 2023, calls for audits of tools that automatically screen job candidates. Failure to comply with the law may result in the imposition of civil penalties of up to $500 for a first violation and each additional violation occurring on the same day as the initial violation, and between $500 and $1,500 for each subsequent violation. The law specifies that "[e]ach day on which an automated employment decision tool is used" in violation of the provision requiring a bias audit "shall give rise to a separate violation." Additionally, the failure to provide any of the required notices constitutes a separate violation.

While the New York City Automated Employment Decision Law applies only to employers in New York City, it's likely to have a much broader impact as large companies that hire employees in New York will likely be forced to update their hiring systems across the board to meet the floor established by the legislation.

# 04

# NEXT STEPS: WHAT SHOULD ORGANIZATIONS DO?

The regulation of AI and ML will continue to be a rapidly developing area of law. To mitigate the risk of legal liability and "future proof" compliance efforts, organizations are wise to build a compliance framework that focuses on predictability and transparency, as well as continuous auditing, refining, and monitoring with programmatic modification of AI and ML systems as appropriate. This can include:

- Crafting policies and procedures to create a compliance-by-design program that promotes AI innovation while ensuring transparency and explicability. In practice, this may involve the development of first-order principles that inform more granular practical guidance, including methods for human intervention where appropriate.
- Instituting cross-disciplinary teams of engineers, compliance and legal professionals, relevant executives, HR professionals, and members from across the organization to recognize problematic applications of AI and ML and cure such applications in a responsible and efficient manner.
- Developing privacy-forward solutions to data usage where possible, such as:
    - Deidentify and anonymize personal data when possible;
    - Create methods for removal of personalized information from machine learning models upon request;

[29] Press Release, Orrick, New State Privacy Laws Zero in on AI (August 11, 2022), https://www.orrick.com/en/Insights/2022/08/New-State-Privacy-Laws-Zero-in-on-AI.

[30] New York City Biometric Identifier Information Law, https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCadmin/0-0-0-42626.

[31] New York City Council, Automated Employment Decision Legislation, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9&Options=Advanced&Search.

- o Enact notice and consent frameworks for the use of individuals' sensitive personal information within the machine learning context.

· Implementing rigorous testing and review practices designed to identify, analyze, and address patterns and outcomes, all focused on continuous improvement.

· Documenting these processes to comply with regulators who may seek further information.

Taking these steps will not only help to future proof compliance efforts as AI and ML regulation continues to develop over the coming months and years, but it will also provide the evidence to show regulators, investors, and the public alike that responsible AI and ML is a top priority. Orrick has assembled further resources about steps organizations can take to maximize the benefits of AI while minimizing regulatory risk.[32] ■

[32] Press Release, Orrick, AI Tips: 10 Steps to Future-Proof Your Artificial Intelligence Regulatory Strategy, (July 1, 2021), https://www.orrick.com/en/Insights/2021/07/AI-Tips-10-Steps-to-Future-Proof-Your-Artificial-Intelligence-Regulatory-Strategy.

# CPI
# SUBSCRIPTIONS

CPI COMPETITION POLICY® INTERNATIONAL