ChatGPT

AI Legislation in the United States and Minnesota: Current Landscape and Future Outlook

Current Federal AI Legislation and Policy

At the federal level, there is **no single comprehensive law specifically regulating AI** in the United States. Instead, the U.S. has taken a patchwork approach: existing laws and agency powers are being applied to AI, and new AI initiatives have mostly come through strategic laws or executive actions rather than broad regulation [1] [2]. Key elements of the current federal landscape include:

- **Strategic R&D Laws:** The *National AI Initiative Act of 2020* (enacted Jan 2021) expanded support for AI research and established a National AI Initiative Office to coordinate a national strategy [3]. Similarly, recent laws like the CHIPS and Science Act (2022) fund AI research and semiconductor development, indirectly shaping AI progress. These laws promote **AI development and innovation** but do not impose new restrictions on AI deployment.

- **Executive Orders and White House Initiatives:** Federal AI policy has been guided by executive actions. In **February 2019**, the Trump Administration launched the *American AI Initiative* via Executive Order 13859, emphasizing R&D investment, resources, and "removing barriers" to AI innovation [1]. In **December 2020**, Executive Order 13960 on *Trustworthy AI in Government* set principles for federal agencies using AI (like transparency, fairness, and security in government AI systems). More recently in **October 2023**, President Biden issued *Executive Order 14110* on **Safe, Secure, and Trustworthy AI**, a sweeping directive engaging over 50 federal agencies and more than 100 actions across eight policy areas [4] [5]. This 2023 order calls for: bolstering AI **safety and security** research, supporting **innovation and competition** (attracting talent and protecting intellectual property), assessing **AI's impact on workers**, addressing **AI bias and civil rights** risks, enforcing **consumer protection** using existing laws, evaluating **privacy** risks, improving **federal government's own use of AI**, and leading in **international AI standards** [5] [6]. Together, these orders signal a federal policy of encouraging AI advancement while beginning to put guardrails around issues of safety, bias, and security.

- **Blueprint for an AI Bill of Rights:** In October 2022, the White House Office of Science and Technology Policy released a non-binding **"Blueprint for an AI Bill of Rights,"** outlining five principles for AI systems: (1) **Safe and Effective Systems**, (2) **Algorithmic Discrimination Protections**, (3) **Data Privacy**, (4) **Notice and Explanation**, and (5) **Human Alternatives** [7]. While this blueprint is guidance (not law), it reflects federal priorities for **AI ethics and accountability**. Agencies are encouraged to adopt these principles, and they have influenced proposed legislation and agency rulemaking efforts.

- **Sector-Specific Regulations and Agencies:** Instead of an AI-specific regulator, various federal agencies oversee AI within their domains using existing statutes:

- *Healthcare:* The **Food and Drug Administration (FDA)** treats certain AI software as medical devices and has approved a growing number of AI-enabled tools (nearly 500–1000 devices) under its medical device authority [8]. The FDA is evolving guidelines for machine-learning medical systems (e.g. how algorithms can update). This provides oversight of AI in **medical diagnostics, imaging, and healthcare** for safety and effectiveness.
- *Finance:* Financial regulators like the **Federal Reserve, SEC, and CFPB** monitor AI in credit, banking, and trading. For example, the **Securities and Exchange Commission (SEC)** has proposed rules on AI in brokerage (to prevent conflicts of interest in automated investment advice) [9]. The **Consumer Financial Protection Bureau (CFPB)** enforces fair lending laws on credit algorithms, and the **U.S. Treasury** has issued a fintech AI framework for banking. These ensure AI in **financial services** complies with anti-discrimination, fairness, and transparency requirements under existing law.
- *Employment/Hiring:* The **Equal Employment Opportunity Commission (EEOC)** and Department of Justice have warned that AI hiring and HR tools can violate equal employment and disability laws. In May 2022, the EEOC and DOJ released guidance that AI hiring tools could unlawfully "screen out" people with disabilities, violating the ADA [10] [11]. In 2023 the EEOC issued guidance on preventing **disparate impact** bias from AI in recruiting or promotions [12] [11]. While not new law, these guidances signal that **anti-discrimination laws (like Title VII and ADA) apply to AI** used by employers.
- *Consumer Protection:* The **Federal Trade Commission (FTC)** has taken an active stance that it can penalize unfair or deceptive AI practices under its broad consumer protection mandate. The FTC warned that selling "inaccurate or biased" AI or making deceptive AI performance claims can violate the FTC Act [13]. It has already brought enforcement actions – for example, it banned a major pharmacy chain from using facial recognition AI in stores without safeguards [14]. The FTC's posture means companies deploying AI must ensure **truthful marketing, fairness, and security**, or face liability under existing consumer protection law.

- *Other domains:* Agencies like the **Department of Transportation** (for autonomous vehicles), **Department of Defense** (for military AI ethics), and **Federal Communications Commission** (which ruled AI-generated robocalls fall under robocall bans [15]) are each addressing AI within their remit. This multi-agency oversight creates a de facto regulatory patchwork for AI until broader legislation arrives [16] [17].

- **Pending Federal Bills:** Congress has introduced numerous AI-related bills, though none have become law yet. Recent proposals target specific concerns: e.g. the *REAL Political Advertisements Act* would mandate disclosures for AI-generated deepfakes in election ads [18], the *No FAKES Act* would protect individuals' likeness from AI replication [19], an *AI Accountability Act* was proposed to require assessments of high-risk AI systems [20], and the leading privacy bill (American Data Privacy and Protection Act drafts) includes provisions giving consumers rights to opt out of automated decision-making [21]. While bipartisan interest is high, Congress has so far taken a cautious approach – many bills emphasize voluntary standards or further study, reflecting concerns about stifling innovation [22]. **No overarching AI regulatory framework has passed** as of 2025, but these bills indicate the directions federal law may soon take (transparency requirements, risk assessments, algorithmic discrimination rules, etc.).

In summary, current federal AI governance relies on **executive guidance and existing law**: encouraging innovation in AI, **applying current laws to new AI uses**, and developing **principles for trustworthy AI**. The U.S. has intentionally not yet enacted a sweeping AI-specific law (unlike the EU's approach), focusing instead on targeted interventions (e.g. an executive order on AI safety, or an agency enforcing sectoral

rules) [1] [23]. However, mounting concerns about AI risks are prompting ever-more federal action, as discussed in later sections on recent trends and anticipated developments.

AI Legislation and Initiatives in Minnesota

Minnesota's state government has begun actively grappling with AI through a mix of **legislation and executive initiatives**, though as of 2025 it, like most states, has not passed a comprehensive AI regulatory framework. Key Minnesota actions include:

- **Facial Recognition and Biometrics (Enacted 2020):** Minnesota was an early mover in regulating law enforcement's use of AI-powered surveillance. In 2020, the state enacted a law prohibiting law enforcement from using drones equipped with facial recognition or other biometric-matching technology **without first obtaining a warrant** [24]. This law creates a privacy safeguard around AI-driven surveillance, ensuring any use of facial recognition by police is subject to judicial oversight. (At the local level, Minneapolis went even further, passing a 2021 city ordinance banning its police from any use of facial recognition technology [25].) These steps reflected concerns about **privacy and accuracy** of early AI surveillance systems.

- **Deepfakes and Synthetic Media (Enacted 2023, Amended 2024):** In 2023, Minnesota's legislature unanimously passed a law addressing malicious **"deepfakes."** The law defines a "deep fake" as a video, image, or audio that realistically depicts someone saying or doing something they never did, using technical means (AI) to fabricate it [26]. The 2023 law made it a crime to use deepfake technology to **influence an election** (e.g. creating fake videos of a candidate) within 90 days of Election Day without a disclosure, with intent to injure a candidate or deceive voters [27]. It also criminalized non-consensual **sexual explicit deepfakes** – making or distributing fake pornographic images or videos of someone without consent is now illegal in Minnesota [28] [29]. In 2024, lawmakers further **strengthened the deepfake law** via HF 4772 [30]. The amendment broadened the election deepfake ban (applying it to primaries and convention campaigns, and requiring any candidate who violates it to forfeit their nomination or office) and adjusted the legal standard to make prosecution easier (changing from "reasonable knowledge" to **"reckless disregard"** as the standard for knowing a media is AI-generated) [31]. With these moves, Minnesota has one of the more robust state legal frameworks addressing **AI-generated disinformation and impersonation**, reflecting bipartisan concern over AI's impact on elections and privacy.

- **AI in Insurance and Consumer Protection (Proposed 2025):** Minnesota is now considering novel AI regulations in sector-specific contexts. For example, in 2025 legislators introduced **SF 1856**, a bill that would **prohibit the use of AI in health insurance utilization review** processes [32]. Utilization review (the process insurers use to approve or deny medical treatments) could not be delegated to AI algorithms under this proposal, indicating lawmakers' concern that automated decisions might unfairly deny care. Another bill, **SF 1886**, was introduced in 2025 to promote **AI transparency in consumer interactions** [33]. This bill would require businesses to **disclose to consumers when they are communicating with an AI system** (via chatbots or voice systems) and not a human [34]. It also would forbid companies from misleading consumers that an AI is human, and require offering an option to switch to a human representative [35]. If enacted, it would empower individuals to know when AI is involved (e.g. in customer service chats) and give them an opt-out, with enforcement by the Minnesota Attorney General and civil penalties up to $5 million for violations [36]. These proposed laws show Minnesota's focus on **AI accountability and transparency** to

protect consumers in sectors like insurance and retail communications. *(As of early 2025, these bills are in committee and have not yet become law.)*

- **AI Impact Studies and Task Forces:** Minnesota's legislature has also explored studying AI's broader impacts. A 2023–24 proposal (A49/S6402 in New York – similar proposals have been seen in MN as well) would create a **state commission to study AI, robotics, and automation** governance [37]. In Minnesota, SF 1117 (2025) was introduced to mandate a study on the **environmental impacts of AI** in the state [38]. While these have not advanced far, they indicate interest in formally assessing AI's implications. At this time, Minnesota has not established a permanent statewide AI commission, but the legislature's directives for reports and the convening of working groups are possible precursors to more concrete regulatory frameworks.

- **Executive Branch Framework – TAIGA:** In addition to legislation, Minnesota's executive branch is proactively developing an AI governance framework for state agencies. In 2023, Minnesota IT Services (MNIT, the state's IT agency) convened the **Transparent Artificial Intelligence Governance Alliance (TAIGA)** [39]. TAIGA is a cross-agency initiative to guide the **responsible use of AI in state government**, aiming to balance innovation with ethics and public trust [40]. In October 2023, TAIGA published a "Public AI Tool Security Standard" for state employees, which provides rules and example use-cases for tools like ChatGPT or Bard [41]. It defines what is permitted or prohibited when employees use public AI services, particularly to prevent sensitive or private data from being fed into these tools [42]. TAIGA has also set forth **guiding principles** for government AI use – emphasizing **accountability, transparency, equity, inclusivity, user-centered design, adaptability, privacy, and security** in any AI deployments [43] [44]. This internal governance effort does not impose requirements on private companies, but it positions Minnesota as a state trying to **"lead by example"** in ethical AI usage. By establishing standards and oversight for its own use of AI, Minnesota is laying groundwork that could inform future statewide policies or regulations.

In sum, **Minnesota's current AI-related laws** have tackled *specific, high-profile issues* (deepfakes, biometric surveillance) and the state is now moving toward broader **transparency and accountability measures** (in consumer protection and insurance). While Minnesota has not yet passed a general AI regulatory act, the legislative interest in 2025 is high. The combination of targeted laws and the TAIGA governance framework suggests Minnesota is building capacity to address AI's risks and opportunities, even ahead of many other states. Policymakers are likely watching the outcomes of these initial laws and pilot programs as they consider more expansive AI regulations in the future.

Comparative State Landscape: Minnesota vs. Other States

Across the U.S., state governments have emerged as "laboratories" for AI policy in the absence of comprehensive federal regulation. Minnesota's approach in context shows both similarities and unique differences compared to other leading states like **California, New York, Illinois, Texas,** and the newly active **Colorado**. Many states have passed narrow laws on specific AI applications (especially related to biometrics or employment), and a few are enacting broader AI governance frameworks. **Figure 1** below provides a snapshot of state AI legislation activity as of mid-2024, illustrating how widespread (or not) AI laws are across the country. States colored in dark blue have enacted AI laws and have additional proposals pending, green states have pending AI bills, orange states have enacted at least one AI-specific law, and grey states have not yet introduced AI legislation:

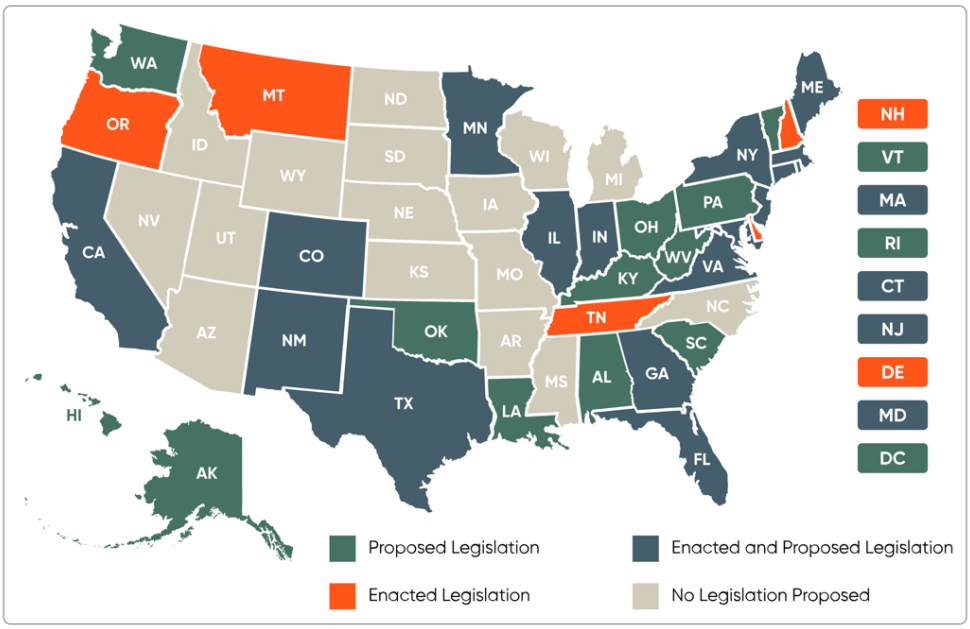

Figure 1: State AI Legislation Activity by mid-2024. Dark blue indicates states with both enacted and proposed AI laws, green indicates states with proposals pending (but no enacted AI-specific law yet), orange indicates states that have enacted at least one AI law, and grey indicates no AI bills proposed in that state as of 2024.

Minnesota, as discussed, has **enacted two AI-related laws** (biometric surveillance and deepfake bans) and is considering new bills in 2025, putting it in the company of many states that have a *few targeted AI laws*. In contrast, a few states have developed more comprehensive or aggressive AI regulatory regimes:

- **California:** California is at the forefront of state-level AI regulation, leveraging its role as a tech hub. It has approached AI primarily through the lens of **privacy, transparency, and consumer protection**. As early as 2019, California implemented a **"Bot Disclosure" law** (Bolstering Online Transparency Act) requiring that automated online accounts (bots) be identified as such when used to sell products or influence voting [45]. This was one of the first laws targeting AI-driven online interactions. California's broad privacy law, the CCPA as amended by CPRA, also addresses automated profiling – it gives consumers the right to know if significant decisions were made by algorithms and to opt out of certain types of automated processing [46] [47]. In 2023–2024, responding to the rise of generative AI, California's legislature passed **multiple AI bills**:
- *AB 2013* (2024) will require developers of generative AI to **publish documentation about the training data** used in their AI systems before making them available to the public [48]. This law (signed by Governor Newsom in Sept 2024) aims to increase transparency around the huge datasets that power generative models.
- *SB 942* – the **California AI Transparency Act** (2024) – will require large-scale AI systems (with over 1 million users in California) to **implement disclosure or watermarking for AI-generated content** [49] [50]. In effect, companies offering generative AI services in California must indicate when content (text, images, etc.) is AI-generated, to inform consumers [50] [51].
- *AB 294 (Definition of AI)* amended California law to formally define "artificial intelligence" for legal purposes [52], ensuring consistent terminology in statutes.
- Notably, California's legislature passed a high-profile bill (*SB 1047*, the **"Safe and Secure Innovation for Frontier AI Act"**) that would have imposed rigorous **safety, testing, and certification**

requirements on advanced AI models, somewhat akin to a mini–EU AI Act for frontier models [53]. However, in September 2024 Governor Newsom **vetoed SB 1047**, citing concerns that it might over-regulate and stifle innovation in the nascent AI industry [54] [55]. The veto message suggested that such AI governance might be better handled at the federal level, but Newsom did **sign the more targeted bills** (like AB 2013 and SB 942) into law [50]. California also has laws restricting government use of facial recognition and requiring audits of automated decision systems in specific contexts, but it has not yet enacted a single unified "AI Act."

- *Trend:* California's approach exemplifies a **focus on transparency, data governance, and specific high-risk AI uses (deepfakes, large models)**. The state is using its market power to force AI providers to be more open about their systems. We see California's strong consumer protection ethos extending into AI (much as it did with privacy). This contrasts with Minnesota, which has so far legislated more on misuse of AI (deepfakes) and specific agency uses, rather than broad transparency requirements on AI developers.

- **New York:** New York has made headlines via **New York City's pioneering AI ordinance** and is now expanding state-level oversight:

- *NYC Local Law 144 (2021)* – This NYC law (enforced from 2023) was the first in the nation to mandate **bias audits for automated employment decision tools (AEDTs)** used in hiring or promotions [56] [57]. It requires that companies using AI or algorithmic tools to screen job candidates must **conduct an annual independent audit for bias** (testing for disparate impact on race/gender) and **notify job applicants** about the AI use [56]. This law, though city-specific, positioned New York as a leader in tackling algorithmic bias in hiring, well before Minnesota or most states have addressed it.
- *State Proposals:* New York State has considered creating a **Temporary State Commission on AI, Robotics, and Automation** to study and recommend regulations (bill A9559/S8755 in 2023) [37]. While that commission was not yet established as of 2024, it signals New York's interest in a broader AI governance strategy. New York has also introduced bills to **ensure transparency in AI usage in insurance** (prohibiting unfair algorithmic factors in auto insurance pricing [58]), a "**Digital Fairness Act**" to mandate notice of personal data usage including algorithms [59], and even a recent requirement that companies report how many jobs are lost due to automation/AI in large layoffs (amending its WARN Act) [60]. That WARN Act amendment, passed in 2023, makes New York the first state to require firms to disclose when layoffs are attributable to AI automation – a move to track AI's impact on employment [60].
- *Deepfakes:* In 2023, New York also passed a law requiring any **AI-altered media in political ads to carry a disclaimer**, underlining concern similar to Minnesota's about AI and election integrity [61] (New York's approach is via disclosure, whereas Minnesota outright banned certain uses).

- *Trend:* New York's trajectory is to regulate **AI in hiring and the workplace**, and to set up governance bodies for broad policy. NYC's bias audit mandate is stricter than anything Minnesota currently has (Minnesota has no equivalent requirement on private employers). Minnesota, however, addressed deepfakes through criminal law, whereas New York has focused more on disclosure and civil oversight. Geographically, New York (like California) is more aggressive in consumer and civil rights aspects of AI, aligning with their general regulatory styles.

- **Illinois:** Illinois has built an early reputation in regulating technologies like biometrics, and it has extended that to AI in specific ways:

- Illinois's **Biometric Information Privacy Act (BIPA)** (2008) is not an AI law per se, but it heavily influences AI use of **facial recognition and fingerprints** by requiring consent and allowing lawsuits for misuse. BIPA's success (numerous lawsuits against tech companies) likely informed Illinois lawmakers on tech regulation.
- In **2020**, Illinois passed the **AI Video Interview Act**, one of the first laws addressing AI in hiring. This law requires employers who use AI analysis on video interviews to **notify applicants**, **obtain consent**, and **explain how the AI works** in evaluating the interview [62]. It also restricts how such interview videos can be shared. This targeted law predated NYC's broader AEDT law and gave candidates in Illinois some transparency and rights in AI-driven hiring processes.
- In **2023-2024**, Illinois took a further step with *HB 3773*, an amendment to the Illinois Human Rights Act. Signed in August 2024, this law (effective Jan 2026) will make it **unlawful for employers to use AI in hiring or employment decisions that results in discriminatory impact** on protected classes [63]. It basically adds AI outcomes to what counts as employment discrimination. It also **forbids using proxies like ZIP code** that could act as stand-ins for race in algorithms [64]. Employers in Illinois will have to notify applicants and employees if AI is used in making significant job decisions [65]. Unlike New York City's law, Illinois' statewide law does not mandate bias audits, but it flatly prohibits discriminatory AI practices and requires notice. Another pending bill in Illinois (HB 5116) has proposed **mandatory annual bias impact assessments for employers using AI**, though that one is still under debate [66].
- Illinois also recently joined states banning certain AI in insurance: a 2024 law disallows life insurers from using AI algorithms that incorporate facial analysis due to concerns over racial bias.

- *Trend:* Illinois has shown leadership in **AI in employment** and **biometric privacy**. It often is cited alongside California as having stringent tech laws. Minnesota's deepfake and police-drone laws actually resemble Illinois' style of addressing specific harms (Illinois also criminalized some deepfake pornography and requires disclosures for political deepfakes). However, Illinois' new employment AI discrimination ban goes beyond what Minnesota has considered so far. Regionally, Illinois positions itself as a Midwest leader on AI oversight, which could pressure neighbors like Minnesota to consider similar workplace protections in the future.

- **Texas:** Texas might be expected to take a light-touch approach, but it has surprisingly been active in certain AI regulations, balanced with pro-innovation moves:

- In **2019**, Texas became one of the first states to outlaw malicious deepfakes in politics, making it a crime to publish a deceptive deepfake video intended to injure a candidate within 30 days of an election [67]. This is very similar to Minnesota's 2023 election deepfake ban (Minnesota's covers 90 days prior). Texas in 2019 defined "deepfake video" in law and set penalties, indicating early recognition of the threat.
- In **2023**, Texas passed two laws targeting **non-consensual pornographic deepfakes**, criminalizing the production or distribution of fake intimate images without consent [68]. Again, this parallels Minnesota's approach and shows a common concern across red and blue states to protect individuals from AI-generated sexual harassment.
- Texas also led in **biometric data regulation** with a 2009 biometrics law (similar to Illinois BIPA) and continues to enforce it, impacting facial recognition uses.
- On the governance side, in 2023 Texas created an **Artificial Intelligence Advisory Council (HB 2060)** [69]. This council is tasked with evaluating the **need for a state AI code of ethics and reviewing the use of AI in state government** [69]. The Texas House Speaker in 2024 formed a

Select Committee on AI & Emerging Technologies, which delivered a report in May 2024 with policy recommendations [70]. These actions signal Texas' intent to craft a broader state AI strategy.

- Indeed, in late 2024 Texas lawmakers drafted a comprehensive bill, the **Texas Responsible AI Governance Act (TRAIGA)**, aiming to be introduced in 2025 [71]. According to reports, this draft Texas bill draws inspiration from the EU AI Act – it would **ban certain high-risk AI systems outright** (like social scoring or AI that manipulates behavior), require risk assessments for others, and generally set state-wide standards [72] [73]. If Texas enacts TRAIGA, it could become the most comprehensive AI law in the U.S. so far, covering both private and public sector AI deployment in the state.

- *Trend:* Texas thus far has a dual approach: **punish malicious AI uses (deepfakes)** to protect citizens, while **promoting a business-friendly AI ecosystem** through advisory councils rather than strict mandates (TRAIGA's fate in a business-heavy legislature will test this). Compared to Minnesota, Texas has a similar deepfake law and likewise is studying AI in government. But Texas is contemplating a broader regulatory framework sooner than Minnesota. Texas's large economy and tech sector (Austin) might drive it to set its own AI rules if federal action lags – potentially creating a different regional model (one perhaps more flexible or innovation-friendly) than California's or New York's.

- **Colorado:** Although not explicitly asked in the prompt, it's worth noting **Colorado** because it made news in 2024 by enacting the country's **first state-level "AI Act."** In May 2024 Colorado passed the **Colorado Artificial Intelligence Act**, which is a relatively comprehensive law focused on **automated decision-making systems** [74]. It defines "high-risk" AI systems (those that make consequential decisions affecting legal or employment rights, healthcare, finance, etc.) and imposes obligations on developers and deployers of such systems [75]. Notably, Colorado's law applies to *all* companies (no size threshold) using high-risk AI in the state, requiring features like **risk assessments and transparency reports**. This law will come into effect in 2025–26 and is seen as a state-level analog to proposals in Congress. Colorado also previously banned life and health insurers from algorithmic discrimination (2021's SB 169 [76]). Colorado's leap to a broader AI law has set a precedent other states are studying. For example, as noted above, a similar comprehensive bill in California (AB 331 in 2024) that started like Colorado's was later narrowed and then died [77], and Texas's draft bill appears to take a different approach.

In comparing these states, some **regional trends** emerge. **West Coast states (CA, WA)** often integrate AI rules into privacy and consumer protection laws (with an emphasis on transparency and risk mitigation), while **Northeastern states (NY, NJ)** lean towards task forces and anti-bias regulations, especially in hiring. **Midwestern states (IL, MN)** have zeroed in on biometrics, surveillance, and civil rights, leveraging existing tech laws (BIPA in IL, data practices in MN) to cover AI scenarios. **Southern states (TX, VA)**, traditionally less restrictive, are nonetheless addressing overt harms like deepfakes and looking at balanced frameworks to both promote AI industry growth and set basic guardrails.

It's also clear that **no single state has "solved" AI governance** – most are incrementally tackling the issue. By the end of 2024, an **overwhelming majority of states (at least 40+) had introduced AI bills**, and roughly one-third of states had passed some form of AI-related law [78]. In 2024 alone, lawmakers in **45 states introduced 635 AI-related bills, with 99 of those enacted into law** [79] – a massive jump from fewer than 200 AI bills the year before [80]. This explosion of state activity means Minnesota is one of many states navigating uncharted territory. The table below summarizes how Minnesota's efforts compare to a few peer states on key dimensions of AI legislation:

State	Key AI-Related Laws/Initiatives (as of 2025)
Minnesota	- *Facial Recognition & Biometrics:* Requires a **warrant for police use of facial recognition on drones** (2020) [24]. - *Deepfakes:* **Criminal ban on election deepfakes** and non-consensual sexual deepfakes (enacted 2023, amended 2024) [27] [81]. - *AI in Insurance:* Proposed ban on **AI for health insurance utilization reviews** (2025) [32]. - *AI Transparency:* Proposed **AI chatbot disclosure and human-alternative requirement** for businesses (2025) [34] [35]. - *Governance:* **TAIGA** executive initiative establishing AI use principles for state agencies (accountability, equity, transparency, etc.) [39] [82] and an AI usage standard for state employees [41].
California	- *Bot Transparency:* **Disclosure required** when bots interact with people for sales or political influence (BOT Act, effective 2019) [45]. - *Privacy & Profiling:* **CCPA/CPRA** gives consumers rights over automated decision-making and profiling (opt-out, access logic) [46]. - *Generative AI:* **Training data transparency law** (AB 2013, 2024) requiring AI developers to publish info on datasets [48]. - *AI Content Disclosure:* **Watermarking/labeling required** for AI-generated content from large platforms (SB 942, 2024) [49] [50]. - *Bias/Impact:* Considered (but did not pass) an **Algorithmic Discrimination bill** covering high-risk AI in employment (AB 2930) [77]. - *Governance:* Exploring a state **Office of AI**; Governor's 2024 directive launched new **initiatives for "safe, responsible AI"** after vetoing the broad AI bill [50].
New York	- *NYC Hiring Law:* **Bias audits and candidate notice required** for AI in hiring decisions (NYC Local Law 144, effective 2023) [56] [57]. - *AI Job Loss Reporting:* **Mandates disclosure of layoffs due to AI automation** in large companies (amendment to NY WARN Act, 2023) [60]. - *Deepfake Disclosure:* Requires **labels on AI-altered political campaign media** (2023 law for election communications) [61]. - *Proposed Commission:* Pending bill to create a **state AI ethics commission** to recommend regulation (A9559/S8755) [37]. - *Insurance/Finance:* Pending **ban on biased insurance algorithms** (no socio-economic proxies in underwriting) [58] and a **Digital Fairness Act** for algorithmic notice in consumer services [59].
Illinois	- *Biometric Privacy:* **BIPA (2008)** – strict consent and liability for collection of biometric data (fingerprints, face scans); indirectly constrains facial recognition AI use (many tech AI face tools avoided in IL due to BIPA). - *AI Video Interviews:* **Requires employer disclosure and consent for AI analysis of job interviews**; candidate can opt out (Illinois AI Interview Act, 2020) [62]. - *Workplace Bias:* **Prohibits AI-driven discrimination in employment decisions**; adds AI outcomes to civil rights protections (HB 3773, signed 2024, effective 2026) [63] [83]. Also requires **notice to employees/applicants** when AI is used in hiring or HR decisions [65]. - *Audits (Proposed):* Proposed bill to mandate **annual bias impact audits for automated hiring tools** (HB 5116) [66]. - *Sectoral:* Banned use of AI-driven credit scoring that acts as proxy discrimination; studying AI in healthcare diagnostics (several bills introduced in 2023 on AI in medicine) [84].

State	Key AI-Related Laws/Initiatives (as of 2025)
Texas	- *Deepfakes:* **Criminalized election deepfakes** (effective 2019) – illegal to publish deceptive AI-generated video of a candidate near an election [67] . **Banned AI "pornographic deepfakes"** without consent (2023) [68] . - *Biometric Privacy:* Texas has a BIPA-like **biometric law (2009)** requiring consent for facial recognition, voiceprints, etc., which underpins lawsuits against AI facial recognition companies. - *Advisory Council:* Created a **State AI Advisory Council (2023)** to develop an AI code of ethics for government and audit state agency AI use [69] . - *Legislative Committee:* House **Select Committee on AI (2024)** studied AI's impacts and recommended policies [70] (e.g. education, workforce training for AI, encouraging AI R&D hubs in Texas). - *Comprehensive Bill (Draft):* Considering the **Texas Responsible AI Governance Act (TRAIGA)** in 2025 – a proposal to regulate high-risk AI, ban certain harmful AI systems (e.g. social scoring), and require **reasonable safeguards by AI developers** [72] [85] . If passed, it would be one of the most extensive state AI laws, balancing innovation with risk controls.

Table 1: Comparison of Selected State AI Legislation and Initiatives. We see common threads (many states outlawing malicious deepfakes and addressing AI bias in hiring) but also unique approaches (e.g. California's focus on AI data transparency, Colorado's comprehensive act). Minnesota's current laws are on par with peers in addressing specific abuses of AI, and its proposed 2025 measures (AI disclosures, insurance AI ban) align with emerging trends in consumer protection. Unlike California or Colorado, Minnesota has not yet pursued an overarching AI regulatory framework, but its **TAIGA initiative** indicates a proactive stance in government use that few states (aside from perhaps Texas's council) have matched.

Recent Trends in AI Legislation (2020–2025)

The period **2020 through 2025** has seen a rapid evolution in how both federal and state authorities approach AI. What began with strategic plans and relatively few laws has transformed into a flurry of regulatory activity. Below is a timeline of major legislative and policy developments in AI over the last five years, highlighting both U.S. federal actions and Minnesota-specific milestones:

- **2020:** AI governance started to gain formal footing in the U.S. On the federal side, Congress passed the *National AI Initiative Act* as part of the FY2021 defense bill (signed January 2021) [3] . This law didn't regulate industry, but it created structures to coordinate AI research, set up an advisory committee, and called for an AI research resource task force. The Trump Administration also issued principles for federal agencies on AI regulation (Jan 2020 OSTP memo) emphasizing a light touch to avoid hampering innovation. In Minnesota, **SF 3072 became law (August 2020)**, making it one of the first states to restrict police use of AI surveillance by requiring warrants for drone-based facial recognition [86] . This reflected growing worries about algorithmic privacy violations. Elsewhere, Illinois's AI Video Interview Act took effect in 2020, and Texas enacted its political deepfake ban (a prelude of things to come nationwide).

- **2021:** The federal government ramped up coordination: the *National AI Initiative Office* was launched under the White House OSTP to implement the national R&D strategy. The *National Security Commission on AI* delivered its final report to Congress, urging the U.S. to accelerate both AI innovation and ethical safeguards (though this led to recommendations, not immediate legislation).

The Biden Administration signaled a different tone on AI – for example, in **June 2021**, the FTC issued guidance that it would go after biased AI under existing law, putting companies on notice. On the state side, **New York City passed its landmark AI hiring bias law in December 2021** [56], which put algorithmic accountability into city legislation for the first time in the U.S. Minnesota in 2021 did not pass new AI laws, but Minneapolis's city council ban on police use of facial recognition (Feb 2021) illustrated local concern after the George Floyd protests about surveillance tech. Nationally, 2021 was a year of **strategy and advisory actions** (federal) and **early local legislation** (NYC, a few states on facial recognition moratoria).

- **2022:** This year saw **principles and frameworks** emerge. In October, the White House released the **Blueprint for an AI Bill of Rights** [7], crystallizing ethical principles for AI – a notable federal acknowledgement of AI risks like discrimination and lack of transparency. Also, NIST (National Institute of Standards and Technology) began developing an **AI Risk Management Framework**, collaborating with industry to set voluntary standards for trustworthy AI (the final NIST AI RMF 1.0 would publish in January 2023). Enforcement of existing laws on AI picked up: the DOJ and EEOC issued guidance in May 2022 on avoiding AI-driven discrimination in employment (especially regarding disabilities) [10]. Meanwhile, Congress introduced the Algorithmic Accountability Act of 2022 (a bill requiring impact assessments for AI systems), and though it didn't advance, it garnered more support than its 2019 predecessor, showing growing legislative interest. In Minnesota, 2022 was relatively quiet legislatively on AI; however, the groundwork for TAIGA was being laid as MNIT recognized the need for a governance approach. Culturally, late 2022 was marked by the release of new powerful AI systems (e.g. OpenAI's ChatGPT in November 2022) which dramatically raised public and government awareness going into 2023.

- **2023:** *"The year AI went mainstream – and regulators took notice."* The emergence of generative AI (ChatGPT's popularity, new image generators) created a sense of urgency in Washington and state capitals. **Federal developments in 2023:** President Biden convened AI company CEOs in May to obtain voluntary **safety commitments** – by July 2023, leading AI firms (OpenAI, Google, Meta, etc.) pledged to implement security testing, share information on AI risks, and watermark AI content [87]. These were voluntary measures brokered by the White House as stopgap governance [88]. In Congress, Senate Majority Leader Chuck Schumer launched a high-profile series of AI Insight Forums (closed-door meetings) with tech leaders, researchers, and senators in fall 2023 [89]. This culminated in a bipartisan Senate **"SAFE Innovation" AI Framework** being released, outlining priorities for AI legislation (security, accountability, protecting foundations of democracy, etc.) [18]. Multiple Senate and House committees held AI hearings – including a notable Senate hearing where OpenAI's CEO Sam Altman testified and **called for AI licensing** of advanced models. By late 2023, Congress was crafting concrete proposals: e.g. a bipartisan bill to create a **Federal AI Commission** (an independent regulator akin to the FTC), and several narrow bills (on deepfake political ads, on requiring audits for bias, etc.). While none passed in 2023, the legislative momentum was the highest to date. The **Biden Administration's Executive Order on AI (Oct 30, 2023)** was a pivotal action [4]. It directed broad oversight measures: requiring developers of the most powerful AI models to **report their safety test results** to the government (using the Defense Production Act authority), initiating development of standards for AI watermarking, ordering the Dept. of Commerce to create guidelines for an AI **certification mark**, and tasking agencies like OSHA, EEOC, CFPB to issue policy guidance on AI in their domains [6] [90]. This EO also announced negotiations on a global code of conduct for AI and pushed for prioritizing AI in cyber defense and education. Essentially, by end of 2023 the U.S. federal government had moved from talk to actionable plans for

oversight – albeit via executive action due to no new law yet. **State developments in 2023:** Minnesota's deepfake law (Aug 2023) was part of a wave – several states (California, Texas, Washington) also passed laws or stiffened penalties for deepfake porn or election interference that year, indicating bipartisan agreement on that issue. States also took very different paths on AI in 2023: Colorado's legislature drafted its AI Act; California's legislature debated over a dozen AI bills (ultimately passing the four noted earlier); Connecticut and Virginia integrated AI provisions into their privacy laws (giving opt-outs for profiling); and some states launched task forces (e.g. North Carolina's AI committee, Vermont's AI commission). A standout event was **New York City's AI hiring law enforcement** starting in July 2023 – it caused many AI hiring tool vendors to scramble to get audits, and some employers paused use of resume algorithms, thus drawing national attention and influencing other states. By late 2023, at least **29 states had enacted some type of AI or automated decision-making law** (often small amendments or study requirements), demonstrating that 2023 was truly a turning point for AI governance across the board [78].

- **2024:** This year has been perhaps the most significant so far for AI legislation, both federally and in states, **marking a shift from planning to implementation**. On the federal front, early 2024 saw tangible outputs from 2023's groundwork: for instance, the **Congressional Research Service** published reports for lawmakers on AI policy options, the Senate's bipartisan AI Working Group released an AI legislative **"roadmap"** calling for ~$30 billion investment and new laws in specific areas (like requiring licenses for advanced AI, mandating AI transparency in critical uses, and aligning with EU standards). In April 2024, the **CRS "Highlights of the AI Executive Order"** report was delivered to Congress, summarizing the steps agencies are taking per Biden's EO [5] [6]. By mid-2024, some *narrow federal AI bills* started moving – for example, the **REAL Political Ads Act** (to require disclaimers on deepfake campaign ads) passed a committee with bipartisan support, given the impending 2024 elections and fears of AI misinformation. The FTC opened investigations into at least one AI company over consumer harm, signaling regulators weren't waiting for new laws to police AI. Meanwhile, **state legislation peaked in 2024**: as noted, 45 states introduced bills and 99 AI-related laws were enacted that year alone [79]. **Colorado's AI Act was signed into law in May**, making history as the first comprehensive state AI statute [74]. **California's legislature passed a slate of AI bills in August 2024**, and although the signature/veto outcomes were mixed (with the broadest bill vetoed [54]), California still ended up enacting the most state AI laws of any state that year. **Illinois' anti-AI-bias employment law was signed in August**, as discussed. **Minnesota in 2024** amended its deepfake law (May) and also quietly began implementing the TAIGA standards within state agencies. We also see emerging topics: *AI and intellectual property* became a hot topic (Congress held hearings on copyright of AI-generated art and whether AI training data usage should be exempt from copyright). *AI in education* prompted several states to consider bans or guidance on AI in schools (New York State Education Dept. issued guidelines for AI use in classrooms, etc.). By the end of 2024, it was evident that the **legislative momentum had dramatically accelerated** – what was once hypothetical discussion is now concrete statutes in many jurisdictions, and companies deploying AI across the U.S. face an increasingly complex compliance landscape.

- **Early 2025:** As of the first quarter of 2025, the trend has continued. The new Congress (119th) has convened with AI as a top agenda item; a bipartisan group of senators is reportedly drafting an "omnibus" AI bill that could consolidate various proposals (though details are still private). The Biden Administration in January 2025 announced it is developing **AI safety standards for federal procurement**, meaning any AI systems bought by the government would need to meet certain bias and security tests – a policy that could influence vendors broadly. In Minnesota, the 2025 legislative

session saw **multiple AI bills introduced (SF 1856, SF 1886, etc.)**, indicating Minnesota lawmakers are actively engaging with the issue as predicted. And notably, in May 2025 the federal government's **National Institute of Standards and Technology (NIST)** released draft guidelines for **AI transparency** that might become reference points for future regulations. Overall, the 2020–2025 trajectory shows a clear shift: **from sparse activity to a flurry of AI legislative efforts**, with 2023 and 2024 being inflection years. Figure 2 below illustrates this rapid increase in AI lawmaking activity over time:

(Imagine a timeline graph here, e.g., number of AI bills introduced nationally each year: 2016 – near zero; 2020 – a few dozen; 2023 – hundreds; 2024 – 600+.)

The key takeaway from recent trends is that **AI regulation has gained bipartisan urgency**. Early efforts focused on exploratory steps (creating task forces, commissioning studies, setting ethical principles), but recent efforts are more directive (imposing requirements, bans, and enforcement mechanisms). Minnesota's progression mirrors this: initial caution (study and internal standards) giving way to targeted regulation of egregious abuses (deepfakes) and now moving toward broader consumer protection (disclosure, oversight of AI in critical services). This rapid evolution sets the stage for the next five years, where we expect even more significant changes.

Forecast and Emerging Developments (2025–2030)

Looking ahead, the remainder of the decade will likely bring **substantial shifts in AI governance** at both federal and state levels. Policymakers, industry stakeholders, and society at large are all grappling with how to harness AI's benefits while managing its risks. Based on current trajectories, expert analysis, and announced initiatives, here are several anticipated developments in the AI regulatory landscape from **2025 to 2030**:

- **Federal Legislation and Possibly a Regulatory Agency:** There is strong expectation that the U.S. Congress will enact at least one major piece of AI legislation by the late 2020s. By 2025, bipartisan interest in AI is at an all-time high – Senate leadership (Schumer's working group) has published an AI "roadmap" with dozens of legislative recommendations, and multiple committees are drafting bills [91]. We anticipate a **federal AI law or package of laws around 2025–2026** that could establish a national framework. This might include: requirements for **AI system transparency** (e.g. disclosure of AI-generated content or labels for high-risk AI outputs), mandates for **risk assessment and testing** of AI systems above a certain impact threshold, and **anti-discrimination rules** for AI decisions in areas like credit, employment, housing, etc. Lawmakers have openly discussed creating a new **federal AI regulatory authority**. This could take the form of an "AI Commission" or empowering an existing agency (like the FTC or NIST) with rulemaking authority over AI. By 2030, it is plausible the U.S. will have a dedicated agency or inter-agency council overseeing AI, ensuring compliance with whatever new laws are passed. The shape is still uncertain – some propose a nimble AI regulator to focus on **frontier models** (e.g. AGI-level systems), others suggest each sector regulator continue to handle AI in their domain. But momentum is building for a more coherent approach. The **SAFE Innovation Framework** and other proposals explicitly call for evaluating a federal licensing regime for the most powerful AI (much like the Nuclear Regulatory Commission for reactors) [89] [18]. If extreme AI capabilities ("GPT-5" and beyond) advance rapidly, Congress may be pressed to implement a **permit or licensing system by late decade** for companies training very large AI models, tied to safety benchmarks and incident reporting.

- **National AI Strategy and Funding Initiatives:** We expect the federal government to continue and expand its strategic support for AI R&D – meaning more funding and infrastructure but tied to **responsible AI requirements**. Building on the National AI Initiative, Congress is likely to fund a **National AI Research Resource (NAIRR)** to give researchers access to computing power (a pilot NAIRR roadmap was delivered in 2023). By 2030, this could be a reality, enabling more controlled and diverse AI development (which also helps address concentration of AI in a few big tech firms). Additionally, federal funding bills (for defense, health, energy) will probably include **provisions requiring ethical AI use** and possibly mandating that grant recipients conduct AI impact assessments or follow the AI Bill of Rights principles. An example foreshadowing this: the FY2025 National Defense Authorization Act under debate includes sections on **AI test and evaluation standards for the Pentagon** and requirements for risk mitigation in any AI used for nuclear command and control. This indicates **AI safety and risk management** will be written into funding legislation, effectively shaping how AI is developed with federal dollars. By 2030, the U.S. might also implement **tax incentives or credits for ethical AI development** – encouraging companies to build bias mitigation or privacy features into AI (similar to how green energy credits work). This proactive approach would complement regulation, using carrots alongside sticks.

- **State Legal Landscape – Patchwork or Convergence:** In the near future, we'll likely see **more states passing AI laws**, potentially leading to a patchwork of slightly different requirements if federal preemption doesn't arrive first. *By 2025-2026*, several states (perhaps **Texas, New York, Massachusetts, Washington**) could join Colorado and California in enacting broad AI accountability laws. **Minnesota** might advance the currently proposed bills (AI disclosures, insurance AI ban) in the next session or two, given bipartisan interest, and could even contemplate an **"AI Bill of Rights" state law or a task force** to recommend comprehensive policies (Minnesota has done this in analogous areas like data privacy in the past). If enough states implement AI transparency or fairness laws, businesses will push for a uniform federal standard to avoid 50 different rules. Thus, one scenario by 2028 is that the accumulation of state AI regulations creates industry pressure resulting in **federal legislation that supersedes state laws** (similar to how state data breach notification laws eventually led to calls for a federal privacy law). Alternatively, if federal action stalls, we may see states enter into **interstate compacts or model laws** to harmonize AI governance regionally (for example, a coalition of midwestern states aligning on AI principles, or states adopting the Uniform Law Commission's model if one is proposed for AI). From 2025 to 2030, **AI in specific sectors will also drive state laws**: we expect more states to address **AI in insurance (to prevent algorithmic bias)**, **AI in education** (some legislatures might restrict AI proctoring or require transparency if AI tutors are used in public schools), and **AI in law enforcement** (with possible bans or rules on facial recognition and predictive policing tools continuing to spread as public scrutiny grows). Minnesota, for instance, might revisit facial recognition at a statewide level (beyond the 2020 drones law) – perhaps setting state standards for police use of any facial recognition and requiring audits or public reporting. In sum, by 2030, the map of state AI laws will be far more filled in: we could have on the order of 30–40 states with meaningful AI statutes, unless a federal law creates a more unified scheme that either preempts or is mirrored by the states.

- **International Influence and Alignment:** The global context will significantly shape U.S. developments. The **EU AI Act** is expected to be finalized by 2024 and in effect by 2026, imposing strict regulations on AI systems (risk-based requirements, conformity assessments, an EU AI Office for enforcement). U.S. companies that operate globally will effectively have to comply with the EU rules for their products, and this could become a de facto standard. U.S. policymakers are already

engaged in dialogues with the EU to seek some interoperability – a likely outcome is that the U.S. will align with Europe on certain **high-level principles and definitions** (to ease compliance for companies). We might see the U.S. endorse **OECD or G7 AI governance frameworks** formally; President Biden has already joined G7 leaders in announcing the **"Hiroshima AI Process"** in mid-2023 to develop global norms, which by 2025 may yield a set of non-binding but influential guidelines on AI safety, ethics, and governance. By 2030, there could be an established **international AI governance regime**: perhaps a treaty or at least a consortium (similar to how the Paris Agreement works for climate) where nations commit to certain AI standards (e.g. not using AI for mass surveillance beyond law, ensuring human oversight in military AI, etc.). The U.S. is likely to play a leading role in such efforts, given the strategic importance of AI in geopolitics (maintaining democratic values against an authoritarian model of AI governance espoused by China, for instance). For Minnesota and other states, international developments will trickle down – for example, if the EU mandates **AI supply chain transparency** (knowing the origin of training data and components), U.S. federal or state laws might incorporate similar requirements to facilitate trade. Companies in Minnesota that export software or AI-driven products to Europe will need to meet those standards, and Minnesota regulators might indirectly adopt them as best practices domestically.

- **Emerging Issues – New Laws for New Challenges:** As AI technology advances, new legal questions will emerge and likely be addressed through legislation or litigation:

- *Intellectual Property:* By 2030, we anticipate clearer rules on **copyright and AI**. Congress may update IP laws to clarify whether AI-generated works are copyrightable and who is the owner (current U.S. Copyright Office stance is that works without human authorship aren't protected, but this may be challenged as AI art becomes prevalent). Additionally, the legality of training AI on copyrighted data is a burning issue – we could see either courts or a new law carve out a "fair use" exception (or require opt-outs) for AI training datasets. How this gets resolved will affect AI companies in Minnesota (like media or software firms) in terms of data licensing costs and practices.
- *Liability and Safety:* If AI systems (e.g. autonomous vehicles or medical AI) cause harm, products liability law and tort law will be tested. We might see federal legislation or state laws to establish **liability regimes for AI** – for instance, assigning liability to the deployer of an AI system, or creating a safe harbor if certain approved safety standards were followed. The concept of **"AI malpractice"** could arise in professional fields (e.g. if a doctor relies on AI and it errs, how is liability shared?). By 2030, there could be case law setting precedents, or even a uniform law on AI liability that states adopt.
- *Workforce and Social Impact:* As AI potentially automates aspects of jobs (from trucking with self-driving vehicles to white-collar AI assistants), we might see labor regulations adapt. Perhaps amendments to laws like the Fair Labor Standards Act to address AI oversight, or collective bargaining agreements including clauses about consultation before AI systems are introduced at workplaces. Minnesota might, for example, integrate AI impact considerations into its workforce development programs or unemployment insurance (supporting retraining for those displaced by AI). New York's requirement to report AI-driven layoffs is likely the first of many such measures to **track and manage AI's economic impact**.
- *Privacy:* If a federal privacy law doesn't pass, more states will pass privacy statutes that include **automated decision-making provisions** (we already see this in California, Virginia, Connecticut, etc., which allow individuals to opt out of profiling and require data protection assessments for AI uses [92] [47]). By 2030, personal AI profiles (AI-generated inferences about individuals) might be

regulated as a data category – meaning companies would have to disclose if they use AI to profile someone and perhaps even **provide explanations or the logic** of algorithms to consumers upon request. This is a frontier of privacy law currently (often termed "Algorithmic Transparency" rights).

- *AI and Elections:* Given the concern about AI misinformation, it's likely by the 2028 presidential election new laws or regulations will be in place to curb **deepfake political propaganda**. We may see a federal law requiring disclaimers on any electioneering communication that uses synthetic media (if not an outright ban of malicious deepfakes as some states have). The FEC (Federal Election Commission) in fact is already considering rules on this as of 2023. By 2030, failing to disclose AI-altered campaign content could be a federal offense.
- *Advanced AI governance:* If by late 2020s we have AI systems approaching human-level cognitive ability (AGI), there could be emergency legislation. Some experts forecast needing a **global cap or monitoring on the largest AI training runs** (due to fears of uncontrollable AI). International agreements or federal laws might impose licensing on training models above a certain compute threshold, along with requirements for **AI safety research** investment by those companies. While speculative, this kind of measure has been openly discussed in Congress in 2023; its realization will depend on how AI technology progresses and public sentiment (which in turn could be influenced by any major AI-related incidents or accidents that occur in coming years).

In any case, **the trajectory is toward more regulation, not less**. Unlike in the social media era where years went by before serious regulatory talk, AI has prompted early and intense engagement from governments. By 2030, we expect a **more mature regulatory ecosystem**: likely a federal baseline law and active enforcement, layered with state-specific rules in some areas, and industry standards (possibly co-regulation where industry bodies certify AI systems for compliance). Minnesota in 2030 will probably have a more robust statutory framework on AI – potentially including statutes requiring algorithmic fairness in public services, procurement standards for AI used by state agencies (building on TAIGA's work), and collaboration with federal authorities on enforcement.

Risks, Gaps, and Strategic Implications

Despite the flurry of activity, there remain significant **gaps in AI legislation and challenges in enforcement**. Organizations operating in this space face a landscape of both legal **risks** and **opportunities**. This section analyzes the key gaps and risks in current regulations, and what they imply strategically for stakeholders (governments, companies, and communities):

- **Patchwork Regulations and Inconsistencies:** In the near term, one major risk is the **patchwork nature** of emerging AI laws. With different states enacting varying requirements (and some cities like NYC adding their own rules), companies deploying AI systems nationally must juggle a complex compliance puzzle. For example, an HR software provider might need to comply with New York City's bias audit mandate, Illinois' notice and consent rules for video interviews, and potentially Minnesota's future disclosure requirement – each slightly different. This patchwork increases compliance costs and complexity, and raises the risk of **unintentional non-compliance**. Smaller companies or startups, in particular, may struggle to keep track of the mosaic of AI-related laws. Additionally, inconsistencies can lead to **uneven protection** for the public: a job applicant in Minnesota might not (yet) have the same algorithmic fairness protections as one in NYC, for instance. Until either federal legislation harmonizes these rules or states adopt more uniform standards, this patchwork will persist. Strategically, this means organizations need robust tracking of

legislation and perhaps a "highest common denominator" approach (adhering to the strictest applicable standard) to mitigate legal risk across jurisdictions.

- **Regulatory Gaps and Unaddressed Harms:** Current laws, both federal and state, have notable blind spots. Many AI applications remain **unregulated or under-regulated**. For instance, there is no specific U.S. law governing **AI recommendation algorithms on social media**, which have huge societal impact (this was highlighted in debates around Section 230 immunity in cases like *Gonzalez v. Google*, but ultimately no changes were made). Another gap is **AI used in public sector decision-making** – apart from some procurement guidelines, there is little oversight of how government agencies (outside Minnesota's internal TAIGA policy) deploy AI in areas like social services eligibility, policing, or DMV processes. This raises equity and due process concerns. **Liability for AI-caused harm** is another gap: if an autonomous vehicle's AI malfunctions and causes an accident, it's not yet clearly delineated how liability is apportioned beyond traditional product liability concepts. The law tends to lag technological realities, so novel AI failure modes may leave victims without adequate redress or companies without clear guidance on liability exposure. Moreover, **AI security** is a relatively under-legislated area – the possibility of AI systems being hacked or manipulated (e.g., adversarial attacks) is real, but cybersecurity regulations (like critical infrastructure security rules) have yet to explicitly incorporate AI-specific considerations. These gaps mean some risks are not being proactively managed by law, placing the onus on organizations to self-govern or face reputational damage and ex-post lawsuits. Strategically, forward-looking organizations should identify these gray areas and voluntarily apply best practices (for example, conducting ethical AI assessments even when not legally required) to fill the void and reduce harm.

- **Enforcement Challenges:** Even where laws exist, enforcement is an issue. Many of the new AI laws rely on agencies that may lack resources or expertise to enforce them effectively. For example, NYC's bias audit law relies on employers to procure audits, but enforcement by the city's Department of Consumer and Worker Protection is still ramping up and may be uneven. At the federal level, agencies like the EEOC and FTC are signaling they will police AI, but these agencies must train staff and develop technical expertise to evaluate AI systems – not a trivial task. There's a risk of **"paper tiger" regulations** that sound good but are not rigorously enforced, which could fail to actually mitigate AI harms. On the flip side, there's also the risk of **over-enforcement or inconsistent interpretation**. Since definitions of AI in laws can be broad or vague, regulators might interpret obligations in unpredictable ways. Companies worry, for instance, about how to practically implement a "notice and explanation" requirement – how detailed must an explanation of an algorithmic decision be to satisfy a legal standard? Without clear guidance, they face uncertainty, and regulators might have differing expectations. This regulatory uncertainty can chill innovation (if companies pull back on AI deployment for fear of unknowingly violating a law) or lead to **legal disputes** that eventually clarify the rules through court precedents – a costly route. Strategically, organizations should engage with regulators early (through public comment processes, industry groups, or sandbox programs) to help shape workable enforcement guidelines. There's also an opportunity for third-party **compliance services and audit firms** to step in – much as the privacy industry blossomed post-GDPR, we are seeing an emerging niche for **AI audit and certification services** that can help bridge the expertise gap for regulators and companies alike.

- **Innovation vs. Regulation Balance:** A crucial implication of the regulatory trends is their impact on innovation and competitiveness. Overly restrictive or inconsistent regulations could **stifle innovation** – for instance, if startups are deterred by compliance burdens, or if companies decide

not to deploy beneficial AI due to liability fears. The White & Case analysis noted U.S. lawmakers are indeed cautious, aiming to foster innovation while addressing concerns [93] [94]. However, failing to regulate meaningful risks can also backfire on innovation in the long run, by eroding public trust. If consumers lose trust in AI (due to incidents like biased hiring systems or a deadly self-driving car crash), there could be a public backlash that prompts draconian measures or simply reduces adoption of AI, harming the industry. Therefore, a strategic implication is that **trustworthy AI is good for business**. Clear but balanced regulations can actually *enable* innovation by providing clear rules of the road. Many tech companies have recognized this and are advocating for reasonable regulation (for example, Microsoft's president Brad Smith has called for licensing of certain AI and safety brakes, and OpenAI has suggested an international agency for superintelligent AI). For Minnesota's economy (which includes medical device companies, agritech, retailers, etc. using AI), maintaining a reputation for **ethical innovation** can be a competitive advantage. Businesses that proactively comply with emerging norms (like Minnesota's upcoming transparency requirements) could differentiate themselves and face less friction with regulators and customers.

- **Equity and Inclusion Gaps:** One risk of current legislation is that it may not fully address the **social equity issues** posed by AI. While bias and discrimination are talked about, most laws so far cover race, gender, etc., but fewer consider disability, economic status, or rural/urban disparities in AI impact. There's a gap in community involvement – affected communities (e.g., those subjected to facial recognition policing or algorithmic lending) have had limited voice in shaping these laws. If regulations are crafted without inclusive input, they might miss certain harms or inadvertently encode majority biases. For instance, an AI health diagnostic device might work poorly for certain subgroups, but if the FDA's approval process doesn't demand diverse evaluation, that issue could be overlooked. The strategic implication here is a call for **multi-stakeholder engagement**. We see the beginnings of this in federal forums and state AI task forces that include civil society and industry experts. By 2030, involving ethicists, community leaders, and domain experts in regulatory development will be crucial to ensure AI laws genuinely protect those at risk of being marginalized by AI decisions. Organizations should be prepared for **more stringent fairness and accessibility requirements** – e.g., ensuring AI tools are accessible to people with disabilities (an issue the ADA guidance touched on) or requiring community impact assessments for public sector AI deployments.

- **Opportunity: Proactive Governance and Standards Adoption:** Amid the risks, there is a strategic *opportunity* for organizations to turn compliance into a strength. Adopting **frameworks like the NIST AI Risk Management Framework** or the ISO 42001 AI management standard (in development) can prepare organizations for future regulations and demonstrate accountability. Several leading AI companies have already issued **AI ethics policies and set up internal AI governance boards** – these not only preempt regulators but also position the companies as responsible players influencing the regulatory narrative. Minnesota's TAIGA initiative exemplifies how a government entity can self-regulate and thereby shape statewide norms. We anticipate the rise of more **public-private partnerships** developing best practices (similar to how the financial industry works with regulators on cybersecurity drills). For Minnesota businesses and institutions, participating in pilots (for example, a Minnesota "AI sandbox" where companies can test AI under regulatory supervision with temporary safe harbors) could be advantageous. The UK has introduced such sandboxes for AI; Minnesota or regional bodies might do so, giving companies a chance to innovate with guidance instead of punishment. Those who engage early with the rules can help tailor them to be practical and can avoid the compliance scramble that laggards face.

- **Enforcement Risks for Non-Compliance:** As regulations mature, enforcement actions will mount. Companies found using AI irresponsibly may face **lawsuits, fines, and reputational damage**. For instance, under Illinois' BIPA, some firms incurred multi-million dollar settlements for facial recognition misuse. We can expect, as more AI laws go into effect (e.g., Colorado's AI Act in 2025, California's new rules in 2026), that regulators and plaintiffs' attorneys will start testing them. There's a risk of **class action litigation** in cases of discriminatory algorithms or data breaches involving AI models (if an AI model leaks private data, it could trigger both privacy and AI-specific claims). The FTC could also make an example of a company with a high-profile AI failure to reinforce its authority – much like it did in the past with data privacy consent decrees. The strategic implication is clear: **non-compliance has real costs**, and they are not just financial. An enforcement action can erode customer trust and employee morale. On the positive side, companies that demonstrably prioritize ethical AI could earn a sort of "goodwill premium" – similar to how companies with strong environmental records may attract consumers and talent. In Minnesota, companies such as Target or Best Buy (major employers using AI in retail and HR) could enhance their brand by championing responsible AI, perhaps even beyond what the law strictly requires.

- **Adaptability and Future-Proofing:** Finally, one cannot ignore that AI technology evolves extremely quickly – regulations might quickly become outdated. Laws written in 2023 about "automated decision systems" might not anticipate, say, widespread AI personal assistants or advanced quantum-AI hybrids in 2027. This poses a risk that legislation becomes obsolete or too rigid. A strategic approach for both regulators and organizations is **flexible, principles-based governance**. Regulators are already considering performance-based requirements (e.g., requiring "reasonable" AI risk mitigation, which can adapt to new tech) rather than very specific rules that could be gamed or outdated. Organizations, in turn, should build **adaptability into their compliance programs**: treat AI governance as an ongoing process (with continuous monitoring and improvement) rather than a one-time checklist. Those who invest in **staying ahead of the regulatory curve** – by monitoring policy trends, engaging in standards development, and being ready to pivot their AI practices – will be best positioned to handle the unpredictable shifts the next years will bring.

In conclusion, the current gaps and challenges in AI regulation present as much of an argument for proactive, strategic action as they do cautionary tales. The landscape is still taking shape; organizations have a chance to influence and lead, rather than merely react. For Minnesota, aligning state efforts (like TAIGA and any new laws) with these broader considerations will be key to ensuring both **protection for citizens and a healthy environment for innovation**.

Strategic Recommendations for AI Stakeholders

Given the analysis above, organizations – whether companies deploying AI, startups developing AI tech, or public sector agencies using AI – should take proactive steps to navigate the evolving regulatory environment. Below are **strategic recommendations** to ensure compliance, adaptability, and foresight in regard to AI regulation, with a focus on Minnesota and U.S. federal trends:

1. **Establish Robust AI Governance Programs:** Organizations should create an internal **AI governance structure** now, rather than wait for laws to mandate it. This can include forming an AI ethics or oversight committee, developing an AI use policy, and inventorying all AI systems in use. Incorporate frameworks like the NIST **AI Risk Management Framework** to systematically assess and mitigate risks (bias, privacy, security) for each AI system [95] . By institutionalizing AI governance,

you not only prepare for likely compliance requirements (e.g. impact assessments, documentation) but also reduce the chance of AI failures. Minnesota organizations might leverage resources from TAIGA's principles [43] [44] as a starting point for internal policies. The goal is to ensure **accountability** – designate clear ownership (e.g. a Chief AI Ethics Officer or AI compliance lead) for AI oversight within your organization.

2. **Proactively Comply with Emerging Transparency and Fairness Norms:** Don't wait until a law forces your hand to implement **transparency, nondiscrimination, and privacy protections** in AI systems. Begin now by providing **notice to users or customers when AI is being used** in a decision that affects them (this could be as simple as a statement on your website or during an application process – and is likely to be required by laws like Minnesota's proposed SF 1886 on AI disclosures [34]). Where feasible, offer **explanations for algorithmic decisions** – even if high-level – and an option for human review of important decisions. These practices align with the White House's AI Bill of Rights principles (e.g. the right to notice & explanation, and human alternatives) and position you to seamlessly comply when such rights become codified [7]. Also, implement **bias testing** for AI models (especially those used in HR, lending, housing, healthcare). For example, run disparate impact analyses on AI outputs by race/gender and keep records of these tests. This not only preempts requirements like NYC's audit law but protects against discriminatory outcomes that could violate existing laws. Many of these measures can be turned into a **competitive advantage** – being able to tell clients or the public that your AI is "fairness-audited" or "transparent by design" can build trust.

3. **Stay Informed and Engage in Policymaking:** The AI regulatory landscape is fluid. Dedicate resources to **monitor legislative and regulatory developments** at federal and state levels. This could mean subscribing to policy update services, joining industry coalitions (like the Software Alliance or chamber committees focusing on tech policy), and participating in public consultations. When Minnesota or federal agencies request comments on AI guidelines – as the **EEOC did in 2023 for its AI guidance** – consider submitting feedback. By engaging, you have an opportunity to **shape regulations** so they are practical and science-based. Minnesota organizations could, for instance, share their experiences with TAIGA's implementation to inform a possible state AI framework. Additionally, cultivate relationships with local policymakers: offer to be a resource on AI topics. Policymakers often welcome input from businesses and researchers to educate themselves. Being at the table early means fewer surprises when new rules emerge. Remember that many AI rules (especially at the state level) are being conceived *now*; your voice can ensure they address real issues without unduly burdening innovation.

4. **Implement Strong Data Management and Privacy Practices:** Since AI is fueled by data, and privacy laws are increasingly intersecting with AI (like rules on algorithmic profiling), ensure your data practices are exemplary. This includes rigorous **data consent and transparency** for data collected that may train AI models – even if using public data, be mindful of privacy expectations and intellectual property (for example, avoid scraping user content without clear rights). Implement processes to **handle data subject requests** about AI (e.g. if someone asks, be prepared to provide what personal data was used in an AI-driven decision about them, and potentially even some explanation). These capabilities might become required as privacy laws evolve [46] [92]. Also, guard against **data bias**: ensure your training data is representative and not skewed in ways that could lead to unfair outcomes. In Minnesota, where there is a strong emphasis on equity in government services, demonstrating careful data stewardship in AI (e.g., in a healthcare AI tool ensuring it works

for diverse populations in the Twin Cities and Greater Minnesota) can also bolster public sector partnerships. In summary, treat data used in AI with the same (or higher) level of care as regulated personal data – it will pay off as regulations tighten.

5. **Invest in AI Auditability and Documentation:** "Documentation" might not sound exciting, but it will likely become a cornerstone of AI compliance. Start building an **"AI audit trail"** for your systems. This means keeping records of: model designs and objectives, training data sources, version histories of models, results of any testing or validation, and decision logs for automated decisions if possible. If an AI system makes an adverse decision about a person (e.g. denies a loan), record the factors involved. This positions you to respond to inquiries from regulators or to consumers exercising their rights. For example, Colorado's new law will require companies to **produce transparency reports for high-risk AI systems** [20] – having the documentation ready will make compliance feasible. Likewise, if down the line Minnesota enacts an AI accountability act that asks for algorithmic impact assessments, you will have much of the information readily available. Moreover, documenting your internal **risk assessments and mitigation steps** can serve as evidence of good faith and diligence, which could be crucial if you ever face a regulatory investigation or lawsuit. Show that you didn't deploy AI recklessly – you assessed it, you tuned it to reduce bias, you monitored outcomes. Essentially, treat it like an accounting audit: no major AI deployment without a paper trail. Tools and platforms for **model governance** are emerging that can help automate some of this (for instance, AI model management tools that log data versions and parameter changes).

6. **Train and Educate Your Workforce on AI Ethics & Compliance:** Regulations and best practices mean little if the people operating AI systems are unaware of them. Conduct training for relevant staff (developers, data scientists, product managers, HR teams implementing AI, etc.) on **AI ethics and the law**. Ensure your tech teams understand concepts like fairness metrics, privacy-by-design, adversarial robustness – and why they matter for compliance (e.g., how a bias in an AI could translate to a legal violation of anti-discrimination law). Likewise, educate your compliance and legal teams about AI technology – perhaps through workshops or hiring an AI specialist – so they can effectively oversee tech deployments. Bridging the gap between technologists and compliance professionals is key. Some organizations are establishing **"AI liaison" roles** or upskilling their privacy officers to also handle AI oversight. In Minnesota's public sector, TAIGA is doing internal training for state employees on safe AI use [96] ; private sector entities should mirror this. Also extend awareness to your C-suite and board – regulatory compliance and ethical AI should be seen as an enterprise risk issue, much like cybersecurity is now. This top-down awareness will ensure adequate resources and attention are given. A well-trained workforce can act as the first line of defense against AI-related risks, catching issues early (for example, an HR recruiter spotting that an AI screening tool might be unfair to certain groups and flagging it for review).

7. **Leverage Technology for Compliance (Regtech for AI):** As requirements like bias audits, explanations, and data tracking become more common, technology can assist with compliance. Consider investing in or using **tools that specialize in AI explainability and auditing**. For instance, there are AI software add-ons that can provide natural-language explanations for a model's decision – useful for both internal debugging and external explanation to users. Other tools can scan for bias in models or monitor drift over time. If you're a firm developing AI, incorporating these tools into your development pipeline will make your products more appealing in a regulated environment. For companies using third-party AI services, demand **transparency from vendors** – ask for model cards, audit results, or compliance statements when procuring AI solutions. In Minnesota, a company

bidding for a state contract that involves AI might gain an edge by demonstrating it has tech in place to ensure compliance with the state's ethical standards. We're also likely to see **regulatory technology (RegTech)** specifically for AI – e.g., platforms that track all applicable AI laws and check your systems against them. Stay on the lookout for such solutions as they mature, as they could automate some compliance tasks and reduce legal overhead.

8. **Plan for Incident Response and Remediation:** Even with best efforts, AI systems can and will fail or cause unintended consequences. Have a plan in place for **AI incidents** – analogous to a data breach response plan. This means defining what constitutes an AI incident (e.g., discovering a bias issue affecting decisions, or an AI outage that disrupts services, or an external report of harm caused by your AI), and how your organization will respond. Who needs to be alerted (legal, PR, executive team)? How will you investigate and contain the issue? How will you communicate transparently to those affected or to regulators? Regulators will expect accountability – a company that quickly addresses an AI flaw and compensates those impacted will fare better than one that ignores or hides it. For example, if an e-commerce recommendation AI starts suggesting offensive or dangerous content, have a kill switch and a customer communication drafted to apologize and correct. Minnesota's community-oriented approach to governance suggests that being forthright about issues (perhaps even voluntarily notifying state authorities if a serious consumer harm occurred due to AI) can build trust and goodwill. It's part of being **resilient and responsive**, which are traits regulators look for (and may even give credit for in enforcement decisions).

9. **Engage in Industry Collaboration and Standards Development:** Many AI regulatory solutions are still being figured out. Collaborating with peers in your industry to develop **codes of conduct or sector-specific standards** can be highly beneficial. Industry self-regulation can sometimes preempt the need for government regulation or inform its shape. For instance, the Partnership on AI (a multi-stakeholder group) has released best practice papers on AI explainability and fairness which could evolve into standards. If you operate in a domain like healthcare, consider joining initiatives setting **standards for AI in medical devices** – FDA often incorporates industry consensus standards in its guidance. In finance, groups like the IEEE or ISO are working on AI standards; contributing to those can give you insight and influence. For Minnesota's numerous medical tech companies, participating in the FDA's pilot programs for AI algorithm pre-certification could be a strategic move to be ahead of required processes. On a local level, Minnesota companies and universities could collaborate to create a **Minnesota AI Ethics Consortium** to share knowledge and perhaps liaise with state government on upcoming issues (the state's history of public-private initiatives in health and environment could be a model). Ultimately, being part of the conversation ensures you won't be caught off guard by new rules and that you can help shape **reasonable, effective… Ultimately, being part of the conversation ensures you won't be caught off guard by new rules and that you can help shape** reasonable, effective regulations** that protect the public without unduly hindering innovation.

10. **Maintain Foresight and Flexibility:** Finally, embrace a forward-looking and adaptable mindset. The AI landscape will continue to shift – new breakthroughs or a major incident could prompt sudden regulatory changes. Engage in **scenario planning** for how potential future developments might affect you. For example, consider how you would respond if a federal AI licensing scheme for advanced AI is introduced, or if a foreign AI regulation (like the EU AI Act) becomes a de facto standard for your products. Build flexibility into your AI strategies: modularize your AI systems so they can be adjusted to comply with different requirements, and keep "human-in-the-loop" options

available so you can quickly toggle between automated and human decision-making if required by law. Encourage your teams to stay educated (perhaps sponsoring continued learning in AI ethics or policy for key staff) so that your organization's knowledge stays current. By cultivating a culture that values **responsible innovation**, you ensure that compliance is not just a one-time effort but an ongoing competency. Organizations that are **agile and conscientious** in this way will not only navigate regulations successfully but can also steer their AI efforts to create genuine social value, aligning with the direction that Minnesota and the broader U.S. are heading.

Appendix: Original Task Prompt

```
# Deep Research Task Guidelines

## Markdown Formatting

**User Instructions Take Precedence:** If the user provides specific
instructions about the desired output format, these instructions should always
take precedence over the default formatting guidelines outlined below.

1. Use clear and logical headings to organize content in Markdown:
   - **Main Title (`#`):** Use once at the top for the document's primary title.
   - **Primary Subheadings (`##`):** Use multiple times for main sections.
2. Keep paragraphs short (3-5 sentences) to avoid dense text blocks.
3. Combine bullet points or numbered lists for steps, key takeaways, or grouped
ideas:
   - Use `-` or `*` for unordered lists
   - Use numbers (`1.`, `2.`) for ordered lists
4. Ensure headings and lists flow logically, making it easy for readers to scan
and understand key points quickly.
5. The readability and format of the output is very important to the user.

## Citations

**IMPORTANT:** You must preserve any and all citations following the `【{cursor}
†L{line_start}(-L{line_end})?】` format.

1. If you embed images with `【{cursor}†embed_image】`, ALWAYS cite them at the
BEGINNING of paragraphs, and DO NOT mention the sources of the embed_image
citation, as they are automatically displayed in the UI.
2. Do not use `embed_image` citations in front of headers; ONLY embed them at
paragraphs containing three to five sentences minimum.
3. No need to search for images: Do not specifically search for images to embed.
If you encounter images that can be opened while researching the main issue, you
may consider them; otherwise, do not go out of your way to find images to embed.
4. Lower resolution images are fine to embed; there is no need to seek higher
resolution versions of the same image.
```

5. You can ONLY embed images if you have actually clicked into the image itself, and DO NOT cite the same image more than once.
6. If an unsupported content type error message appears for an image, embedding it will NOT work.

Comprehensiveness

Be as detailed and comprehensive as possible! The user will wait a long time for your answer, so the output should be **very comprehensive**.

Stay Updated

Your internal knowledge is likely outdated at this point in time. **DO NOT rely solely on your training data or memorized information.** Use searches to gather the latest insights and understand the current state of research before diving deeper into any topic. You are obviously on the wrong track if the user is asking for a recent update but your answer only contains facts known before 2024 as it is now 2025.

Deep Research Task

Create a deep research report on the current and future landscape of AI-related legislation in the United States, focusing on both federal-level policy and Minnesota-specific laws. The output should be structured for use in a consulting context, supporting strategic planning and regulatory awareness. The research should cover:

1. Current Federal AI Legislation – Overview of existing U.S. federal laws and executive actions related to artificial intelligence, including AI development, deployment, safety, transparency, privacy, accountability, and sector-specific governance (e.g., healthcare, finance, hiring).

2. Current AI Legislation in Minnesota – Overview of Minnesota’s current legislative activity around AI, including proposed and enacted bills, regulatory initiatives, task forces, or commissions. Include publicly available plans or frameworks for AI regulation.

3. Comparative State Context – Compare Minnesota’s legislative progress with other states leading in AI regulation (e.g., California, New York, Illinois, Texas). Highlight similarities, differences, and regional trends.

4. Recent Trends (2020–2025) – Analyze how AI legislation has evolved federally and in Minnesota in the past five years. Include timelines or summaries of major events or bills to show legislative momentum and shifts.

5. Forecast & Emerging Developments (2025–2030) – Forward-looking analysis of anticipated regulatory shifts, pending legislation, stakeholder movements, or potential federal frameworks. Include expert forecasts or institutional

roadmaps.

6. Risks, Gaps & Strategic Implications – Identify gaps in legislation, enforcement risks, and strategic opportunities for compliance or advocacy. Address implications for innovation, funding, and AI deployment.

7. Data & Sources – Use authoritative sources including congress.gov, whitehouse.gov, mn.gov, Brookings, CSET, Stanford HAI, peer-reviewed publications, and reputable legal or tech policy outlets.

8. Visuals & Comparative Charts – Include charts, maps, or tables comparing legislation across states, timelines of major events, and regulatory forecasts.

9. Recommendations – Strategic recommendations for AI-related organizations seeking compliance, adaptability, and foresight regarding AI regulation in Minnesota and federally.

10. Append the original prompt to the end of the output.

Format the report using clear sections with headers. Include visual elements and tables where useful to enhance clarity and comparison.

---

1 2 3 7 13 14 15 18 19 20 21 22 23 74 75 87 88 89 93 94 95 AI Watch: Global regulatory tracker - United States | White & Case LLP
https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states

4 5 6 90 congress.gov
https://www.congress.gov/crs_external_products/R/PDF/R47843/R47843.8.pdf

8 9 16 17 60 62 76 78 The Outlook of US AI Regulations in 2025: A Concise Summary | Zartis
https://www.zartis.com/us-artificial-intelligence-regulations-in-2025-a-concise-summary/

10 11 12 EEOC Issues New Guidance on Employer Use of AI and Disparate Impact Potential - Ogletree
https://ogletree.com/insights-resources/blog-posts/eeoc-issues-new-guidance-on-employer-use-of-ai-and-disparate-impact-potential/

24 26 27 28 29 30 31 81 86 Minnesota AI Policy | Track State AI Legislation — multistate.ai
https://www.multistate.ai/ai-policy-overview-minnesota

25 Minneapolis bans its police department from using facial recognition ...
https://techcrunch.com/2021/02/12/minneapolis-facial-recognition-ban/

32 SF 1856 as introduced - 94th Legislature (2025 - 2026)
https://www.revisor.mn.gov/bills/text.php?number=SF1856&version=0&session=ls94&session_year=2025&session_number=0

33 34 35 36 MN SF1886 | BillTrack50
https://www.billtrack50.com/billdetail/1847457

37 NY State Assembly Bill 2023-A9559
https://www.nysenate.gov/legislation/bills/2023/A9559

38 Bill Text: MN SF1117 | 2025-2026 | 94th Legislature | Introduced | LegiScan
https://legiscan.com/MN/text/SF1117/id/3102909

39 40 41 42 96 Minnesota’s Intentional Approach to Artificial Intelligence
https://mn.gov/mnit/media/blog/index.jsp?id=38-593353

43 44 82 Transparent Artificial Intelligence Governance Alliance / Minnesota IT Services
https://mn.gov/mnit/taiga/

45 US state-by-state AI legislation snapshot - Lexology
https://www.lexology.com/library/detail.aspx?g=d0c88d95-695f-4ef1-913f-a4c1ca6a9d12

46 47 56 57 84 92 The State of State AI Laws: 2023 – EPIC – Electronic Privacy Information Center
https://epic.org/the-state-of-state-ai-laws-2023/

48 49 52 53 77 California Privacy and AI Legislation Update: September 2, 2024 | Byte Back
https://www.bytebacklaw.com/2024/09/california-privacy-and-ai-legislation-update-september-2-2024/

50 51 Governor Newsom Vetoes Sweeping AI Regulation, SB 1047 | Center for Security and Emerging Technology
https://cset.georgetown.edu/article/governor-newsom-vetoes-sweeping-ai-regulation-sb-1047/

54 Why Gavin Newsom vetoed California's bold bid to regulate AI
https://calmatters.org/economy/2024/09/california-artificial-intelligence-bill-veto/

55 California Gov. Newsom vetoes AI safety bill that divided Silicon Valley
https://www.npr.org/2024/09/20/nx-s1-5119792/newsom-ai-bill-california-sb1047-tech

58 59 61 Artificial Intelligence 2023 Legislation
https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation

63 64 65 66 83 Illinois Joins Colorado and NYC in Restricting Generative AI in HR (Plus a Quick Survey of the Legal Landscape Across the US and Globally) | The Employer Report
https://www.theemployerreport.com/2024/08/illinois-joins-colorado-and-nyc-in-restricting-generative-ai-in-hr-a-comprehensive-look-at-us-and-global-laws-on-algorithmic-bias-in-the-workplace/

67 68 69 70 Texas AI Policy | Track State AI Legislation — multistate.ai
https://www.multistate.ai/ai-policy-overview-texas

71 Texas Legislature to Consider Sweeping AI Legislation in 2025
https://www.insideglobaltech.com/2024/11/13/texas-legislature-to-consider-sweeping-ai-legislation-in-2025/

72 Texas' Left Turn On AI Regulation - Forbes
https://www.forbes.com/sites/jamesbroughel/2025/01/26/texass-left-turn-on-ai-regulation/

73 85 Texas Considers Comprehensive AI Bill | Healthcare Law Blog
https://www.sheppardhealthlaw.com/2024/12/articles/artificial-intelligence/texas-considers-comprehensive-ai-bill/

79 80 Artificial Intelligence (AI) Legislation — multistate.ai
https://www.multistate.ai/artificial-intelligence-ai-legislation

91 [PDF] Roadmap_Electronic1.32pm.pdf - Senator Chuck Schumer
https://www.schumer.senate.gov/imo/media/doc/Roadmap_Electronic1.32pm.pdf