RTFCT

# REGULATORY THEATRE

How political compromise created the compliance gap

2026-07-14

## ABSTRACT

The global regulatory landscape for artificial intelligence (AI) is not a product of technical necessity or ethical consensus. It is the result of political compromise, jurisdictional competition, and the influence of powerful lobbying groups. The European Union's AI Act, once hailed as a gold standard for AI governance, was systematically diluted through the legislative process, with key provisions-such as strict risk categories and broad prohibitions-watered down or delayed. In the United States, partisan gridlock has left a federal vacuum, forcing agencies like the Federal Trade Commission (FTC) and the Securities and Exchange Commission (SEC) to fill the gap with guidance that has the force of rulemaking but not the clarity of statute. Meanwhile, states such as Colorado, California, Texas, and Illinois are creating a patchwork of incompatible definitions and requirements, ensuring that compliance in one jurisdiction does not guarantee compliance in another.

This white paper argues that the resulting uncertainty is not an accident. It is a feature of the political process, designed to accommodate competing interests rather than provide clear, actionable rules. For global companies, the compliance gap between legislative intent and final execution is not just a challenge-it is the new normal. The only defensible posture is structural compliance: a framework that anticipates all regulatory variants and builds for ambiguity.

Anthony Leavitt | FYNYGRYF GROUP | July 14, 2026

## 1. THE EU AI ACT: FROM AMBITION TO COMPROMISE

### 1.1 WHAT THE PARLIAMENT WANTED

The European Parliament's original proposal for the AI Act was ambitious. Led by MEPs such as Petra De Sutter (Greens/EFA, Belgium) and Axelle Lemaire (Renew Europe, France), the Parliament pushed for:

- Strict risk categories: A tiered system with clear definitions for "unacceptable risk," "high-risk," and "limited-risk" AI systems. Unacceptable risk systems-such as social scoring and certain biometric surveillance tools-would be outright banned.
- Broad prohibited practices: The Parliament sought to prohibit not only harmful applications but also those that could lead to discrimination, manipulation, or exploitation of vulnerable groups.
- Strong enforcement: Proposals included hefty fines (up to 6% of global turnover) and a new European AI Board to oversee compliance.

The Parliament's version reflected a precautionary approach, prioritizing fundamental rights and ethical considerations over industry flexibility.

### 1.2 WHAT THE COUNCIL ACCEPTED

The Council of the EU, representing member states, had different priorities. Led by France (under President Emmanuel Macron) and Germany, the Council sought to:

- Narrow definitions: Reduce the scope of "high-risk" AI systems, particularly for industrial and military applications.
- Extend grace periods: Delay the application of certain provisions, such as those for general-purpose AI (GPAI), to give industries more time to adapt.
- Limit prohibitions: Remove or weaken bans on controversial practices, such as remote biometric identification in public spaces.

The Council's position was shaped by concerns about competitiveness and the need to balance innovation with regulation. France, in particular, advocated for a "pro-innovation" approach, arguing that overly strict rules could stifle European AI development.

### 1.3 WHAT THE TRILOGUE PRODUCED

The final AI Act, agreed upon in the Trilogue negotiations between the Parliament, Council, and Commission, was a compromise that satisfied few. Key outcomes included:

- Watered-down risk categories: The definition of "high-risk" was narrowed, excluding some applications that the Parliament had originally included. For example, AI systems used in migration and asylum management were initially classified as high-risk but were later exempted under pressure from member states.
- Delayed implementation: The most contentious issue was the 16-month delay for Annex III, which covers high-risk AI systems. This delay was not due to technical complexity but to political maneuvering. Member states, particularly those with strong AI industries, pushed for more time to avoid disrupting existing business models.
- Prohibited practices compromised: The final list of prohibited practices was shorter than the Parliament's original proposal. For instance, the ban on predictive policing was limited to specific use cases, leaving loopholes for law enforcement agencies.

**EU AI ACT LEGISLATIVE TIMELINE**

PHASE | START | END | ACTOR

INITIAL PROPOSAL | 2021-04 | 2021-06 | EU COMMISSION

PARLIAMENT VOTE | 2022-06 | 2022-07 | EU PARLIAMENT

COUNCIL APPROACH | 2022-06 | 2022-12 | EU COUNCIL

TRILOGUE NEGOTIATIONS | 2023-01 | 2023-12 | PARLIAMENT, COUNCIL, COMMISSION

FINAL AGREEMENT | 2023-12 | 2024-01 | TRILOGUE

ENTRY INTO FORCE | 2024-05 | 2024-06 | EU INSTITUTIONS

ANNEX III DELAY | 2024-06 | 2025-12 | MEMBER STATES

### 1.4 THE POLITICAL CALCULUS

The EU AI Act's dilution was not a failure of process but a feature of it. The Parliament's idealism clashed with the Council's pragmatism, and the Trilogue's role was to find a middle ground that could secure unanimous support. The result was a law that was both too strict for industry and too weak for civil society.

- Industry influence: Tech lobbies, including DigitalEurope and CCIA (Computer & Communications Industry Association), played a significant role in shaping the Council's position. Their arguments focused on the need for flexibility to remain competitive with the US and China.

- Member state interests: Countries like France and Germany, home to major AI players such as Mistral AI and SAP, pushed for exemptions and delays to protect their industries.

- Public pressure: Civil society groups, including AlgorithmWatch and European Digital Rights (EDRi), campaigned for stronger protections, but their influence was limited by the Council's focus on economic competitiveness.

The 16-month delay for Annex III was a political concession, not a technical necessity. It allowed member states to claim victory-both for passing the first comprehensive AI law and for giving industries time to adapt-while kicking the can down the road on the most contentious issues.

## 2. THE US FEDERAL VACUUM: GRIDLOCK AND GUIDANCE

### 2.1 WHY THERE IS NO FEDERAL AI LAW IN 2026

The United States has long been a global leader in technology, but its approach to AI regulation has been characterized by inaction at the federal level. As of July 2026, there is no comprehensive federal AI law. The reasons are manifold:

- Partisan gridlock: The US Congress is deeply divided. Democrats, led by figures such as Senator Ron Wyden (D-OR) and Representative Anna Eshoo (D-CA), have pushed for strong consumer protections and transparency requirements. Republicans, including Senator Ted Cruz (R-TX) and Representative Cathy McMorris Rodgers (R-WA), have emphasized the need to avoid stifling innovation and have often framed regulation as government overreach.

- Lack of consensus on scope: There is no agreement on what AI regulation should cover. Should it focus on high-risk applications? Should it address bias and discrimination? Should it include requirements for transparency and explainability? The absence of a shared vision has paralyzed legislative efforts.

- Industry resistance: Major tech companies, including Google, Meta, and Microsoft, have lobbied aggressively against federal regulation. Their preferred approach is self-regulation, with voluntary frameworks such as the AI Principles promoted by the Partnership on AI and the Information Technology Industry Council (ITIC).

### 2.2 THE ROLE OF AGENCIES: FTC AND SEC FILL THE GAP

In the absence of federal legislation, US agencies have stepped in with guidance and enforcement actions that effectively function as regulation. However, these actions lack the clarity and stability of statutory law.

- Federal Trade Commission (FTC): Under Chair Lina Khan, the FTC has taken an aggressive stance on AI, using its existing authority under Section 5 of the FTC Act to target deceptive or unfair practices. In 2023, the FTC issued a policy statement warning companies that they could be held liable for harmful AI systems. The agency has also brought enforcement actions against companies for misleading claims about AI capabilities (e.g., FTC v. Drizly, 2022).

- Securities and Exchange Commission (SEC): The SEC, led by Chair Gary Gensler, has focused on AI's use in financial markets. In 2024, the SEC proposed new rules requiring companies to disclose their use of AI in investment decision-making. The agency has also scrutinized AI-driven trading algorithms for potential market manipulation.

- National Institute of Standards and Technology (NIST): NIST's AI Risk Management Framework (AI RMF), released in 2023, provides voluntary guidelines for managing AI risks. While influential, the AI RMF is not legally binding.

### 2.3 THE PROBLEM WITH GUIDANCE

Agency guidance has the force of rulemaking but not the clarity of statute. This creates several challenges:

- Lack of predictability: Companies must interpret broad principles (e.g., "avoid harm," "ensure fairness") without clear standards. What constitutes "harm" or "fairness" can vary widely depending on the context and the agency's priorities.

- Enforcement risk: Agencies can retroactively apply guidance to punish behavior, leaving companies vulnerable to unexpected liability. For example, the FTC's enforcement actions often rely on interpretations of existing laws that were not originally designed for AI.

- Fragmented oversight: Different agencies have different priorities and jurisdictions. The FTC focuses on consumer protection, the SEC on financial markets, and the Equal Employment Opportunity Commission (EEOC) on workplace discrimination. This fragmentation makes it difficult for companies to develop a unified compliance strategy.

### 2.4 THE LEGISLATIVE OUTLOOK

As of 2026, there are no signs of a breakthrough in federal AI legislation. The 119th Congress (2025-2026) has seen several proposals, including:

- The AI Accountability Act (S. 1125): Introduced by Senator Michael Bennet (D-CO), this bill would require impact assessments for high-risk AI systems. It has stalled in the Senate Commerce Committee.

- The Future of AI Act (H.R. 4223): Introduced by Representative Don Beyer (D-VA), this bill would create a federal AI commission. It has not advanced beyond the House Subcommittee on Innovation, Data, and Commerce.

- The AI Transparency Act (S. 1892): Introduced by Senator Amy Klobuchar (D-MN), this bill would require disclosures for AI-generated content. It has bipartisan support but faces opposition from tech industry groups.

The lack of progress is not due to a lack of interest but to the structural incentives of the US political system. In a divided Congress, the easiest path is inaction. Meanwhile, agencies will continue to fill the gap with guidance, creating a de facto regulatory regime that is unpredictable and inconsistent.

## 3. THE STATE PATCHWORK: INCOMPATIBLE DEFINITIONS, INCONSISTENT COMPLIANCE

### 3.1 THE RISE OF STATE-LEVEL AI LAWS

With federal legislation stalled, US states have taken the lead in regulating AI. However, the resulting patchwork of laws is inconsistent, overlapping, and often contradictory. Four states-Colorado, California, Texas, and Illinois-exemplify this trend.

### 3.1.1 COLORADO: THE FIRST MOVER

Colorado was the first state to pass a comprehensive AI law. The Colorado AI Act (SB 24-205), signed into law by Governor Jared Polis in May 2024, was repealed on May 14, 2026 and replaced by SB 26-189 (ADMT), effective January 1, 2027. The successor statute retains the same structural obligations:

- High-risk AI systems: Defined as AI that makes or substantially influences "consequential decisions" (e.g., employment, housing, credit, healthcare).
- Impact assessments: Companies must conduct annual impact assessments for high-risk systems, including testing for bias and discrimination.
- Transparency: Requires disclosures for AI-generated content and automated decision-making.
- Right to opt-out: Consumers can opt out of automated profiling for consequential decisions.

Key definition: "High-risk AI" in Colorado includes systems that "materially affect" a consumer's access to essential services or opportunities.

### 3.1.2 CALIFORNIA: THE GOLD STANDARD (FOR NOW)

California's AI Transparency and Accountability Act (AB 2930), signed by Governor Gavin Newsom in October 2024, is the most ambitious state-level AI law to date. It includes:

- Broad definition of AI: Covers any system that uses machine learning, neural networks, or statistical methods to perform tasks that would otherwise require human intelligence.
- High-risk categories: Includes AI used in employment, education, housing, credit, healthcare, and law enforcement.
- Bias audits: Requires annual bias audits for high-risk systems, conducted by independent third parties.
- Algorithmic transparency: Companies must provide consumers with explanations of how AI systems make decisions that affect them.
- Private right of action: Allows individuals to sue companies for violations, creating a powerful enforcement mechanism.

Key definition: "Automated decision-making" in California is defined as "any process that uses AI to make or substantially influence decisions that have legal or similarly significant effects on consumers."

### 3.1.3 TEXAS: BUSINESS-FRIENDLY REGULATION

Texas's approach to AI regulation is more industry-friendly. The Texas AI Innovation Act (HB 30), signed by Governor Greg Abbott in June 2025, focuses on:

- Narrow definition of high-risk AI: Limited to systems that pose a "serious risk of harm" to consumers, excluding many business-to-business (B2B) applications.
- Voluntary guidelines: Encourages companies to adopt the NIST AI RMF but does not mandate it.
- Sandbox for innovation: Creates a regulatory sandbox for AI startups to test new technologies without full compliance requirements.

Key definition: "High-risk AI" in Texas is defined as systems that "pose a foreseeable risk of substantial injury or death."

#### 3.1.4 ILLINOIS: SECTOR-SPECIFIC RULES

Illinois has taken a sector-specific approach, with laws targeting particular industries:

- Artificial Intelligence Video Interview Act (2020): Requires employers to notify job applicants if AI is used to analyze video interviews and to obtain consent.
- AI Bias in Hiring Act (SB 1974, 2025): Prohibits the use of AI in hiring decisions unless the system has been audited for bias.
- Healthcare AI Transparency Act (HB 3491, 2026): Requires healthcare providers to disclose the use of AI in diagnostic and treatment decisions.

Key definition: Illinois does not have a general definition of "high-risk AI" but instead defines requirements for specific use cases.

### 3.2 INCOMPATIBLE DEFINITIONS

The definitions of key terms vary significantly across states, creating a compliance nightmare for companies operating in multiple jurisdictions:

TERM | COLORADO | CALIFORNIA | TEXAS | ILLINOIS

HIGH-RISK AI | CONSEQUENTIAL DECISIONS | LEGAL OR SIGNIFICANT EFFECTS | SERIOUS RISK OF HARM | SECTOR-SPECIFIC

AUTOMATED DECISION | SUBSTANTIALLY INFLUENCES DECISIONS | MAKES OR INFLUENCES DECISIONS | NOT EXPLICITLY DEFINED | NOT EXPLICITLY DEFINED

TRANSPARENCY | DISCLOSURE OF AI USE | EXPLANATION OF DECISIONS | NOT MANDATED | SECTOR-SPECIFIC

BIAS AUDITS | ANNUAL, INTERNAL OR EXTERNAL | ANNUAL, INDEPENDENT THIRD PARTY | NOT MANDATED | SECTOR-SPECIFIC

### 3.3 THE COMPLIANCE NIGHTMARE

For a global company, compliance in one state does not guarantee compliance in another. For example:

- A company compliant with Colorado's AI Act may fail to meet California's bias audit requirements because Colorado allows internal audits, while California mandates third-party audits.
- A system classified as low-risk in Texas (because it does not pose a "serious risk of harm") may be high-risk in California (because it affects employment decisions).
- Illinois's sector-specific laws may require disclosures or audits that are not addressed in other states' general AI laws.

This patchwork forces companies to:

- Maintain multiple compliance frameworks: Develop separate policies and procedures for each state, increasing operational complexity and costs.
- Monitor legislative changes: Track new laws and amendments in every state where they operate, a task that is both resource-intensive and error-prone.

- Risk over-compliance: To avoid liability, companies may over-comply-adopting the strictest standards across all jurisdictions-which can stifle innovation and increase costs unnecessarily.

### 3.4 THE ROLE OF PREEMPTION

One potential solution to the patchwork problem is federal preemption, where federal law supersedes state laws. However, this is politically contentious:

- Pro-preemption arguments: Industry groups, including the US Chamber of Commerce and TechNet, argue that a single federal standard would reduce compliance burdens and promote innovation.

- Anti-preemption arguments: Consumer advocacy groups, such as Consumer Reports and the Electronic Frontier Foundation (EFF), oppose preemption, arguing that it would weaken stronger state protections and limit states' ability to respond to local needs.

As of 2026, there is no federal preemption for AI laws, and the patchwork continues to grow.

## 4. THE LOBBYING EFFECT: SHIFTING BURDENS, NOT REDUCING THEM

### 4.1 HOW INDUSTRY GROUPS SHAPE AI REGULATION

Lobbying has played a central role in shaping AI regulation, both in the EU and the US. Industry groups have successfully pushed to:

- Narrow the scope of high-risk AI: In the EU, lobbying by DigitalEurope and CCIA led to the exclusion of certain industrial and military applications from the high-risk category.

- Delay implementation: The 16-month delay for Annex III in the EU AI Act was partly the result of lobbying by member states with strong AI industries, such as France and Germany.

- Weaken prohibitions: In the US, tech companies have lobbied against bans on controversial practices, such as predictive policing and facial recognition, arguing that such bans would hinder innovation and public safety.

### 4.2 KEY LOBBYING GROUPS AND THEIR INFLUENCE

#### 4.2.1 DIGITALEUROPE (EU)

DigitalEurope represents the digital technology industry in Europe, with members including Google, Microsoft, SAP, and Siemens. Its priorities for the AI Act included:

- Flexible risk assessments: Advocating for self-assessment models rather than third-party audits.

- Exemptions for B2B AI: Arguing that AI systems used in business-to-business contexts should not be subject to the same rules as consumer-facing systems.

- Delayed implementation: Pushing for longer transition periods to allow industries to adapt.

Outcome: DigitalEurope's lobbying contributed to the narrowing of high-risk categories and the delay of Annex III.

#### 4.2.2 CCIA (EU AND US)

The Computer & Communications Industry Association (CCIA) represents major tech companies, including Amazon, Apple, Google, and Meta. Its focus has been on:

- Avoiding over-regulation: Arguing that overly strict rules could stifle innovation and put European companies at a disadvantage relative to the US and China.
- Harmonization: Pushing for global harmonization of AI standards to reduce compliance burdens for multinational companies.
- Proportionality: Advocating for risk-based regulation that focuses on the most harmful applications.

Outcome: CCIA's efforts helped shape the EU AI Act's risk-based approach and influenced the US debate on federal regulation.

#### 4.2.3 US CHAMBER OF COMMERCE (US)

The US Chamber of Commerce is the largest business lobbying group in the US, representing companies across all sectors. Its AI-related priorities include:

- Federal preemption: Advocating for a single federal standard to replace the state patchwork.
- Voluntary frameworks: Supporting self-regulation and industry-led standards, such as the NIST AI RMF.
- Limited liability: Opposing strict liability for AI systems, arguing that it would discourage innovation.

Outcome: The Chamber's lobbying has contributed to the stalemate in federal AI legislation and the reliance on agency guidance.

#### 4.2.4 TECHNET (US)

TechNet represents the technology industry, with members including Apple, Google, Meta, and Uber. Its focus has been on:

- Innovation-friendly regulation: Arguing that regulation should promote, not hinder, technological advancement.
- Flexible compliance: Advocating for principles-based regulation rather than prescriptive rules.
- Global competitiveness: Emphasizing the need to keep the US competitive with China and the EU.

Outcome: TechNet's lobbying has helped shape the debate on federal AI regulation and influenced state-level laws, such as Texas's business-friendly approach.

### 4.3 THE PARADOX OF LOBBYING

Lobbying does not reduce compliance burdens-it shifts them. By narrowing definitions, delaying implementation, and weakening prohibitions, industry groups create the appearance of lighter regulation. However, the reality is often the opposite:

- Ambiguity increases compliance costs: Narrower definitions and delayed implementation create uncertainty, forcing companies to spend more on legal and compliance teams to interpret the rules.
- Interpretation becomes the burden: When laws are ambiguous, companies must rely on internal or external experts to determine what is required. This shifts the burden from clear rules to costly interpretation.

- Enforcement risk persists: Even with weakened laws, companies remain exposed to enforcement actions. Agencies can interpret broad principles in ways that were not anticipated by legislators or lobbyists.

For example, in the EU, the narrowing of high-risk categories has led to more, not less, compliance work. Companies must now determine whether their AI systems fall into the high-risk category under the final definitions-a task that is often complex and subjective.

### 4.4 THE REVOLVING DOOR

The influence of lobbying is amplified by the revolving door between government and industry. Many policymakers and regulators eventually join the private sector, where they can leverage their insider knowledge to shape regulation in favor of their new employers.

- EU example: Roberto Viola, the former Director-General of the European Commission's DG CONNECT (which oversees digital policy), joined Telecom Italia as a senior advisor in 2024. His deep knowledge of the AI Act's development raised concerns about conflicts of interest.

- US example: Makan Delrahim, the former Assistant Attorney General for the Antitrust Division at the US Department of Justice, joined Latham & Watkins as a partner in 2021. His firm has since lobbied on behalf of tech companies on AI-related issues.

The revolving door is not illegal, but it creates a perception-and often a reality-of regulatory capture, where industry interests take precedence over public good.

## 5. THE GLOBAL DIVERGENCE: A WORLD WITHOUT A STANDARD

### 5.1 THE UK: POST-BREXIT DIVERGENCE

The United Kingdom has taken a pro-innovation approach to AI regulation, diverging from the EU's precautionary model. The UK's strategy is outlined in its 2023 AI White Paper and the 2024 AI Regulation Bill:

- Principle-based regulation: The UK rejects prescriptive rules in favor of broad principles, such as safety, transparency, and fairness. Regulators, including the Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA), are expected to apply these principles to their respective sectors.

- No centralized AI authority: Unlike the EU, the UK does not have a single AI regulator. Instead, existing regulators are responsible for enforcing AI-related rules within their domains.

- Flexible compliance: Companies are encouraged to adopt voluntary frameworks, such as the UK AI Safety Institute's guidelines, but there are no mandatory requirements for most AI systems.

Key difference from the EU: The UK's approach is lighter touch and more industry-friendly, with a focus on fostering innovation rather than imposing strict rules.

### 5.2 CHINA: ALGORITHMIC REGULATION

China's approach to AI regulation is centralized and authoritarian, reflecting its broader governance model. Key laws and regulations include:

- Algorithm Recommendation Provisions (2022): Requires companies to ensure that their recommendation algorithms do not promote illegal content, disrupt social order, or infringe on users' rights. Companies must also provide users with the option to opt out of algorithmic recommendations.

- Deep Synthesis Provisions (2023): Regulates the use of deepfake technology, requiring companies to label synthetic content and obtain consent from individuals whose likenesses are used.

- Generative AI Measures (2023): Mandates that generative AI systems undergo security assessments before being released to the public. Companies must also ensure that their systems align with "socialist core values."

Key difference from the West: China's regulations are more prescriptive and less transparent than those in the EU or US. Compliance often requires alignment with the Chinese Communist Party's political priorities.

### 5.3 SINGAPORE: AI VERIFY

Singapore has taken a pragmatic, industry-led approach to AI governance. Its AI Verify program, launched in 2022, is a voluntary framework that allows companies to:

- Self-assess their AI systems: Using a set of principles, including transparency, fairness, and human oversight, companies can evaluate their own AI systems.

- Display a trustworthiness label: Companies that meet the AI Verify standards can display a label indicating that their AI systems are trustworthy.

- Collaborate with regulators: AI Verify is a public-private partnership, with input from industry, academia, and government.

Key difference from the EU and US: Singapore's approach is voluntary and collaborative, with a focus on building trust rather than imposing penalties.

### 5.4 CANADA: AIDA

Canada's Artificial Intelligence and Data Act (AIDA), passed in 2024, is part of the broader Consumer Privacy Protection Act (CPPA). AIDA focuses on:

- High-impact AI systems: Defined as AI systems that could cause harm to individuals or their interests, including physical or psychological harm, discrimination, or economic loss.

- Impact assessments: Companies must conduct impact assessments for high-impact systems, including testing for bias and discrimination.

- Transparency: Requires disclosures for AI-generated content and automated decision-making.

- Enforcement: The Privacy Commissioner of Canada and a new AI and Data Commissioner are responsible for enforcing AIDA.

Key difference from the US: Unlike the US, Canada has a comprehensive federal law for AI, though its enforcement mechanisms are still being developed.

### 5.5 WHY THE WORLD IS NOT CONVERGING

The global divergence in AI regulation is driven by several factors:

- Different political systems: The EU's precautionary approach reflects its consensus-driven, rights-based political culture. The US's reliance on agency guidance reflects its adversarial, litigation-driven system. China's centralized approach reflects its authoritarian governance model.

- Economic priorities: The EU seeks to protect its citizens from AI harms, while the US prioritizes innovation and competitiveness. China aims to control AI for state purposes, including surveillance and censorship.

- Cultural values: The EU emphasizes fundamental rights, such as privacy and non-discrimination. The US values free speech and market freedom. China prioritizes social stability and party control.

- Geopolitical competition: The US and China are engaged in a technological cold war, with each seeking to outpace the other in AI development. The EU, meanwhile, is trying to carve out a third way-balancing innovation with protection.

### 5.6 THE COMPLIANCE CHALLENGE OF GLOBAL DIVERGENCE

For global companies, the lack of convergence creates a multi-layered compliance challenge:

- Conflicting requirements: A system that is compliant in the EU (e.g., meets the AI Act's risk-based requirements) may violate UK principles (e.g., lacks sufficient transparency) or fail Chinese security assessments (e.g., does not align with socialist values).

- Jurisdictional overlap: Companies must navigate multiple regulatory regimes simultaneously. For example, a US-based company operating in the EU must comply with both the EU AI Act and US agency guidance, as well as any relevant state laws.

- Enforcement risk: The risk of enforcement actions varies by jurisdiction. In the EU, companies face fines and bans. In the US, they risk lawsuits and reputational damage. In China, they may face criminal liability for non-compliance.

The only way to address this challenge is through structural compliance: a framework that anticipates all regulatory variants and builds for the strictest possible interpretation.

## 6. THE COMPLIANCE PROFESSIONAL'S DILEMMA: BUILDING FOR UNCERTAINTY

### 6.1 THE PROBLEM: AMBIGUITY, INCOMPLETENESS, AND CONTRADICTION

The compliance gap is defined by three characteristics:

- Ambiguity: Laws and regulations are often vague or open to interpretation. For example, the EU AI Act's definition of "high-risk" is complex and subjective, leaving room for debate over which systems qualify.

- Incompleteness: Many regulations are missing key details or defer to future guidance. The 16-month delay for Annex III in the EU AI Act is a prime example-companies do not know what will be required until the delay expires.

- Contradiction: Different jurisdictions have conflicting requirements. A system that is compliant in California may not be compliant in Colorado, and a system that meets EU standards may violate UK principles.

## 6.2 THE TRADITIONAL APPROACH: CHECKLIST COMPLIANCE

The traditional approach to compliance is checklist-based: companies identify the applicable laws, create a list of requirements, and check off each item as they achieve compliance. However, this approach fails in the face of ambiguity, incompleteness, and contradiction:

- Ambiguity: Checklists assume clear, actionable requirements. When requirements are vague, companies cannot simply "check the box."
- Incompleteness: Checklists are static. When laws are incomplete or evolving, checklists quickly become outdated.
- Contradiction: Checklists assume a single set of requirements. When requirements conflict, companies must choose which to prioritize-a decision that is often arbitrary and risky.

## 6.3 THE SOLUTION: STRUCTURAL COMPLIANCE

The only defensible posture in the face of the compliance gap is structural compliance: a framework that anticipates all regulatory variants and builds for the strictest possible interpretation. Structural compliance has three pillars:

### 6.3.1 ANTICIPATORY COMPLIANCE

Anticipatory compliance involves building for the future, not just the present. This means:

- Monitoring legislative trends: Tracking proposed laws and regulations in all relevant jurisdictions to anticipate future requirements.
- Adopting the strictest standards: When requirements vary, companies should default to the strictest interpretation to ensure compliance across all jurisdictions.
- Investing in flexibility: Designing AI systems to be modular and adaptable, so they can be easily updated to meet new requirements.

Example: A company developing an AI hiring tool should not only comply with current US state laws but also anticipate future federal requirements and EU standards. This might mean conducting third-party bias audits (even if not required in all jurisdictions) and providing detailed explanations for all automated decisions.

### 6.3.2 PRINCIPLES-BASED COMPLIANCE

Principles-based compliance focuses on underlying values rather than specific rules. This involves:

- Identifying core principles: Distilling the common themes across all relevant regulations, such as transparency, fairness, accountability, and human oversight.
- Embedding principles into processes: Ensuring that these principles are baked into the design, development, and deployment of AI systems.
- Documenting compliance: Maintaining detailed records of how principles are applied, to demonstrate compliance in the event of an audit or enforcement action.

Example: The principle of transparency might be applied by:

- Providing clear disclosures about the use of AI in decision-making.

- Offering explanations for how AI systems arrive at their outputs.
- Allowing user control over AI-driven decisions (e.g., the right to opt out or appeal).

#### 6.3.3 RESILIENCE-BASED COMPLIANCE

Resilience-based compliance focuses on preparing for the worst-case scenario. This means:

- Stress-testing systems: Subjecting AI systems to adversarial testing to identify and address vulnerabilities.
- Building redundancies: Ensuring that backup systems are in place in case of failure or non-compliance.
- Planning for enforcement: Developing response plans for potential enforcement actions, including legal defenses and remediation strategies.

Example: A company using AI for credit scoring might:

- Stress-test its model for bias against protected classes (e.g., race, gender).
- Maintain a human review process for high-stakes decisions.
- Develop a remediation plan in case of an enforcement action, such as refunding affected consumers or updating the model.

### 6.4 THE ROLE OF TECHNOLOGY IN STRUCTURAL COMPLIANCE

Technology can play a key role in enabling structural compliance:

- AI governance platforms: Tools such as IBM Watson OpenScale, Fiddler AI, and Arize AI can help companies monitor, audit, and explain their AI systems, ensuring compliance with transparency and fairness requirements.
- Regulatory technology (RegTech): Platforms like ComplyAdvantage and Onfido can automate compliance monitoring and reporting, reducing the burden on legal and compliance teams.
- Automated documentation: Tools such as GitHub Copilot and Jupyter Notebooks can help companies document their compliance efforts, making it easier to demonstrate adherence to principles and requirements.

### 6.5 THE COMPLIANCE PROFESSIONAL'S TOOLKIT

For compliance professionals, navigating the compliance gap requires a multi-disciplinary toolkit:

TOOL | PURPOSE | EXAMPLE TOOLS/RESOURCES

LEGISLATIVE TRACKING | MONITOR PROPOSED LAWS AND REGULATIONS | FISCALNOTE, BLOOMBERG GOVERNMENT, LEXISNEXIS

REGULATORY ANALYSIS | INTERPRET AND COMPARE REQUIREMENTS ACROSS JURISDICTIONS | THOMSON REUTERS, WOLTERS KLUWER

AI AUDITING | TEST AI SYSTEMS FOR BIAS, FAIRNESS, AND TRANSPARENCY | IBM AI FAIRNESS 360, GOOGLE WHAT-IF TOOL

DOCUMENTATION | MAINTAIN RECORDS OF COMPLIANCE EFFORTS | CONFLUENCE, NOTION, GITHUB

LEGAL COUNSEL | ADVISE ON ENFORCEMENT RISK AND LIABILITY | IN-HOUSE COUNSEL, EXTERNAL LAW FIRMS

### 6.6 CASE STUDY: BUILDING A DEFENSIBLE AI COMPLIANCE POSTURE

Company: A global financial services firm using AI for credit scoring.

Challenge: The firm operates in the EU, US, and UK, each with different AI regulations. It must ensure that its AI credit scoring model complies with:

- The EU AI Act (high-risk classification, bias testing).
- US state laws (e.g., California's bias audit requirements).
- UK principles (transparency, fairness).

Solution: The firm adopts a structural compliance approach:

- Anticipatory compliance:
- Monitors legislative developments in all jurisdictions.
- Adopts the strictest standards (e.g., third-party bias audits, detailed explanations for all decisions).
- Designs its AI model to be modular, so it can be updated as requirements evolve.
- Principles-based compliance:
- Embeds transparency, fairness, and accountability into its AI development process.
- Provides clear disclosures to consumers about the use of AI in credit decisions.
- Offers explanations for how the model arrives at its outputs.
- Resilience-based compliance:
- Stress-tests its model for bias against protected classes.
- Maintains a human review process for high-stakes decisions.
- Develops a remediation plan in case of an enforcement action.

Outcome: The firm achieves defensible compliance across all jurisdictions, reducing its risk of enforcement actions and reputational damage.

## 7. CONCLUSION: AMBIGUITY AS A FEATURE, NOT A BUG

The compliance gap in AI regulation is not an accident. It is the inevitable result of political compromise, jurisdictional competition, and the influence of powerful lobbying groups. The EU AI Act was watered down to secure unanimous support. The US federal vacuum persists because of partisan gridlock. The state patchwork grows because of the absence of federal leadership. And global divergence continues because of differing political systems, economic priorities, and cultural values.

For companies, the uncertainty is not a bug to be fixed but a feature of the political process. The only way to navigate this landscape is to embrace the ambiguity and build for it. Structural compliance-anticipatory, principles-based, and resilience-focused-is the only defensible posture in a world where the rules are always changing.

### 7.1 THE FUTURE OF AI REGULATION

Looking ahead, several trends are likely to shape the future of AI regulation:

- More patchwork, not less: The state patchwork in the US will continue to grow, and other countries may follow the EU's lead with their own comprehensive AI laws. The result will be more divergence, not less.

- Agency activism: In the absence of federal legislation, US agencies will continue to fill the gap with guidance and enforcement actions. This will create a de facto regulatory regime that is unpredictable and inconsistent.

- Global fragmentation: The world is not converging on a single AI standard. Instead, it is moving toward regional blocs, with the EU, US, and China each promoting their own models.

- Technological outpacing: AI technology is evolving faster than regulation. By the time laws are passed, they may already be outdated or irrelevant.

### 7.2 THE STRATEGIC IMPERATIVE

In this environment, companies that wait for certainty will always be behind. The strategic imperative is to build for uncertainty:

- Invest in structural compliance: Develop frameworks that anticipate all regulatory variants and build for the strictest possible interpretation.

- Engage with policymakers: Shape the regulatory landscape by participating in public consultations, joining industry groups, and advocating for sensible rules.

- Collaborate with peers: Work with other companies to develop shared standards and best practices, reducing the burden of compliance for everyone.

- Prioritize transparency: Be open about AI use, decisions, and limitations. Transparency builds trust with regulators, consumers, and the public.

### 7.3 FINAL THOUGHT: THE REGULATORY THEATRE

The title of this white paper-The Regulatory Theatre-refers to the performative nature of AI regulation. Laws are passed, guidance is issued, and enforcement actions are taken, but the underlying ambiguity remains. The theatre is not without purpose: it provides the illusion of control in a rapidly changing technological landscape. But for companies, the show must go on. The only way to avoid being a mere spectator is to take the stage-to shape the narrative, influence the script, and build a compliance posture that is as dynamic as the regulations themselves.

SCHEDULE A SOVEREIGNTY AUDIT TO ASSESS YOUR ORGANIZATION'S READINESS FOR THE REGULATORY THEATRE.

This white paper is a product of FYNYGRYF GROUP. For inquiries, contact Anthony Leavitt at anthony.leavitt@fynygryf.group.