# Top Trends in AI Public Policy and Regulations for 2024

Published 17 November 2023 - ID G00805314 - 48 min read

By Analyst(s): Katell Thielemann, Brian Prentice, Bart Willemsen, Nader Henein, Tsuneo Fujiwara, Svetlana Sicular, Christie Struckman, Jorge Lopez, David Gregory

Initiatives: Executive Leadership: Enterprise Strategic Planning and Execution; Digital Future

As governments globally attempt to define policies and regulations for trustworthy and responsible AI, executive leaders must anticipate their emergence. We provide executive leaders with the nine trends driving policymaking today, and their implications for enterprise strategic plans.

## Overview

### Opportunities

- As policymakers and regulators around the world ponder the impact of AI and how to safely deploy the technology in their jurisdictions, executive leaders should anticipate what regulatory focus areas will rise to prominence.
- Much can be learned from the prior deployments of technologies with profound societal impacts, such as social media, and those lessons learned directly inform the nine top trends in this research.
- But AI also poses new and different challenges for societies and organizations alike, so it is imperative for executive leaders to become familiar with them and ponder how they will prepare their organizations for them.

### Recommendations

Executive leaders seeking to inform their enterprise strategic planning should:

- Become familiar with the AI policy and regulations efforts underway in all jurisdictions where they operate. Use them as a baseline for your own policies, but don't rely on them alone to prepare your organization.

- Review their strategic plans in light of the nine top trends in this research to create a SWOT (strengths, weaknesses, opportunities, threats) analysis of what these policy trends could mean for their own organizations and industries.
- Develop their own internal AI policies, using inputs from across their enterprise and the trends in this research, and release them in plain language, easily understandable by all employees.

## Strategic Planning Assumptions

By 2027, the productivity value of AI will be recognized as a primary economic indicator of national power.

By 2025, the concentration of pretrained AI models among 1% of AI vendors will make responsible AI a societal concern.

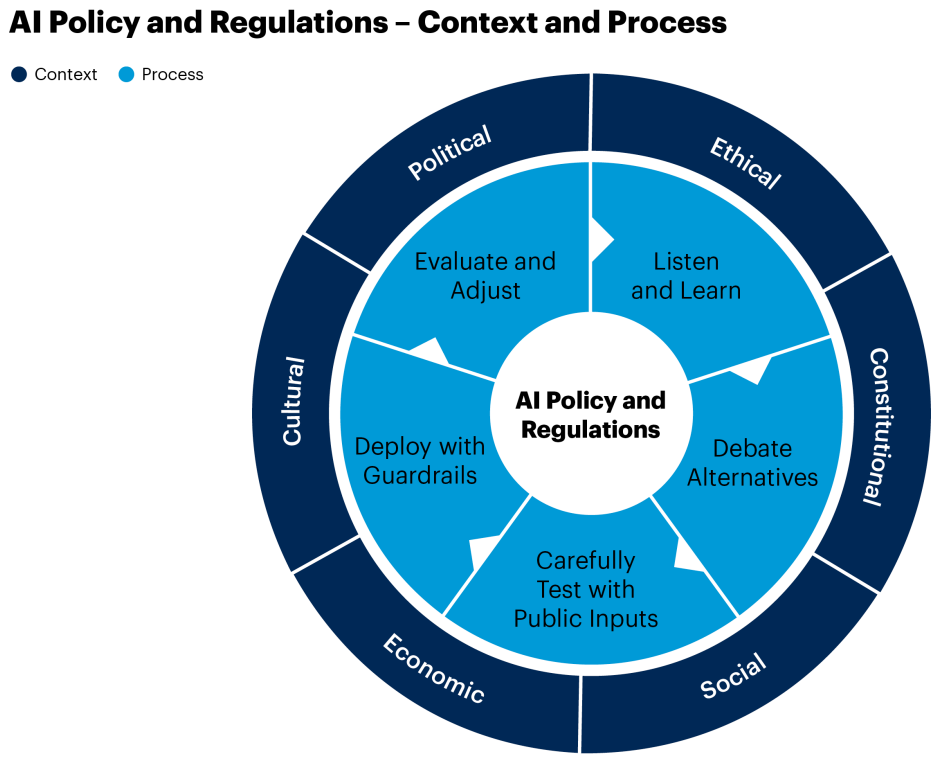
## What You Need to Know

AI, particularly machine learning, has been around for the past two decades, and has been incorporated into thousands of products and services, many of which have become automated.

With the democratization of access to generative AI (GenAI), and the many new solutions it is helping to create to solve business problems, many more products and services will be moving in that direction. However, this will happen at unprecedented scale and speed, and with unpredictable impacts on all aspects of societies.

Because of the level of excitement for — and fear of — AI and GenAI, policy and regulatory work is emerging in most countries globally. These efforts are happening at all levels of jurisdictions (national, state, local) according to their ethical, constitutional, social, economic, cultural and political underpinnings (see Figure 1).

Figure 1: AI Policy and Regulations — Context and Process




Source: Gartner
805314_C

Gartner

As a global technology and business advisory firm, Gartner enjoys a unique position of visibility across public- and private-sector end users, vendors, and academic institutions alike. Through tens of thousands of yearly interactions and numerous published research notes on the responsible use of AI and AI governance, we have inventoried the nine top trends policymakers and regulators are currently pondering. These should be considered by executive leaders as they develop their strategic roadmaps for the next 5 years.

These trends are directly relevant to many roles, including:

- **Chief executive officers (CEOs),** who will need to steer their organizations both internally and in the new competitive landscape that AI will create, with yet-to-be-defined rules of engagement.
- **Chief information officers (CIOs),** who will need to successfully deliver digital transformation efforts with AI at unprecedented scale and speed.
- **Chief financial officers (CFOs),** who will have to make ROI decisions in a rapidly changing dynamic environment with few guardrails.

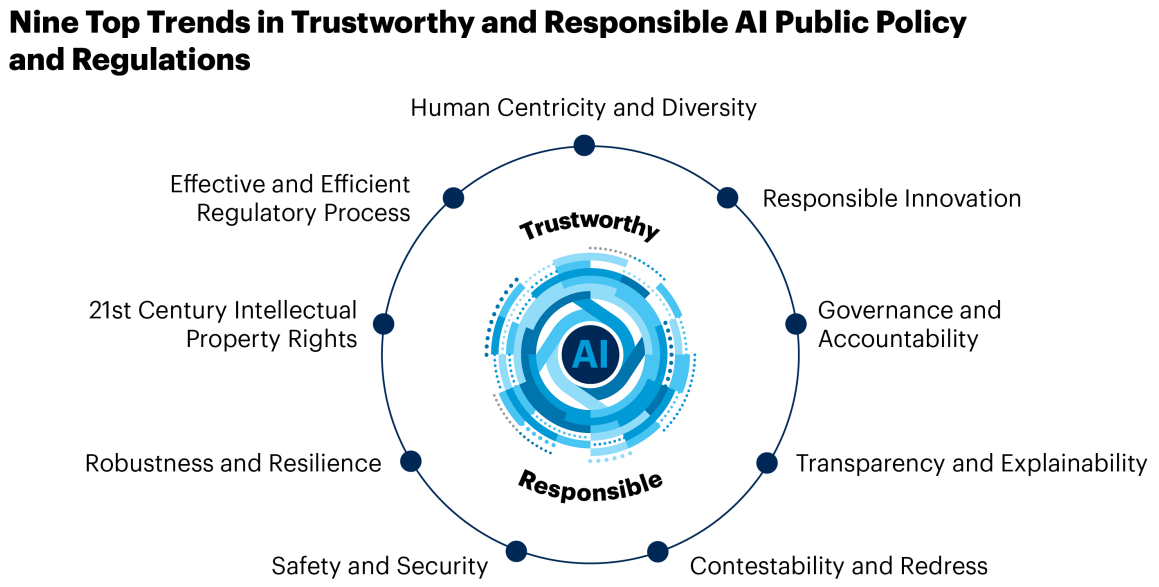
- **Chief human resources officers (CHROs),** who will have to make many decisions about skills, hiring and employee relations in a new world of AI ubiquitous in the workplace.
- **General counsels (GCs),** who will need to maneuver through an unsettled regulatory environment and emerging jurisprudence in a mosaic of approaches from one jurisdiction to the next.
- **Chief data analytics officers (CDAOs),** who will see their roles elevated in importance as all other C-suite leaders turn to them for guidance.
- **Chief information security officers (CISOs),** who will see the threat landscape dramatically increase, but will also be able to tap AI for better detection and response to cyberattacks.

**Table 1: Trends Profiles: Click links to jump to profiles**

| | | |
|---|---|---|
| Human Centricity and Diversity | Responsible Innovation | Governance and Accountability |
| Transparency and Explainability | Contestability and Redress | Safety and Security |
| Robustness and Resilience | 21st Century Intellectual Property Rights | Effective and Efficient Regulatory Process |
| | | |

Source: Gartner

Figure 2: Nine Top Trends in Trustworthy and Responsible AI Public Policy and Regulation




## Human Centricity and Diversity

*Back to Top*

*Analysis by Svetlana Sicular, Christie Struckman*

**Description:**

Even though technology should not exist for technology's sake, human centricity is too often overlooked. Human-centered AI is a design principle calling for AI to benefit people and society. It assumes a partnership model of people and AI working together to enhance cognitive performance, including learning, decision making and new experiences. It is sometimes referred to as "human in the loop," "augmented intelligence" or "centaur intelligence," but in a wider sense, even a fully automated system must have human benefits as a goal.

> **Only 55% of IT and information security leaders responding to a 2023 Gartner Peer Connect survey said they use or plan to use humans in the loop as one of the strategies to mitigate risks associated with generative AI tools or foundational models.1**
>
> — *Gartner (2023)*

AI has the potential to greatly help humans, whether from advances in medicine or by automating mundane, repetitive or risky tasks to usher in more time for human creativity.

Human centricity can also help AI. While foundation models (the basis of GenAI) have been around for some time, developing without much fanfare, ChatGPT attracted over 1 million users in just five days, [2] because its design is human-centric, both in approachable user interface and in natural-language outputs, to which humans can easily relate.

But we also know from history that, left unchecked, organizations focused on monetizing clicks and dwell times to push marketing revenue can deploy technology dangerous to people. They will often harness addictive and harmful tactics, lulling people in a sense of false confidence in their decisions. In its push to automate, AI can also exacerbate long-standing human ethical and moral dilemmas, such as:

- The classical trolley problem: An ethical dilemma about which action to pursue when one path would save one person, and another would save five. Should AI solve autonomously for the value of life? Would you develop a good-enough model for a medical treatment covered by insurance, or the best possible procedure that might not be covered by insurance?
- Equity vs. equality problems: Optimizing for equality (around one parameter, such as age, gender or race), is already a challenge for AI. Optimizing for equity (which requires combinations of all these parameters) is many orders of magnitude more difficult. Would you hire a woman with disabilities, or a 60-year-old African-American man? Where is the slippery slope of using too much facial recognition to find criminals in public transportation, even if you mistakenly arrest the wrong person along the way?

At the same time, because they are created by humans, technologies carry the biases of their creators — humans are fallible as well. Yet humans select the problems to solve, and they evaluate the solutions. Humans must ask the "right" questions and spot the "right" answers. Humans must select the "right" data and apply the "right" algorithms. Humans test and validate AI; they provide feedback.

While a lot of effort today is directed at understanding AI training and learning, very little time is spent focusing on the human teaching challenge. How does one select the "right" humans to manage the process? Human teaching differentiates the best models from the mediocre ones; it can save resources and safeguard AI systems. How to ensure that our educational systems are geared toward ensuring critical thinking, if that's what will differentiate human performance? How does one prevent harm to humans as they review offensive outputs? A new role of "AI rater" has emerged, and increasingly, these raters are speaking up about how undertrained, underpaid, and stressed they are. [3]

Just as importantly, how do organizations prevent biases from creeping in, even involuntarily? When it comes to AI, those biases can be dangerously extrapolated at scale.

One core way to deal with biases is to ensure diversity of inputs into AI. This could include diversity of datasets, diversity of algorithmic use, diversity of regional languages and cultures, diversity of skill sets and disciplines, or even diversity in determining what problems to solve with AI. Prominent AI researchers argue that diversity in AI carries important economic, innovation ("power of the crowd" versus "group think"), and societal fairness implications. [4]

**Why Trending:**

Human centricity and diversity are cornerstone principles of Trustworthy and Responsible AI, and increasingly included in AI policy and regulations discussions in the European Union, [5] in Japan, [6] in the U.S., [7] or in Australia. [8]

Some technology companies are also starting to realize the value of human-centric AI. Examples include:

- IBM's AI Principles: "The purpose of AI is to augment human intelligence." [4]
- Microsoft CEO public statements: "Humans need to be 'unquestionably' in charge of powerful AI to keep things from getting out of control." [9]

- Google investment in targeted research team: “People + AI Research (PAIR) is a multidisciplinary team at Google that explores the human side of AI by doing fundamental research, building tools, creating design frameworks, and working with diverse communities.” [10]

**Implications:**

Executive leaders should expect AI policymakers and regulators to:

- Revisit the foundation of existing educational systems and look for reengineering opportunities. New approaches to education are required to support human centricity and diversity, and should include:
  - Critical thinking education — necessary to take advantage of the right approaches among a plethora of available ones and to protect people from disinformation and other AI harms.
  - Personalized education: AI enables people to learn in the best possible way for everyone. This will take society to the next level of literacy and aptitude.
  - Ways to enable more people to study AI, and actively recruit so that they come from diverse backgrounds.
- Prioritize research and development efforts on the “human teaching AI” discipline, along with the current focus on “AI training/learning.”
- Require the role of AI validators, to ensure transparency about:
  - The diversity and provenance of data used to fully represent the intent sought, as well as the diversity of data that includes adversarial examples to ensure models work as designed
  - The diversity of models, depending on the problem/decision context, to assure AI robustness, transparency and resilience to adversarial conditions
  - The diversity of thought and backgrounds of humans involved
- Consider both large generative foundation models that aggregate a diversity of data, methods, and creators, as well as smaller predictive and generative (often open-source) models that recognize differences in language, culture, history, laws, social norms, economic ambitions and the like.

**Actions:**

- Develop a mechanism of involving diverse people to give varied perspectives, and to ask and answer the hard AI-related questions. Set expectations that the answers will drift over time. Ensure continuous monitoring of the AI's output to capture the drift and other issues in a timely manner.
- Plan a responsible AI strategy to equally focus on intentions and consequences. Establish metrics, measures and criteria to encourage people to do the right things and provide valuable feedback. Develop and put in place measures before and after the AI technology is rolled out.
- Be intentional and transparent about AI-related human actions, including (but not limited to) decisions. The most fundamental part of human-centered AI is actions, not just principles. Define policies to concentrate on the greatest business and societal impact, while leaving creative freedom to people, enabling them to deliver human-centered AI productivity and breakthrough solutions that recognize diverse environments.

**Further Reading:**

Activate Responsible AI Principles Using Human-Centered Design Techniques

A Comprehensive Guide to Responsible AI

Postdigital Governments Must Use Human-Centered Design to Build Cognitive Empathy

## Responsible Innovation

*Back to Top*

*Analysis by Jorge Lopez, Katell Thielemann*

**Description:**

Innovation can take many forms. For instance, innovation can be accidental or purposeful, tightly controlled or democratized, done via public funded resources or in the secrecy of a stealth startup, proprietary or open-sourced. When it comes to AI, it can be all of the above and more.

For policymakers and regulators, it will be a careful balancing act:

- On one side, inappropriate, weak, poorly funded, uncoordinated, laissez-faire approaches to innovation can have negative effects on a global scale, as evidenced by the societal impacts of social media platforms.
- On the other hand, a command-and-control regulatory approach would stifle innovation and put countries at a competitive disadvantage on the global stage.

Novel approaches will likely include the use of test beds, living labs, and "regulatory sandboxes" that provide testing environments for innovation, with guardrails for public health, safety and consumer protections. However, these approaches should also lift other existing restrictions to allow for exploration and testing during a predetermined time limit. [11]

**Why Trending:**

When it comes to AI, the stakes are so high — geopolitically, economically and societally — that a determined approach to responsible innovation will be a focus for countries and organizations alike in the future.

> **Thirty-two percent of technology leaders responding to a 2023 Gartner Peer Connect survey, who said their organizations currently use generative AI beyond ChatGPT, cited research and development as one of the use cases.[12]**

Responsible innovation is a cornerstone principle of trustworthy and responsible AI, and is increasingly included in AI policy and regulations discussions to ensure that AI is:

- Purposeful, with a stated goal that can be referred to over time to check for drift from original intent.
- Not prebiased to a specific result by manipulating inputs, process or outputs.

- Ethics-based: Whether they are public-sector-oriented, industry-specific, or in private companies or academia, R&D organizations should follow a code of ethics transparent to the public.
- Shareable: Research data created by public funds should be curated, widely shared and maintained under open data policies.
- Documented, peer-reviewed, and published in plain language nonexperts can understand.
- Cross-disciplined, diverse, inclusive, accessible.
- Incentivized to overcome the traditional "Valley of Death" for emerging technologies, moving from research to commercialization and prototypes to industrialization.
- Nimble and designed to prevent "too big to fail" issues when deployed.

An example is the U.S. National Artificial Intelligence Research and Development Strategic Plan, updated in May 2023. [13]

**Implications:**

Executive leaders should expect AI policymakers and regulators to:

- Mandate all publicly funded AI R&D investments to be outcomes-based (as opposed to requirements-based), to allow for human creativity in achieving goals.
- Incentivize the bidirectional flow of ideas and innovations between public and private organizations by simplifying government acquisition processes and bringing IP protection frameworks into the 21st century.
- Create test beds, living labs, or "regulatory sandboxes" to test innovation at societal scale, with applicable guardrails in place for public health, safety, privacy and consumer protection.

- Create national-level labs for research and development. These organizations should:
  - Have defined charters
  - Openly communicate with the public on efforts and outcomes, and provide a feedback mechanism
  - Engage widely with academia and the private sector
  - Specifically earmark investments for open-source AI guardrails
  - Fund societal-impact research that individual corporations are not incentivized to self-fund
  - Create frameworks for international cooperation

**Actions:**

- Define an AI R&D anchored to outcomes-based goals.
- Look for opportunities in government R&D efforts to incentivize research. This could take the form of public-sector contracts, opportunities to commercialize R&D efforts from academia, or the ability to leverage large datasets shared by the public sector with private industry.
- Ensure internal R&D teams develop, document and train employees on ethics-based research guardrails.

**Further Reading:**

Use Generative AI in Applied Innovation to Drive Business Value

Target Impactful Innovations With a Customized Innovation Framework

## Governance and Accountability

*Back to Top*

*Analysis by Tsuneo Fujiwara, Bart Willemsen*

**Description:**

Governance and accountability are core societal principles, and traditional approaches attempt to find balance between control and autonomy by establishing guardrails supported by policies, rules and laws, as well as institutions such as law enforcement and court systems.

In the case of the scale and speed of innovation in the field of AI, traditional governance approaches based on policies, metrics and hierarchical organizational layers are challenged. These approaches must become adaptive throughout the innovation life cycle, as well as at all levels of an organization. This means both enterprise governance and accountability, as well as data governance and accountability. Traditional command-and-control approaches will stifle innovation, while complete autonomy will yield unpredictable results. Meanwhile, transparent accountability leads to good governance.

Additionally, it remains largely unsettled which roles within organizations are responsible, accountable, consulted and/or merely informed (RACI matrix). Even if responsibility is shared, the various roles involved need to know what part each has to play.

**Only 42% of IT and information security leaders responding to a 2023 Gartner Peer Connect survey said they use or plan to use AI governance as one of the strategies to mitigate risks associated with generative AI tools or foundational models.[1]**

**Why Trending:**

Without governance and accountability, policies and regulations are worthless. The increasing complexities involved with the use of AI technology mandate an approach that creates structure out of chaos.

For this reason, some policymakers and regulators are evaluating a three-pronged approach for AI governance. This approach is structured with the following elements:

**Element No. 1: Define a risk-informed AI governance framework.** This will help to frame the intent and purpose of AI deployment based on a jurisdiction's ethical, cultural, constitutional, political, economic or social context. For example, the risk factors could be based on:

- Cost-benefit of having mandated humans in the loop, level of skills of these people, bias-controlled training for the people and the like
- Societal impact (for example, any intent or purpose to target minors or other vulnerable populations should be controls-based)
- Thresholds of number of impacted citizens (for example, any intent or purpose that will affect more than 2% of the population should, at a minimum, be outcomes-based)
- Pedigree of source data (for example, to align to an agility-based or autonomous style, all data must be from trusted sources, following an established, fully transparent life cycle)
- Complexity of algorithms, their ecosystems and their interactions over time, with the need to remain explainable
- Concentration risks of providers and opacity of automated decision making at scale in sectors underpinning critical infrastructure (for example, automated contracts and negotiation models that could have massive impacts on financial markets if hacked)

**Element No. 2: Define a range of categories based on this risk-based framework for intent and purpose.** These categories could include:

- Prohibited activities — Governance prohibits, by law or internal policies, the use of AI for certain societally undesirable purposes, and accountability comes with severe punishment, including criminal penalties. Examples could include commercial AI applications designed to harm humans, disrupt society at large or discriminate at scale, as well as other applications prohibited by laws.
- Controls-based governance and accountability — Decision making according to rules, policies, standards and directives dominates this style. Activities controlled by law or regulatory compliance requirements (e.g., to support safety or privacy mandates) find this style of governance most appropriate.
- Outcomes-based governance and accountability — Achieving outcomes while balancing risk, return and performance on investments, within organizational guardrails. This style is appropriate when dynamic business processes and risk appetite change the way that organizational outcomes are achieved. Initiatives such as multichannel customer experience and supply chain analytics find this governance style suitable.

- Agility-based governance and accountability — Empowering roles and teams with the authority to make distributed and/or mandated decisions that create value for the organization. This style relies more on people's competencies, principles, attitudes and ways of working, rather than on authority and/or rules. It can best support AI activities, such as self-service or internal innovation labs, within ethically mature organizations in self-contained and controlled environments.
- Autonomous governance and accountability— Driving value and managing risk from decisions made in real time by people and "things." In some AI scenarios, human intervention in decision making impedes realization of business value or mission outcome. Fraud detection AI algorithms, for example, use distributed data sources and real-time threat intelligence to make autonomous decisions.

**Element No. 3: Define roles and responsibilities/decision rights and accountability.** This is necessary because AI is a human-created technology with no agency on its own. Examples of roles include:

- Users
- Providers (internal and external), to include designers, creators, validators, trainers, suppliers, service providers, deployers, controllers, auditors or processors
- Overseers: Board directors, digital ethics boards, inspectors general in public-sector agencies, independent oversight agencies for GenAI large language model (LLM) creators and the like

For all these roles, responsibilities/decision rights and accountability should follow. For example:

- Creators of AI should have a responsibility to clearly articulate the potential and actual human impact of their work.
- Users should have a responsibility and opportunity to protect their sensitive data and IP. Users should also have disclosure, contestability and redress decision rights.
- Providers should have a responsibility to deploy monitoring capabilities to detect and intervene in case of data drift, model drift or unintended outcome, as soon as it occurs.

- Trainers should have a responsibility to explain the provenance of data, the legitimacy of its use for a stated purpose, the curation of the data for this purpose and transparent demonstration of bias control mechanisms.

**Implications:**

Executive leaders should expect AI policymakers and regulators to:

- Define a risk-based framework aligned to ethical, constitutional, political, economic, cultural and social concepts applicable to the jurisdiction in question.
- Set the stage for adaptive governance and accountability throughout the entire AI life cycle along a prohibited, controls-based, outcomes-based, agility-based and autonomous spectrum.
- Articulate and define specific roles, along with requirements and decision rights for each.
- Evaluate the need to create a stand-alone governmental agency to create registration, licensing and oversight mechanisms. This should start with a focus on the highest-risk scenarios that mandate a prohibited or controls-based approach, where requirements, and decisions rights will be difficult to enforce.
- Outline conditions of AI providers' and users' accountability for erroneous outcomes.

**Actions:**

- Define governance rules, roles, structures, processes and culture based on business impact and complexity of the potential AI solution to be implemented.
- Confirm that the AI output is abiding by regulations by enhancing control on biases within the model, following corroboration and validation of output within the different jurisdictional expectations of what is and is not considered acceptable to train AI tools.
- Devise a mechanism to continuously monitor and correct any AI output that is not abiding by regulations or conforming to governance rules.

**Further Reading:**

Applying AI — Governance and Risk Management

How to Ensure Your Vendors Are Accountable for Governance of Responsible AI

4 AI Governance Actions to Make a Swift Business Impact

## Transparency and Explainability

*Back to Top*

*Analysis by Nader Henein, Brian Prentice*

**Description:**

As data mining emerged in the early 2000s, many organizations realized the value of data insights to build products and services that would attract more prospects and drive engagement. This transition heralded a new age where data became the "new oil" — a commodity that would be collected, processed and reprocessed for value and profit. This transition happened fast and lacked transparency in intent, data provenance, and methods used. Users ("data subjects") were rarely consulted, and slowly cumbersome and confusing terms of service appeared to retroactively grant organizations unlimited usage rights to data collected. [14]

When it comes to AI, explainability attempts to answer the seemingly simple question of "How was this decision reached?" With models that seek to classify circles and squares into two categories of shapes, it is fairly easy to diagram the decision tree followed by the AI model to reach a final state. But with complex neural networks that include hidden layers, explainability becomes orders of magnitude harder. Today, with LLMs that have billions of parameters, it is nearly impossible to explain how an answer was reached with any level of confidence.

**Only 19% of IT and information security leaders responding to a 2023 Gartner Peer Connect survey said they are using or implementing tools for model explainability, and only 24% said they are using or implementing tools for model monitoring to address risks.[1]**

**Why Trending:**

Governments globally, such as in the U.K., [15] the U.S., [16] and Australia [8] are focusing on transparency and explainability, because they are necessary for effective policies and regulations:

- Only with transparency and explainability can oversight and accountability take place.
- Explainability, particularly, forms the basis of verification. It allows a demonstration of fairness and oversight over potential bias. From a liability standpoint, explainability also allows a determination of fault, should the models prove inaccurate and lead to harm. This is especially important if a component (such as a foundational model) is provided by one party, then adjusted or exploited by another.
- Transparency and explainability are a cornerstone of trustworthiness, and discussions currently center around users' reasonable rights to know, balanced against IP protection, when it comes to:
  - The very intent and purpose for the existence of AI
  - The training of AI models
  - The inputs into AI models, including transparency of complex data pipelines (transformations), the origins of data sources, and a means to detect and mitigate human bias in the original data
  - The inner workings of the models themselves
  - The outputs of AI models, including explainability specific to various personas who receive these outputs

**Implications:**

Executive leaders should expect AI policymakers and regulators to:

- Ensure that providers (internal and external), to include designers, creators, validators, trainers, suppliers, service providers, deployers, controllers, auditors or processors of AI systems make available accessible plain-language documentation, including:
  - Notification of AI use
  - Clearly articulated purpose and intent of the AI system
  - Clear descriptions of overall system functioning (to include data used, how model is trained, and any mechanism, algorithmic or human, that is used to supervise outputs)
  - Notice that such systems are in use, and their maintenance/monitoring conditions
  - The individual or organization responsible for the system, and explanations of outcomes that are clear, timely and accessible
  - A feedback loop that enables users to easily share their opinions on the AI insights they received, to improve the model when it's important
- Disallow disclosure of the information above to be buried within terms and conditions or acceptable use policies. Instead, this information will likely have to be provided as a product/service commitment prior to the user employing the AI-integrated solution, to ensure that:
  - Consumers are allowed to assess what an AI product/service does relative to what is promised and, if divergent, they should have access to redress through truth in advertising or product liability laws.
  - Organizations procuring AI have full visibility into the AI practices of their supply chains and contractually mandate adherence to the trustworthy and responsible AI policies and regulations of their jurisdictions.
  - AI providers do not use complex legal agreements that average users cannot understand or challenge.
- Allow for vetted, independent third parties to be able to access and audit AI models in the prohibited, controls-based and outcomes-based governance categories

- Prioritize research and development efforts on:
  - Understanding the existing motivations for and mechanisms of today's opacity challenges
  - Anticipating what new ones may come up as the result of AI
  - Developing mitigating solutions that will support end-user trust

**Actions:**

- Establish a clear set of guidelines for customer transparency, grounded in both the organization's regulatory duties and its environmental, social and corporate governance (ESG) principles.
- Provide individual users with a clear and concise outline when their data is used to train machine learning models, or when they are subject to automated decision making. Transparency is not simply a matter of regulatory requirement; it is the basis for developing and maintaining positive sentiment with your customers.
- As your organization adopts and/or trains AI capabilities for the purpose of decision making, ensure that you maintain the capacity to explain how decisions are reached. A detailed, step-by-step outline may not be possible, but the organization should maintain the capacity to reach the same outcome through traditional means.
- Appoint an executive sponsor that has the authority to ensure that the organization's guidelines for transparency are tracked and followed.
- Track the evolution of government regulation as it relates to transparency obligations, with the expectation that there is unlikely to be consistent regulations between countries.

**Further Reading:**

10 Privacy Policy Updates to Boost Transparency and Achieve Compliance

Market Guide for Consent and Preference Management

Lack of Focus on AI Licensing Will Result in Higher Costs, Risks and Long-Term Headaches

## Contestability and Redress

*Back to Top*

*Analysis by Nader Henein*

**Description:**

AI has found its way in an increasing number of use cases over the last decade. However, users have historically not been made aware when their data is used to train models upon which AI capabilities are built, or when they are subject to the automated decision making that impacts their daily lives.

Should they be made aware, most users currently have no mandated and/or standardized recourse to:

- Object to the automated processing of their data for training purposes.
- Request models be retrained without their data.
- Object to the automated processing of their data for decision.
- Request clarification as to how an automated decision was reached (explainability).
- Raise a complaint with a regulatory body that is empowered to investigate and assess the automated decision-making process against a set of rights and requirements.

**Why Trending:**

Policymakers and regulators are focusing on this trend because user empowerment is a cornerstone of public trust. The U.K., [15] China [17] and Australia [8] are examples of countries looking at contestability and redress as a component of trustworthy and responsible AI.

They realize that, to prevent trust erosion or excessive unwarranted trust, users must be afforded a contestability and redress process to air their concerns. Further, the concerns should be addressed in a structured forum through an organization with proper legal authority, and with a defined and unambiguous mandate to create a level playing field available to all.

This will also allow innovation to continue without hindrance, while maintaining the needed guardrails to protect users from the unintended harm that comes with any emerging technology.

**Implications:**

Executive leaders should expect AI policymakers and regulators to:

- Establish an independent organization with the authority to act as a clearinghouse or proxy, logging user concerns, managing escalations and dispensing regulatory orders based on a set of defined principles.
- Mandate that organizations:
  - Maintain and keep up to date (at least every six months) a public "automated data processing notice" where users can review the use cases where their data is subject to automated (AI-based) processing, or AI-based decision making.
  - Provide a process where users and organizations can raise a concern relating to the automated processing of their data or IP.
  - Define a time limit (for example, 45 days) for the organization to address the concern.
  - Introduce an escalation process so at the end of the time limit, if the concern is not satisfactorily addressed, the affected party can choose to escalate their concern to an independent clearinghouse or other designated regulatory body for:
    - Investigation to determine the accuracy of the automated data processing notice.
    - Assessment of whether harm has occurred, and what redress (to include fines) may be necessary.
    - Action, including suspension of processing data as needed, until the matter is resolved to the satisfaction of the clearing house/regulator.

**Actions:**

- Track both your organization's regulatory and reputational exposure to consumer rights when using personal data to train new AI models, or when an individual is subject to automated decision making.
- Work across the C-suite to gain visibility into which data the organization manages, as well as current and planned future business uses of that data.
- Coordinate with system owners to create a process that captures consumer complaints in a structured workflow and tracks communication timeliness, as well as response efficacy.
- Ensure your organization has the capacity to remediate consumer escalations satisfactorily, within reason. Institute governance policies, such as data retention for both internal and external (e.g., customers, partners) data, and that the policy has a process to manage exception requests.

**Further Reading:**

Progress Update: How Privacy Leaders Are Responding to CPRA Retention and Deletion Requirements

Practical Privacy — Managing Data Retention and Backups

Guidebook for Implementing a Data Deletion Initiative

## Safety and Security

*Back to Top*

*Analysis by Katell Thielemann*

**Description:**

AI, like any human-created technology, can create opportunities to enhance security and safety practices — for example, by:

- Enhancing vulnerability detection
- Reducing false positives
- Improving clarity in uncertain situations

- Providing remediation assistance
- Automating code documentation
- Enrichment of security alerts with contextual information

> **By 2027, generative AI will contribute to a 30% reduction in false positive rates for application security testing and threat detection by refining results from other techniques to categorize benign from malicious events.[18]**
>
> — *Gartner Strategic Planning Assumption*

But AI, like any human-created technology, is also fallible and can create many security and safety risks in the hands of bad actors, from hacktivists to nation-states who seek to deploy adversarial AI, which could include:

- Misinformation/disinformation
- Fraud schemes
- Data leaks/exfiltration
- Data poisoning
- Data manipulation
- Supply chain attacks
- Model training tampering
- Adversarial model duplication
- Prompt injection
- Malware code generation
- Vulnerability detection
- Synthetic identities and impersonation

- Hyperautomation of attacks at a scale and velocity that overwhelms defenses

In addition, security and safety risks can occur throughout the entire AI life cycle while designing, creating, testing, deploying, procuring, maintaining or retiring it.

**Respondents to the 2023 Gartner CIO Generative AI Survey said that "[r]isk of misuse with bad actors creating higher-quality misinformation, phishing emails, malware, fraud and spam" was their top concern about GenAI (56%), followed by 'hallucination' of facts and making reasoning errors (50%).[19]**

**Why Trending:**

Unfortunately, humans have decades of failed experiences with secure and error-free technology, from Edison's "bug" in the 1878 quadruplex telegraph system to ever-increasing disclosed cybervulnerabilities databases. AI can create many safety and security hazards for humans, whether financial, emotional or otherwise, with embezzlement, blackmail, bullying, political or reputational damage threats.

In addition, because automation efforts are driving increasingly connected physical assets to become cyber-physical systems (CPS), concerns over human physical safety can no longer be dissociated from worries about cybersecurity.

In the 1980s, a "bug" in the code that controlled the Therac-25 radiation therapy machines resulted in the deaths of patients. [20] By the 2010s, we had moved from "bugs" to malware specifically designed to harm humans in industrial facilities. [21]

History is repeating itself — as the scale and speed of AI innovation and deployments supersede "safe and secure by design," thousands of algorithms are being deployed without any security and safety guardrails.

This is why just about every country from the U.S. [16] to Japan [6] is focusing efforts on safety and security as a core trend of trustworthy and responsible AI.

**Implications:**

Executive leaders should expect AI policymakers and regulators to:

- Provide flexibility for public and private organizations to “defend with AI,” using it to improve security and risk management, optimize resources, defend against emerging attack techniques, or even reduce costs.
- Fund public efforts and encourage private investments to research and quickly share information on “attacked by AI” incidents, and best practices to prevent, detect, respond to and proactively disable attacks.
- Name an independent organization to oversee the defining and sharing of best practices to securely and safely build AI applications. This organization should also ensure mechanisms (internal and external) are in place to test the security and safety of the tools before release to the public.
- Incentivize organizations, both public and private, to invest in cybersecurity and insider threat safeguards to protect proprietary and unreleased model weights, so they are released only when intended and when security assurances are met.
- Allow third parties to look for and report vulnerabilities, and encourage AI tool producers to have vulnerability disclosure programs.
- Allow public-sector agencies to use the power of the public-sector purse in public procurements to mandate attestation and verification that these best practices are being followed.
- Define rules, requirements, monitoring and reporting of safe and secure consumption of AI by public sector organizations and agencies.
- Mandate red-team testing (adversarial testing for risks and bad behavior in AI models) for foundation models that could impact national security, public health and safety, or economic prosperity.
- Mandate AI providers to be able to identify artifacts created with their technology. For example, provide content watermarking, fingerprinting, authentication and provenance.

**Actions:**

- Evaluate the growing number of AI-enhanced security tools to help automate security operations.

- Actively participate in information sharing and analysis centers (ISACs) for your industry to stay on top of threats and new emerging attack vectors that leverage AI.
- Protect your reputation by monitoring a variety of channels where disinformation about your organization could appear and proliferate.
- Get ready for new security challenges by analyzing new adversarial actors and actions that employ AI. Learn from financial fraud detection experience, as fraudsters have been exploiting AI techniques for a long time.
- Establish boundaries for your own organization's use of AI, and document them in internal policies.

**Further Reading:**

4 Ways Generative AI Will Impact CISOs and Their Teams

Market Guide for AI Trust, Risk and Security Management

How to Securely Design and Operate Machine Learning

## Robustness and Resilience

*Back to Top*

*Analysis by David Gregory, Katell Thielemann*

**Description:**

To resist adversarial intrusion, and adapt to unexpected changes and an ever-changing risk landscape while remaining effective over time, as well as support recovery from failures, AI systems must be robust and resilient. They have to be designed and deployed in a way that ensures they are reliable enough to maintain full functionality in the event of cyberattacks or infrastructure failure. Where AI systems support applications that relate to cyber-physical systems (CPS) in which human and asset safety is important, resilience becomes even more critical.

In addition, organizational resilience is usually tested when something goes wrong, and business continuity or incident response plans need to be activated. Quick decision making with often insufficient information becomes necessary. Decisions and actions of responding personnel are scrutinized, in some cases by public inquiries, legal challenges and media attention. Those responsible for the management of the disruption can only make their decisions based upon the information available to them at that specific time. If AI is used to make these decisions, it will be unclear whether ultimate accountability lies with the decision maker, or the person who programmed the AI algorithm to create the information relied upon. Robust, transparent and explainable audit trails will be necessary.

**Why Trending:**

Policymakers and regulators are particularly concerned with this trend due to the lack of confidence that negative societal impacts of AI at scale can be reined in. Some will argue that, because of their self-learning attributes, AI algorithms will pose particular threats unless guardrails are deployed that allow models to be retired quickly without adverse impact.

**Implications:**

Executive leaders should expect AI policymakers and regulators to:

- Mandate that providers create and publish risk-based assessments to ensure AI systems are only created for a stated intended purpose, and incorporate “resilience-by-design” approaches to specifically resist, absorb, adapt and recover in the face of threats.
- Mandate full transparency for decisions made in incident response scenarios that rise to the level of public interest and scrutiny.
- Require a kill switch, or “safety brakes,” to be designed into AI systems, aligned to the controlled-based and outcomes-based governance categories, and activated if systems break into other computers or replicate themselves.

**Actions:**

- Conduct a business impact analysis of AI deployments to ensure that additional points of failure are not being introduced.

- Map AI dependencies so that workaround strategies can be implemented if something goes wrong.
- Limit what AI-provided information will be relied upon to support time-sensitive and critical decision making during a business- or mission-critical disruption.
- Implement a test-and-exercise strategy to build capabilities of critical incident responders, using scenarios with and without AI-provided data.
- Work with AI programmers and third parties to ensure innovations have resilience built in upfront.

**Further Reading:**

Roundup of Gartner's Research on Organizational Resilience

5-Step Roadmap to Achieving Organizational Resilience

Outlook for Organizational Resilience, 2023

## 21st Century Intellectual Property Rights

*Back to Top*

*Analysis by Brian Prentice*

**Description:**

In many ways, IP rights for AI align to existing fundamentals. For example:

- IP exists exclusively in the human domain; it is how original human creations can be transformed into something owned.
- IP confers benefits to both its owners and society more broadly; property, when used and developed, creates wealth.
- Since property coexists with the concept of theft, functioning societies protect owners from theft — the act of taking another person's property or services without that person's permission or consent, with the intent to deprive the rightful owner of it.
- Learning, on the other hand, is not theft; the role it plays in societal advancement is the central benefit that justifies the creation of an intangible property right.

But:

- AI is a tool, not a person; it is not sentient and self-directed. AI can create nothing without human intent and human input. AI cannot own property.
- AI fundamentally alters the efficiency of the creative process, as it radically reduces the time, resources and expertise needed to make things.

**Why Trending:**

IP rights is a trending topic because AI challenges the current rules for intellectual property rights at their very core and will force policymakers and regulators to revisit long-standing positions.

For example:

- AI challenges the role of copyrighted content to train LLMs; lawsuits are being filed alleging that LLMs are being trained with copyrighted material without the permission of the owner. [22] Major media organizations are approaching LLMs in a similar fashion to the way they have approached internet search engines. Namely, they are seeking to strike landmark deals for the use of news content to train LLMs. [23]

- Many argue that open-source LLMs should exist as a counterbalance to potential monopolies, since the interplay between AI and IP is not restricted to what goes into an algorithm or LLM or what comes out. It is about the IP treatment of the algorithm or LLM itself. Open-source AI models can limit monopolistic or cartel-like control over AI technology; open-source software (OSS) models introduce the possibility of a proliferation of AI solutions that would otherwise be cost- or risk-prohibitive to many small and medium businesses. Many policymakers and regulators will want to consider open-source AI and not favor approaches that only large, well-funded AI companies, with significant human resources and defined corporate structure, can comply with.

- AI will further strain an already challenged patent system. In jurisdictions that have a broad scope of patentable subject matter (e.g., discrete software, business methods), such as the U.S., patent and trademark offices are unable to keep up. Total patent pendency is currently at 25.3 months (about two years), a 10% increase over the same period two years ago. [24] From these delays flow a decrease in patent quality, a subsequent increase in "patent trolling," and burdens on the judicial system. AI is likely to dramatically increase patent applications. While AI might be able to dramatically increase the efficiency of the patent process, it is unlikely to resolve problems associated with examiner expertise. The result will be even longer patent pendency problems, along with all the associated side effects.

**Implications:**

Executive leaders should expect AI policymakers and regulators to:

- Ensure that the way AI can learn from copyrighted material reflects the same means available to humans.
- Allow copyright owners to manage and enforce access to their IP.
- Treat any act that knowingly seeks to create or fine-tune AI from copyrighted material that has restricted access as theft subject to criminal and civil penalties.
- Allow for copyrights and patents to be granted to individuals or organizations for the creative work and inventions they produce, without consideration of whether AI was used in its creation. This is because of the problems associated with determining and assessing thresholds for the amount of AI-supported creation and invention, and the subsequent need to police gaming of the copyright and patent system.
- Revisit the possibility of reducing copyright protections to 10 years and patent protection to five years, to reflect the efficiency gains of AI and minimize the cost of an inefficient patent process,
- Specific to GenAI, create and maintain national LLMs to expand IP creation. This should be seen as a 21st-century version of establishing a Library of Congress. This should be limited to a single version of a general-purpose LLM, trained on publicly available information. The LLM should be free to citizens, government agencies and domestic businesses. The LLM should be licensed under a permissive open-source license (e.g., Apache, MIT), thus allowing citizens to create proprietary solutions using it. A secondary purpose of a government-created OSS LLM would be to limit the motivation of governments to regulate LLMs in a way that restricts OSS LLMs.

**Actions:**

- Direct greater effort toward innovating new practices/processes with AI, and treat all AI innovations as IP assets.
- Shift the focus of IP-related GenAI risk management efforts from the IP losses related to prompt-based LLMs, to the protection of IP that comes out of an LLM.
- Ensure those responsible for tracking GenAI technology advancements include open-source options as part of their assessments.

**Further Reading:**

Intellectual Property Management Essentials for R&D Leaders

How to Protect Your Innovation's Intellectual Property

Three Key Steps to Monetizing R&D Intellectual Property

## Effective and Efficient Regulatory Process

*Back to Top*

*Analysis by Katell Thielemann*

**Description:**

David Collingridge, at Aston University in Birmingham, England, posed an important dilemma in 1980: Any effort to control innovative technology faces a double bind. During the initial stages, when control would be possible, not enough is known about the technology's harmful social consequences to warrant slowing its development. By the time those consequences are apparent, however, control has become costly and slow. [25]

**More than half of the technology and service provider (TSP) leaders participating in Gartner's 2023 TSP Generative AI Survey had no policies in place with respect to the use of GenAI.[26]**

Through decades of technology innovations, we have learned that policies and regulations are warranted:

- When laws and regulations already exist, but need to be updated to account for new advances in technology and new use cases
- When innovative technologies create situations not addressed by existing laws
- When they do not hinder innovation, impose unnecessary costs or burdens, or artificially create winners and losers in the market
- When evidence suggests that emerging technologies with the potential of enormous societal impact are being self-regulated by organizations rushing to bring them to market

Over the last few decades, we have also seen different approaches to technology policies and regulations emerge. For example:

- Product liability laws: anchored in theories such as harm and due care, negligence, product defects and breach of contract/warranty.
- Privacy laws: anchored in theories such as human rights to privacy, ownership, consent, fair and lawful processing, purpose limitation, and data security.
- Special interests: to protect vulnerable populations (e.g., children's privacy), sector-specific (e.g., financial institutions, healthcare providers protecting consumers), or aligned to geopolitical sovereignty concerns (e.g., data localization and access laws)

And we have learned several valuable lessons along the way:

- Effective and meaningful public participation and community engagement is a foundational principle of the regulatory development in democratic societies. Some countries like the U.S. are, for instance, taking proactive steps to encourage government agencies to develop processes to ensure this public engagement applies broadly to all levels of society, not just the largest, most-well-funded or most-informed advocacy groups. [27]

- The proliferation of AI efforts using all types of data (internal, external, anonymized, personally identifiable, etc.) for all kinds of purposes (research, monetization, curiosity etc.) means that a single set of regulation cannot control all. Many AI efforts will be innocuous with no societal impact, while others could alter the lives of millions of citizens. The scope of regulations will likely target the most impactful applications of AI.
- Developing policy, legislation and regulations is an inherent governmental function that affects the rights and obligations of individuals, and should be conducted by officials who can be held accountable by political or constitutional means. Developing technology-related regulations requires not only policy, legal and technological knowledge, but also multidisciplinary acumen (ethics, socioeconomic, geopolitical, etc.) and creativity.

- Technology-related policies and regulations are best deployed and enforced through a multipronged approach — for example, a combination of:
  - A central regulatory body — a lead agency or commission charged with overseeing rulemaking and enforcement (like the Federal Trade Commission, Equal Employment Opportunity Commission, Federal Aviation Administration, etc. in the U.S.). Such a central regulatory body would:
    - Review and approve processes and methodologies, aligned to standards developed with industry inputs, that define what expected performance and outcomes should look like.
    - Develop a framework for professional licensing for AI developers, akin to engineering licenses.
    - Harmonize against other regulations — for instance, as they relate to energy, environmental and sustainability policies, since AI efforts use significant amounts of electricity. Another key decision point in the U.S. specifically is whether the Section 230 [28] exemption for content liability for social media companies should extend to AI.
    - Coordinate best practices and lessons learned with key stakeholders in academia, private industries, and with international partners.
  - Regulatory sandboxes — "learning periods" to allow use cases to be tested in controlled legal and societal environments (these have been tested for fintech, autonomous driving and drone operations in specific jurisdictions, for instance).
  - "Coalition of willing" — government agencies, as well as standards-setting bodies, industry groups, professional associations and the like.
  - Enforcement via courts/judicial actions by aggrieved parties. In this case, legislators and regulators would determine whether a private course of action (as in the Biometric Information Privacy Act [BIPA] legislation in Illinois) would be advisable or not.

**Why Trending:**

Most countries believe that AI needs to be regulated. This is because it represents a step change, due to the velocity, autonomy, opacity, scale and reach of use cases, mixed with an elevated level of uncertainty around its impact on individuals, economies, societies and geopolitics.

As with responsible innovations, policymakers and regulators are looking for an appropriate balance:

- Overregulating could increase the risk for personalized “microdirectives” and automated law enforcement. Examples could include automated, personalized, AI-generated rules, reminders and law enforcement for any deviation, which would make humans slaves to regulations.
- Overregulating could also stifle innovation and commerce.
- A too-narrowly-framed regulatory approach would mean having to play catch-up, as technology changes rapidly and exponentially, while social, economic and regulatory systems change slowly and incrementally. Technology-related policies and regulations should be flexible and reversible as societal and market conditions constantly change.
- A too-broad/nonexistent regulatory process could lead to a chaotic approach, where predatory behaviors go unchecked and lead to broader societal issues, such as lack of trust in institutions.

**Implications:**

Executive leaders should expect AI policymakers and regulators to:

- Be performance- and outcomes-based, as opposed to requirements-driven.
- Require all AI regulators to develop and advertise statements of regulatory priorities that articulate the scope of regulations based on intent and impact.
- Make AI regulatory processes open and participatory by establishing forums for digital public comment campaigns, listening sessions, public hearings and/or “deliberative democracy” efforts to directly connect citizens with decision-making processes (examples include assemblies, “minipublics” with diverse representation, etc.). The outreach process must be designed to be timely, transparent, accessible, equitable, meaningful and built for continuous improvement.

- Invite voluntary industry consensus standards into the AI regulatory processes.
- Not allow AI to create AI policies and regulations on its own, or be used in the process; human agency is needed, so regulations must involve officials who can be held accountable by political or constitutional means.
- Write all AI policies and regulations in plain language that most of the population in the given jurisdiction should understand (for example, “plain English”).
- Work on deliberately harmonizing AI policies and regulations with others to prevent overlap or confusion, and encourage reciprocity to prevent undue costs.

**Actions:**

- Dedicate a resource, at least part-time, to track all AI policymaking and regulatory trends in all jurisdictions where you operate.
- Evaluate the pros and cons of participating in public sector agencies’ outreach for industry inputs in the form of requests for information (RFIs), either directly or via industry groups.
- Develop your own internal AI policies using inputs from across your enterprise and the trends in this research, and release them in plain language, in a location easily reachable by all employees.

**Further Reading:**

Tool: Regulatory Impact Assessment

Market Guide for Regulatory Tracking Solutions

4 Paths to Staying Ahead of Regulatory Change

## Evidence

[1] **2023 Gartner Generative AI Security and Risk Management Strategies One Minute Insight Study:** This study is based on responses of 150 IT and information security leaders at organizations where generative AI or foundational models are in use, in plans for use, or being explored. The responses were collected from 1 through 7 April 2023.

[2] Chart: ChatGPT Sprints to 1 Million Users, The Wire.

[3] America Already Has an AI Underclass, The Atlantic.

[4] AI Ethics, IBM.

[5] Title III, Chapter 4 and Recitals 65 and 65a, European Parliament.

[6] Social Principles of Human-Centric AI, Japan Cabinet Secretariat.

[7] Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, U.S. Federal Register.

[8] Australia's AI Ethics Principles, Australian Government Department of Industry, Science and Resources.

[9] CBS Mornings (@CBSMornings). 8 February 2023. "Google's dominance could be challenged by big breakthroughs in artificial intelligence — after Microsoft unveiled some of the most powerful AI ever made public [Video attached] [Tweet]", X.

[10] People + AI Research, Google.

[11] New Commission Staff Working Document Sheds Light on Experimentation Spaces for Regulatory Learning, European Commission.

[12] The Generative AI and ChatGPT Adoption and Use One Minute Insight is based on responses of 200 IT leaders (CIO, VP of IT, Director of IT, Manager of IT). The responses were collected from 31 March through 4 April 2023.

[13] National Artificial Intelligence Research and Development Strategic Plan 2023 Update, U.S. Office of Science and Technology Policy, and Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, U.S. White House.

[14] Zoom's Terms of Service Changes Spark Worries Over AI Uses. Here's What to Know, CBS News.

[15] A Pro-Innovation Approach to AI Regulation, U.K. Department for Science, Innovation and Technology.

[16] Blueprint for an AI Bill of Rights, Office of Science and Technology Policy (U.S.).

[17] New Generation Artificial Intelligence Ethics Code Released, Ministry of Science and Technology of the People's Republic of China.

[18] See 4 Ways Generative AI Will Impact CISOs and Their Teams.

[19] **2023 Gartner CIO Generative AI Survey:** This survey was conducted online from 16 May through 15 June 2023 to get a baseline on how CIOs are thinking about generative AI and what they think their role will be. In total, 80 CIOs participated. Seventy-six were members of Gartner's CIO Research Circle, a Gartner-managed panel, and four were from an external survey link shared via social channels and analyst contacts. Research Circle participants were from North America (n = 41), EMEA (n = 21), Asia/Pacific (n = 8) and Latin America (n = 4). Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[20] Killed by a Machine: The Therac-25, Hackaday.

[21] Triton/Trisis Attack Was More Widespread Than Publicly Known, Dark Reading.

[22] Sarah Silverman Sues Meta, OpenAI for Training AI Models on Her Book, Yahoo! Finance.

[23] AI and Media Companies Negotiate Landmark Deals Over News Content, Financial Times.

[24] Patents Pendency Data September 2023, U.S. Patent and Trademark Office.

[25] 2012: What Is Your Favorite Deep, Elegant, or Beautiful Explanation?, Edge.org.

[26] **2023 Gartner TSP Generative AI Survey:** This survey was conducted online from 28 March through 10 April 2023 to explore how technology and service providers (TSPs) utilize generative AI in content marketing. In total, survey participants included 43 TSP leaders utilizing or considering utilization of generative AI in the next six months. Forty-two TSP leaders were members of Gartner's Research Circle, a Gartner-managed panel, and one was from an external survey link shared via social channels and analyst contacts. Research Circle member participants were from EMEA (n = 19), North America (n = 17) and Asia/Pacific (n = 6). Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[27] Broadening Public Participation and Community Engagement in the Regulatory Process, U.S. Executive Office of the President.

[28] Department of Justice's Review of Section 230 of the Communications Decency Act of 1996, U.S. Department of Justice Archives.

Gartner Peer Community is a place for technology leaders to engage in discussions with peers and share knowledge in real time. Users go through a strict validation and verification process to ensure they are authentic. The surveys are designed by Gartner Peer Community editors and appear in the Survey Reports section of the platform. Surveys are summarized in a One-Minute Insight once the respondent threshold is met.

Of the Peer Community Benchmark Survey data considered for this topic, only the responses that met the minimum criteria were included in this synthesis:

- For technology users, surveys with more than 100 responses
- For business users, surveys with more than 50 responses

The results of this synthesis are representative of the respondents that participated in the survey. It is not market representative. The call-outs are representative responses that reinforce the main results, and are selected by editors to provide a deeper understanding of participants' perspectives and experiences. They offer insights, anecdotes or examples that support and contextualize the survey findings.

## Table 1: Trends Profiles: Click links to jump to profiles

| | | |
|---|---|---|
| Human Centricity and Diversity | Responsible Innovation | Governance and Accountability |
| Transparency and Explainability | Contestability and Redress | Safety and Security |
| Robustness and Resilience | 21st Century Intellectual Property Rights | Effective and Efficient Regulatory Process |

Source: Gartner