Gen™

2025

Driving Innovation Through Thoughtful Public Policy:

AI Recommendations from Gen

Gen™

Executive Summary

Given the speed at which the AI revolution is progressing, legislators and regulators in the United States face the challenge of finding the right balance between regulation and freedom, as well as safety and innovation.

In the United States, Gen believes that AI policy should include:

- Supporting and enacting a comprehensive **nationwide AI law** to manage the technology's development, use, security and safety.

- Supporting and enacting **state-level policies** governing consumer protection to safeguard people online from fraudulent, dangerous or defective AI technologies.

- **Regulating organizations and companies** to manage their AI development and usage.

- Developing **programs to raise public awareness** regarding the issue of content and entity authenticity on the internet and the risks associated with sharing personal information publicly.

- Enacting **laws regarding ownership** of AI-generated data including data used for generative AI training and clarify rules of recycling AI-generated content, including the use of digital avatars and personas.

- Addressing and **legally targeting the elimination of deepfakes and misinformation**.

- **Mandating transparency** and explainability regarding AI providers and their systems.

- Ensuring regulatory certainty of **AI standards**.

We look forward to creating partnerships to advance these AI conversations. We believe partnering with groups like the Congressional Artificial Intelligence Caucus, which informs policymakers of the technological, economic and social impacts of advances in AI, are vital to the future of these technologies, and we are excited at the opportunity to share our perspectives with government officials, regulators and other policymakers. As an example, we have been excited by our collaboration in the past with the Cyber Threat Alliance, who has been instrumental in promoting legislation and regulations that can effectively manage cyber issues while promoting American technological innovation.

"Our society meets an increasing number of new challenges to protect safety, freedom and trust in an AI-enabled digital environment. The challenges can be overcome but need action from all participants in the digital world: citizens, private organizations, policymakers and governmental bodies. Building a safer and more trusted AI-supported digital world has the potential to greatly benefit our society, and Gen is excited to join in creating the future of AI."

Howie Xu - AI & Innovation

Background

As the United States prepares for a change in president and welcomes new members to Congress, policy makers will no doubt want to continue America's leadership in Artificial Intelligence (AI) technologies, despite a rapidly evolving digital and geopolitical landscape. While there is no comprehensive AI law in the U.S. yet, initiatives at both the federal and state levels have addressed related issues like privacy, safety, accountability and transparency for decades. In 2022, the White House Office of Science and Technology Policy published its Blueprint for an AI Bill of Rights, which outlined five principles to guide the design, use and deployment of AI systems to protect the American public. Later in October 2023, President Biden signed the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, which established standards for AI safety, security, privacy and equity, while promoting innovation and competition. The order directed federal agencies to protect rights and safety around AI, improve its procurement and strengthen its deployment and is a continuation of previous actions President Biden has taken to ensure the safe and trustworthy development of AI in the U.S.

Separate action has been taken by independent federal agencies and organizations. The Federal Trade Commission (FTC) issued guidelines around AI concerns and opportunities. The National Institute of Standards and Technology (NIST) published AI standards and a risk management framework to help companies identify and manage the associated risks. The National AI Research Resource Task Force published a roadmap for increasing access to resources essential to AI research and development. State legislatures have taken their own approaches as well, like California's and Illinois' AI and biometric privacy laws. In Congress, the introduction of measures like the AI Disclosure Act, Future of AI Innovation Act and Secure AI Act indicate a willingness to create a framework for AI policy that includes a more overarching federal law, similar to the European Union's AI Act. However, as the new Trump administration comes to power, the American tech policy environment will likely see some changes from the current direction. In the spirit of supporting a robust and clear policymaking process for AI, Gen created key policy recommendations with a focus on prioritizing economic competitiveness, national security and a pro-innovation regulatory stance.

We believe AI policy principles should address the following issues:

Use and Disclosure of Generated Content

The generative capabilities of AI models can appear across a variety of domains—from generating images, videos, sketches and text documents to creating audio, speech and music —with technology making it easy to use and high quality and only getting better every day. While AI generated outputs cannot match human originality and authenticity, the capabilities of current generative models have reopened challenging discussions about copyright, utility, social engineering, malicious content and false reproduction of material.

Deepfakes and Misinformation

Generative AI makes it easy to generate faces and use audio and video footage to impersonate individuals into saying. or doing anything. We are seeing this more and more every day.

> "Deepfakes leverage AI techniques to dramatically decrease the skill requirements and increase the scale at which disinformation content can be personalized to an individual's characteristics. The use of deepfakes more than doubled from 2022 to 2023. In 2024, over 10 percent of companies have reported attempted or successful attempts at deepfake fraud and more than 400 firms globally experience CEO fraud every day through email scams."
>
> **Siggi Stefnisson** - Cyber Safety Technology

Generative AI models can generate virtually anything when provided with the appropriate prompt. Misinformation by generative AI can be intentional, such as bad actors using AI to supercharge misinformation creations, but can also be unintentional, such as generative AI producing misinformation as a result of hallucination. Additionally, while AI can offer new possibilities for creativity and storytelling, enabling artists to push the boundaries of digital expression, deepfakes raise ethical concerns around consent, misrepresentation, and eroding trust among the public.

Personal Information, Identity and Behavioral Models

Today, our "digital life" is intertwined with the internet through various communication channels, online services and social networks. These aspects of digital engagement often utilize search engines and sometimes, unknowingly, are also leveraging various forms of AI that now run behind virtually all digital services.

In today's digital world, primary pitfalls for protecting personal information and identity include:

1. The identity (or even existence) of people we communicate with is much harder to gauge than in the physical world.

2. Our own level of online privacy is more difficult to estimate and control.

3. The truthfulness of information obtained from the internet is harder to assess and verify.

4. The intentions of others we engage with on the internet are more challenging to determine.

Cybersecurity

Cybersecurity encompasses the internet, computer networks, interconnected computers and a myriad of devices from mobile phones to cars. Due to its complexity, designers regularly overlook or misjudge errors, making the system vulnerable to those who discover these mistakes, potentially gaining unauthorized access to documents, or in extreme cases, control over a system. In addition, nation states are actively and intentionally leveraging their cyber capabilities for state-sponsored cyber influence operations. Taken as whole, cyber warfare, fraud, scams and hacking are severe threats to the efficiency, integrity and safety of the world today.

Fairness and Safeguards

The quest for fairness in AI models with regard to humans has long been accompanied by research and regulation toward what is termed as "Fair AI." This primarily involves legal protection and self-regulation within companies developing AI solutions to shield users from automated discrimination. For example, AI has been known to disadvantage certain groups in the job market, especially when AI is deployed in hiring processes or other scenarios where software assesses individual data.

Artificial Intelligence Policy Principles at Gen

As a global leader in Cyber Safety, Gen recognizes its responsibility to lead in addressing the transformative challenges and societal impacts posed by the rapid growth of AI. We see numerous exciting cybersecurity and productivity AI cases; yet, AI-generated threats and risks are developing and increasing at an enormous speed.

At Gen, we are fully committed to providing the best possible protection to consumers around the globe. To do so, we are investing in ethical and responsible AI to protect consumers and drive our growth.

In that framework, we have identified five AI policy principles to guide our AI research, use and deployment:

1. **Integrity:** We use and create AI in only positive, legal and ethical ways.

2. **Accountability:** We assess the unique risks of AI and stand accountable for the outputs of the tools we build and use.

3. **Data Protection:** We protect company and customer information, including intellectual property and personal data. We are committed to minimizing the amount of personal data required for these tools and limiting the duration for which such data is retained.

4. **Human Involvement:** We control the outputs of AI by incorporating human oversight into our processes where necessary or required.

5. **Transparency:** People should be able to understand when they are significantly impacted by AI. We strive to be clear how the AI tools we build work, and how they affect stakeholders.

About Gen

Gen is a global leader in Cyber Safety, with dual headquarters in Tempe, Arizona and in Prague, Czech Republic. The company marks its presence in over 150 countries, catering to nearly 500 million customers worldwide. The Gen portfolio includes comprehensive cybersecurity solutions from a family of trusted brands such as Norton, Avast, LifeLock, Avira, AVG, ReputationDefender, and CCleaner.

Powering Digital Freedom lives at the heart of everything Gen does. This goes beyond the Company's mission to create solutions that enable people to navigate their digital lives safely, privately, and confidently. It is about empowering both the generations of today and future generations to be able to take advantage of the ease technology offers, worry free. That is why Gen approaches everything we do with the customers and communities we serve in mind. We champion the simplification and safeguarding of customer experiences in the ever-evolving digital landscape, reinforcing our role as a leader in digital security and empowerment.

If you want more information, please reach-out to:

Kim Allman
Head of Corporate Responsibility,
ESG & Government Affairs
Kim.Allman@GenDigital.com

United States: 60 E Rio Salado Pkwy STE 1000 Tempe, AZ 85203

Czech Republic: Enterprise Office Center Pikrtova 1737/1A 140 00 Prague 4

© 2025 Gen Digital Inc. All rights reserved.