AI AGENT Act

An artificial intelligence (AI) agent is a system that can perceive its environment, can act autonomously or according to preestablished rules or objectives, and make decisions with minimal human oversight in service of a defined goal. AI agents are being deployed for research assistance, in cybersecurity and software development, scheduling and email management, customer service and support, and more.

As AI agents become more widespread and consumer-facing, it is **critical that customers, whether they be individuals or businesses, have real choices in a marketplace**. In order to avoid a market dominated by a few major players and encourage innovation and small business growth, there needs to be real competition. To really work, that consumer choice has to be **balanced with reasonable privacy, cybersecurity, and reliability mechanisms** – ensuring that consumer-facing AI agents aren't abusing consumers trust or subjecting them (or services they access) to privacy or security risks. An AI agent that has access to a user's most sensitive data and access rights – including email, e-commerce accounts, and credit cards – must behave in fiduciary-like manner to protect users.

With the AI AGENT Act, agentic AI **startups will be able to compete on equal terms with the biggest tech companies –** creating new opportunities to tilt the balance back towards consumers. Investment capital and human talent will have more opportunities to grow businesses. **Users will be empowered** through trusted custodial agents acting on their behalf in a variety of online contexts, such as e-commerce, social media, online personal finance, and travel booking.

Summary

The AI AGENT Act opens digital markets up to competition from consumer-empowering digital intermediaries, establishing a framework for an online and connected ecosystem where:

- AI agents are able to **openly and securely access** a range of online platforms
- AI agents act with a **duty of loyalty** to their user
- AI agents strictly **protect user data and privacy,** with restrictions on monetizing or otherwise commercially using user data beyond what's strictly necessary
- Users are able to freely change AI agents and **maintain access to certain online platforms, activities, or communities**

This bill will:

- Establish rights and responsibilities for guaranteed secure access by AI agents to certain large online platforms

- Create a Federal Trade Commission registry of trusted, secure AI agents – with a regulatory environment swift enough to approve innovative user services or quickly curtail products that violate consumers' trust
- Require AI agents protect users' privacy and user data and act transparently in a user's best interest and in a manner that makes clear to third-party websites and online service providers that an AI agent has valid authorization
- Direct NIST to identify technical standards and open protocols to make online services more accessible to AI agents and to ensure consensus-based standards around critical mechanisms like authentication
- Protect businesses, users, and online providers from AI agent abuse or misuse