Secure AI Milestones: From Spark to Flame

The release of public generative Artificial Intelligence (AI) tools in late 2022 sparked wide-spread interest and prompted a discussion that continues today. As this infographic highlights, a global surge of activity in the past 18 months has solidified the important role safety, security, and trustworthiness play in the development, adoption, and regulation of AI. Foundational to this effort are Privacy Enhancing Technologies (PETs) which uniquely enhance and preserve the privacy of data throughout its lifecycle, enabling users to capitalize on the power of AI while mitigating risk and prioritizing protection.

JANUARY 2023

Under direction from Congress**, NIST develops the Artificial Intelligence Risk Management Framework** to help organizations incorporate trustworthiness into the design, development, use, and evaluation of AI products, services, and systems**.**

OCTOBER 2023

The release of **the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems** promotes safe, secure, and trustworthy AI and provides voluntary guidance for actions by organizations developing advanced AI systems.

OCTOBER 2023

The White House's **Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence** tasks Congress and federal agencies to use available policy and technical tools, including Privacy Enhancing Technologies (PETs) to protect privacy and combat broader risk.

NOVEMBER 2023

The **NCSC Guidelines for Secure AI System Development** identifies security as a core requirement, not just in the development phase, but throughout the life cycle of the system and identifies PETs as a means of mitigating risk to AI systems.

NOVEMBER 2023

The Bletchley Declaration, signed by global leaders representing 28 countries while gathered for the AI Safety Summit, notes the importance of trustworthy and responsible AI that accounts for privacy and data protection.

FEBRUARY 2024

The U.S. Government creates **the NIST AI Safety Institute Consortium** in support of the development and deployment of safe and trustworthy AI, bringing together leaders from industry, civil society, and academia to set safety standards and protect the innovation ecosystem.

MARCH 2024

The European Union approves **the EU Artificial Intelligence Act,** the world's first major set of regulatory ground rules to govern artificial intelligence, which dictates that the right to privacy and to protection of personal data must be guaranteed throughout the lifecycle of the AI system.

MARCH 2024

The United Nations General Assembly adopts a U.S.-led resolution on AI, the first ever standalone resolution to establish a global consensus approach to AI governance, encouraging member states to promote safe, secure, and trustworthy AI systems worldwide.

MAY 2024

Global economic policy forum OECD updates its AI Principles to guide AI actors in their efforts to develop trustworthy AI, which requires trust in all aspects of personal data collection, management and use, such as acquiring reliable data, using it responsibly, keeping it secured, and maintaining transparency about its use.

MAY 2024

The Roadmap for AI Policy in the United States Senate identifies areas of consensus that merit bipartisan consideration to harness the full potential of AI while prioritizing responsible innovation, which includes foundational trustworthy AI topics, such as transparency, explainability, privacy, interoperability, and security.

POWERED BY ENVEIL ENCRYPTED VEIL

Enveil leverages Privacy Enhancing Technologies (PETs) to enable secure data usage, collaboration, monetization, and Secure AI. A proud participant in the U.S. AI Safety Institute Consortium, the company is committed to delivering software solutions that advance Secure AI efforts in the commercial and public sector markets. Enveil's capabilities have been recognized in Gartner's Market Guide for AI Trust, Risk, and Security Management and are being leverage by customers at scale today.

Find the full list of sources at enveil.com/secure-AI