MEDIA ADVISORY

Contact:
Jim Ormond
ACM Media Relations
212-626-0505
ormond@hq.acm.org

Tom Romanoff
ACM Policy Director
212-626-0543
romanoff@hq.acm.org

AI "Vibe Coding" Could Reshape Software Development but Lacks Key Safeguards, ACM Technology Policy Council Warns

New TechBrief Outlines Productivity Gains Alongside Rising Risks Around Security, Reliability, and Long-Term Code Quality

New York, NY — April 30, 2026 — Generative AI tools are rapidly transforming how software is built—and raising new risks in the process, according to a new TechBrief from the Association for Computing Machinery's Technology Policy Council (TPC) on the rise of "vibe coding."

The TechBrief, "AI-Assisted Software Development, or Vibe Coding: Benefits and Risks of AI-Driven Software Development," examines a growing approach to programming in which developers as well as non-technical users describe what they want to build in natural language, and AI systems generate, debug, and sometimes execute the underlying code—a shift gaining traction as AI coding assistants are rapidly adopted across enterprise and developer workflows.

While vibe coding can speed up development and make software creation more accessible, the TechBrief finds that it often skips over core engineering practices that ensure systems are secure, reliable, and maintainable.

"I use AI-assisted coding every day for both my personal and professional projects, and it's transformed how I develop software," said Simson Garfinkel, Chief Scientist at BasisTech and lead author of the TechBrief. "It's making developers dramatically more effective, but it's also introducing security vulnerabilities, increasing technical debt, and producing code that can be difficult to maintain. To use these tools safely, strong software engineering practices are still required, including clear specifications, meaningful testing, and enforced standards."

The TechBrief highlights several risks tied to AI-generated code including security vulnerabilities inherited from training data, inconsistent or missing testing, and systems that become difficult for humans to review or maintain over time. It also points to the rise of "agentic" AI coding tools that can execute code across systems, increasing the risk of unintended actions such as exposing sensitive data, deleting critical files, or executing malicious instructions introduced through prompt injection attacks.

The ACM Technology Policy Council emphasizes that these limitations stem from how current AI systems generate code, often without enforcing specifications or systematically validating outputs. It also includes steps organizations should take when adopting AI-assisted development:

- **Apply rigorous testing and verification:** Use established software engineering practices, including formal methods, to validate AI-generated code.
- **Audit AI-generated outputs:** Leverage specialized tools—including AI systems—to identify security vulnerabilities and defects.
- **Implement strong governance controls:** Require human oversight and review, particularly for code execution and deployment.
- **Plan for maintainability:** Ensure systems can be understood, reviewed, and managed by human developers over time.

“AI systems do not understand what they’re producing, and they are not capable of reasoning about the consequences,” Garfinkel added. “As a result, we are only beginning to understand the broader impact of this technology, which is evolving rapidly.”

The TechBrief concludes that while vibe coding is likely to play a central role in the future of software development, improving code quality and accountability will be essential to making it safe and sustainable at scale.

Read the full TechBrief: https://dl.acm.org/doi/book/10.1145/3807518.

ACM’s TechBriefs are designed to complement ACM’s activities in the policy arena and to inform policymakers, the public, and others about the nature and implications of information technologies. Earlier ACM TechBriefs have covered topics such as buying vs building LLMs, automated speech recognition, governmental digital transformation, accessibility, and generative artificial intelligence among others.

About the ACM Technology Policy Council

ACM’s global Technology Policy Council sets the agenda for global initiatives to address evolving technology policy issues and coordinates the activities of ACM’s regional technology policy committees in the US and Europe. It serves as the central convening point for ACM’s interactions with government organizations, the computing community, and the public in all matters of public policy related to computing and information technology. The Council’s members are drawn from ACM’s global membership.

About ACM

ACM, the Association for Computing Machinery, is the world’s largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field’s challenges. ACM strengthens the computing profession’s collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.