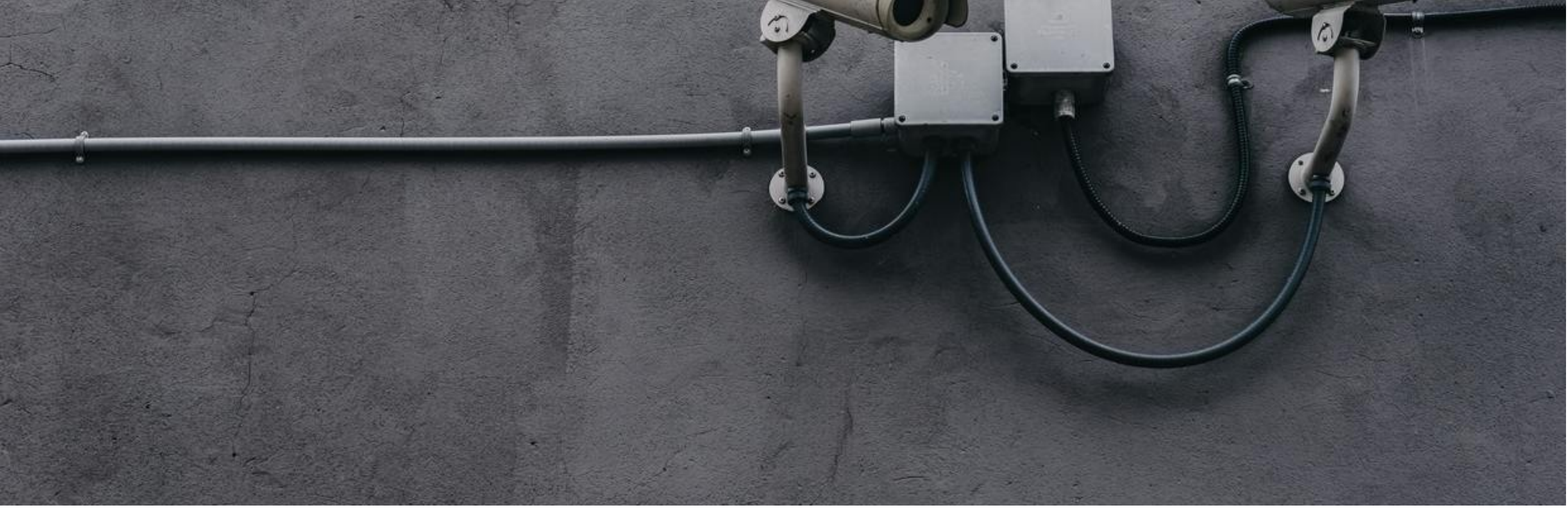

Spotlight on AI and Policy: Regulation, Privacy, and Risk

Authors: Rohita Biswas, Cinthya Souza Simas, Sara Tóth Martínez, María Belén Moyano, Gerhard G. Steinmann, Roland Mertelsmann

Submitted: 18. March 2026
Published: 18. March 2026
Volume: 13
Issue: 2
Affiliation: Journal of Science, Humanities and Arts (JOSHA), Freiburg im Breisgau, Germany
Languages: English
Keywords: Biosecurity; Governance; Privacy; Validity; Disclosure; Misinformation.
Categories: News and Views
DOI: 10.17160/josha.13.2.1132

Abstract:

This editorial curation brings together six timely articles examining how artificial intelligence is reshaping policy, security, privacy, and public trust. It moves from biosecurity risks created by generative protein design to the urgent need for science- and evidence-based AI governance. It also highlights the fragility of consumer genetic privacy, showing how weak legal protections can leave highly sensitive data vulnerable to misuse. At the same time, the collection explores how AI can distort knowledge production itself: from synthetic participants that may mislead social science research, to the hidden use of AI in scientific writing and peer review. Finally, it turns to AI-generated video and the erosion of visual credibility in public life. Together, these pieces reflect JOSHA's commitment to curating debates that connect technological innovation with societal responsibility.

JOSHA Journal of Science, Humanities and Arts

March 2026 Volume 13, Issue 2

Spotlight on AI and Policy: Regulation, Privacy, and Risk

Rohita Biswas, Cinthya Souza Simas, Sara Tóth Martínez, María Belén Moyano, Gerhard G. Steinmann, Roland Mertelsmann.

editorial@josha-archive.org

Journal of Science, Humanities and Arts, Freiburg im Breisgau, Germany

Abstract

This editorial curation brings together six timely articles examining how artificial intelligence is reshaping policy, security, privacy, and public trust. It moves from biosecurity risks created by generative protein design to the urgent need for science- and evidence-based AI governance. It also highlights the fragility of consumer genetic privacy, showing how weak legal protections can leave highly sensitive data vulnerable to misuse. At the same time, the collection explores how AI can distort knowledge production itself: from synthetic participants that may mislead social science research, to the hidden use of AI in scientific writing and peer review. Finally, it turns to AI-generated video and the erosion of visual credibility in public life. Together, these pieces reflect JOSHA's commitment to curating debates that connect technological innovation with societal responsibility.

Keywords: Biosecurity; Governance; Privacy; Validity; Disclosure; Misinformation.

1. Strengthening nucleic acid biosecurity screening against generative protein design tools

By Bruce J. Wittmann *et al*

Generative AI protein-design tools expand the ability to modify proteins for beneficial applications, but they also create a new biosecurity weakness at a key chokepoint: commercial DNA (nucleic acid) synthesis ordering. The study evaluates whether widely used, “best-match”–style biosecurity screening software can reliably detect AI-redesigned variants of proteins of concern when those variants are engineered to be more sequence-divergent yet still plausibly functional. Using an AI red-teaming workflow, the authors generated large sets of “synthetic homologs” with open-source protein sequence generative models and assessed how often existing screening pipelines would flag them, revealing a detection vulnerability for AI-redesigned sequences. A coordinated, cybersecurity-style disclosure process was then used to support rapid mitigation, and screening “patches” were developed and deployed to improve detection of higher-risk synthetic homologs; no generated proteins were constructed or experimentally tested.

This article was previously published in *Science* on October 2, 2025.

Read the full article here

2. Advancing science- and evidence-based AI policy

By Rishi Bommasani *et al*

Policymakers worldwide are struggling to govern rapidly advancing AI systems. The authors argue that effective AI governance must be grounded in strong scientific evidence. However, they note that the current evidence base on AI risks and impacts is still immature. They classify AI risks into malicious use, system malfunctions, and broader systemic effects. Some harms, such as scams, bias, and privacy violations, are already well documented. Other risks, including large labor disruptions and loss of control, remain uncertain and debated. The paper highlights an “evidence dilemma” between acting too early and waiting too long. To address this, the authors urge pre-release evaluations of AI models. They also call for greater transparency, post-deployment monitoring, and protection of independent research.

This article was previously published in *Science, Volume 389, Issue 6759,* on July 31, 2025.

Read the full article here

3. The precarious future of consumer genetic privacy

By Natalie Ram *et al*

This article argues that the 2025 bankruptcy and sale of 23andMe's genetic database exposed serious weaknesses in U.S. laws protecting direct-to-consumer (DTC) genetic data and biospecimens, urging Congress to enact stronger, comprehensive safeguards. Although the company's data were sold to a nonprofit linked to its founder, the authors warn that future sales could involve unrelated buyers, increasing risks of exploitation and misuse. They explain that genetic data are uniquely sensitive, identifiable, and implicate not only individuals but also their relatives, yet U.S. protections remain fragmented: HIPAA does not apply to most DTC companies, proposed federal bills are narrow in scope, and state Genetic Information Privacy Acts vary widely and leave significant gaps. Additional concerns include unilateral changes to terms of service, potential discrimination by life and disability insurers, law enforcement access to consumer databases, and the often-overlooked transfer and commercialization of stored biospecimens containing extensive genomic and health information. Concluding that market forces and existing legal frameworks fail to ensure meaningful consumer control, the authors call for a robust federal genetic privacy law, stricter consent requirements, limits on data sharing and reidentification, and stronger safeguards for both genetic data and physical samples.

This article was previously published in *Science, Volume 389, Issue 6765,* on July 31, 2025.

Read the full article here

4. AI-generated 'participants' can lead social science experiments astray

By Cathleen O`Grady

There is a growing interest among some researchers in using AI-generated participants to avoid the difficulty of recruiting human subjects. Jamie Cummins evaluated how well large language models can mimic human responses by testing 252 combinations of models and settings. He found that results vary widely depending on methodological choices, to the point that two researchers could reach opposite conclusions. Although some see potential in this tool, Cummins warns that it may be especially dangerous when representing minorities that are underrepresented in training data. Indira Sen notes that much more discussion is needed before these systems are widely adopted.

This article was previously published in *Science, Volume 390, Issue 6769*, on October 9, 2025.

Read the full article here

5. Far more authors use AI to write science papers than admit it, publisher reports

By Jeffrey Brainard

This article reports on a study by the American Association for Cancer Research (AACR) showing that far more academic authors use artificial intelligence (AI) in their manuscripts than disclose. Among 7177 submissions analyzed between January and June 2025, 36% of abstracts contained some AI-generated text, while only 9% of authors admitted using AI; AI was also detected in methods sections and peer-review reports. The study used a deep learning–based detection tool that showed low false positives on pre-ChatGPT papers, though experts caution that such tools are not infallible and require human judgment. The article discusses reasons for underreporting, including fear of rejection and unclear norms across disciplines, and notes that while AI can legitimately assist with language editing, it may also signal problematic practices such as paper mills. Publishers are now weighing routine AI screening despite concerns about scale, accuracy, and an emerging “arms race” between detection systems and AI text generation.

This article was previously published in *Science, Volume 389, Issue 6766*, on September 25, 2025.

Read the full article here

6. AI video generators are now so good you can no longer trust your eyes

By Brian X. Chen

OpenAI's Sora and similar A.I. video generators from major tech companies are presented as an inflection point for "visual proof," because realistic, instantly generated clips can now circulate at the same speed as ordinary social media videos. The article explains how Sora is used (prompt-to-video, photo-to-video, a scrolling feed, and easy sharing) and argues that these tools will make it harder to treat video as an objective record, increasing the need to evaluate visuals with the same skepticism people already apply to text. Through hands-on testing, it shows how guardrails can still allow harmful outputs—such as fabricated dashcam footage usable for insurance fraud, persuasive-but-false health claims, and defamatory fake "news" segments—while also outlining broader impacts like copyright conflict and rapid copycat proliferation. It closes by noting that watermarks and embedded provenance signals can be removed or bypassed, and that "spot-the-fake" tips will age quickly as models improve, shifting the practical burden toward verification habits and reduced reliance on high-velocity video feeds.

This article was previously published in *The New York Times*, on October 9, 2025.

Read the full article here

Acknowledgements

GPT-5.2 version of Chat-GPT (Open AI) and Gemini (Google) was used during the writing process as part of JOSHA's policy of experimentation with AI tools. However, JOSHA takes full responsibility for its content.