§ 9201. Findings

Congress finds the following:

(1) Gaps currently exist on the underlying research needed to develop tools that detect videos, audio files, or photos that have manipulated or synthesized content, including those generated by generative adversarial networks. Research on digital forensics is also needed to identify, preserve, recover, and analyze the provenance of digital artifacts.

(2) The National Science Foundation's focus to support research in artificial intelligence through computer and information science and engineering, cognitive science and psychology, economics and game theory, control theory, linguistics, mathematics, and philosophy, is building a better understanding of how new technologies are shaping the society and economy of the United States.

(3) The National Science Foundation has identified the "10 Big Ideas for NSF Future Investment" including "Harnessing the Data Revolution" and the "Future of Work at the Human-Technology Frontier", with artificial intelligence is a critical component.

(4) The outputs generated by generative adversarial networks should be included under the umbrella of research described in paragraph (3) given the grave national security and societal impact potential of such networks.

(5) Generative adversarial networks are not likely to be utilized as the sole technique of artificial intelligence or machine learning capable of creating credible deepfakes. Other techniques may be developed in the future to produce similar outputs.

(Pub. L. 116–258, § 2, Dec. 23, 2020, 134 Stat. 1150.)

§ 9202. NSF support of research on manipulated or synthesized content and information security

The Director of the National Science Foundation, in consultation with other relevant Federal agencies, shall support merit-reviewed and competitively awarded research on manipulated or synthesized content and information authenticity, which may include—

(1) fundamental research on digital forensic tools or other technologies for verifying the authenticity of information and detection of manipulated or synthesized content, including content generated by generative adversarial networks;

(2) fundamental research on technical tools for identifying manipulated or synthesized content, such as watermarking systems for generated media;

(3) social and behavioral research related to manipulated or synthesized content, including human engagement with the content;

(4) research on public understanding and awareness of manipulated and synthesized content, including research on best practices for educating the public to discern authenticity of digital content; and

(5) research awards coordinated with other federal agencies and programs, including the Defense Advanced Research Projects Agency and the Intelligence Advanced Research Projects Agency,[1] with coordination enabled by the Networking and Information Technology Research and Development Program.

(Pub. L. 116–258, § 3, Dec. 23, 2020, 134 Stat. 1151.)

§ 9203. NIST support for research and standards on generative adversarial networks

(a) In general

The Director of the National Institute of Standards and Technology shall support research for the development of measurements and standards necessary to accelerate the development of the technological tools to examine the function and outputs of generative adversarial networks or other technologies that synthesize or manipulate content.

(b) Outreach

The Director of the National Institute of Standards and Technology shall conduct outreach—

(1) to receive input from private, public, and academic stakeholders on fundamental measurements and standards research necessary to examine the function and outputs of generative adversarial networks; and

(2) to consider the feasibility of an ongoing public and private sector engagement to develop voluntary standards for the function and outputs of generative adversarial networks or other technologies that synthesize or manipulate content.

(Pub. L. 116–258, § 4, Dec. 23, 2020, 134 Stat. 1151.)

§ 9204. Generative adversarial network defined

In this chapter, the term "generative adversarial network" means, with respect to artificial intelligence, the machine learning process of attempting to cause a generator artificial neural network (referred to in this section as the "generator"[1] and a discriminator artificial neural network (referred to in this section as a "discriminator") to compete against each other to become more accurate in their function and outputs, through which the generator and discriminator create a feedback loop, causing the generator to produce increasingly higher-quality artificial outputs and the discriminator to increasingly improve in detecting such artificial outputs.

(Pub. L. 116–258, § 6, Dec. 23, 2020, 134 Stat. 1152.)

Editorial Notes

REFERENCES IN TEXT

This chapter, referred to in text, was in the original "this Act", meaning Pub. L. 116–258, Dec. 23, 2020, 134 Stat. 1150, known as the Identifying Outputs of Generative Adversarial Networks Act and also as the IOGAN

---

[1] So in original. Probably should be "Activity,".

[1] So in original. Probably should be followed by a closing parenthesis.