AI and Democracy: Content Authenticity Technology

Lindsay Gorman

Senior Fellow for Emerging Technologies, The Alliance for Securing Democracy at the German Marshall Fund of the US

Presentation before the Virginia State Legislature Joint Commission on Technology and Science

From AI in Self-Driving Cars to AI in Democracy

Democracy, Technology, and Authoritarianism:

Does technology now favor tyranny?

Democracies rely on objective reality

- Source: Business Insider (April 17, 2018). “A viral video that appeared to show Obama calling Trump a 'dips---' shows a disturbing new trend called 'deepfakes',” https://www.businessinsider.com/obama-deepfake-video-insulting-trump-2018-4.

Democracy-Affirming Technologies

THE WHITE HOUSE

BRIEFING ROOM

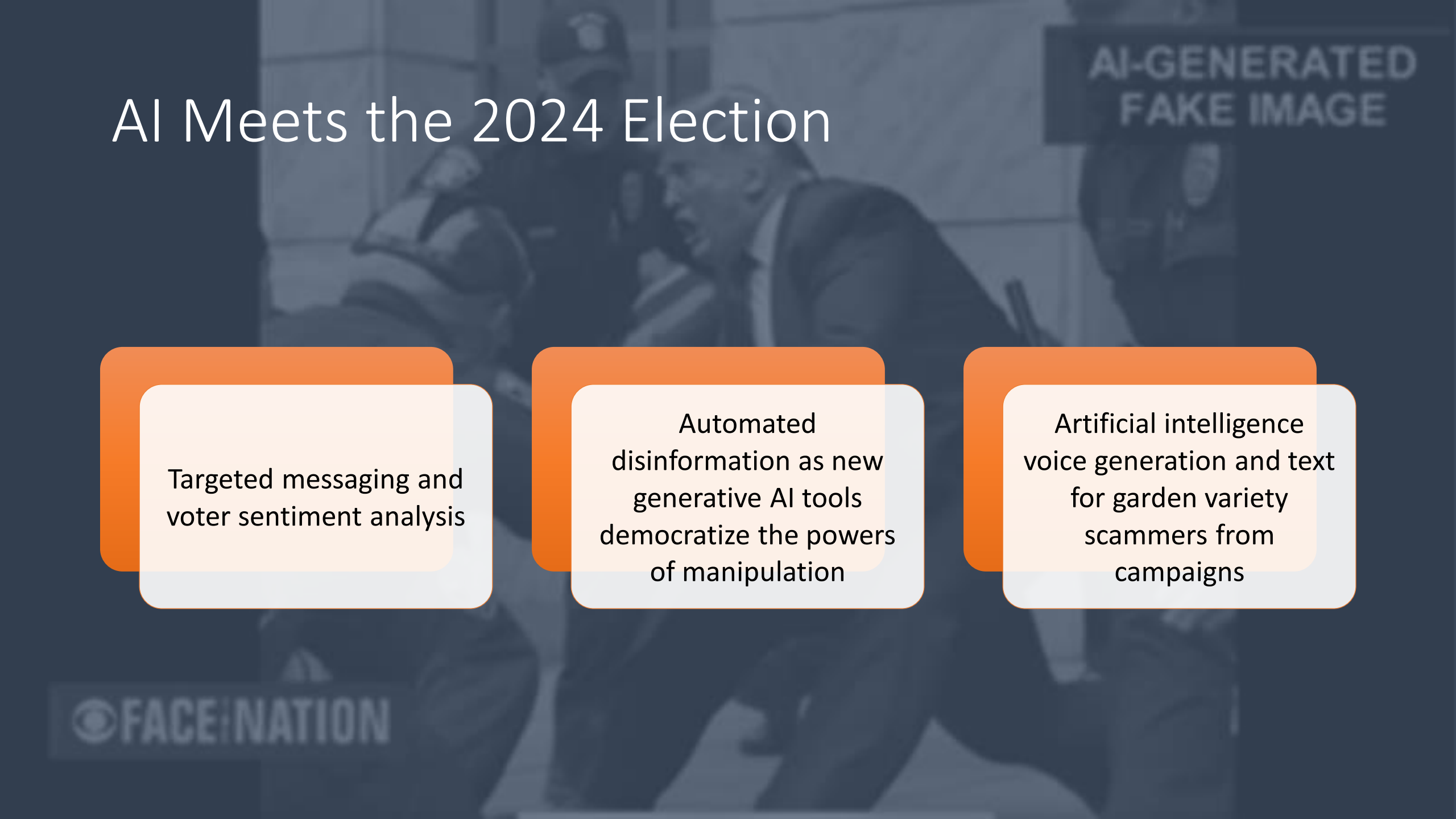
White House Announces Launch of the International Grand Challenges on Democracy-Affirming Technologies for the Summit for Democracy

DECEMBER 08, 2021 • PRESS RELEASES

Today, the White House Office of Science and Technology, with federal agencies and domestic and international stakeholders, announces the launch of a new initiative: a series of International Grand Challenges on

- Build democratic values into the next generation of technologies to go viral.
- Values? Trust, transparency, accountability, privacy.

AI Meets the 2024 Election



Targeted messaging and voter sentiment analysis

Automated disinformation as new generative AI tools democratize the powers of manipulation

Artificial intelligence voice generation and text for garden variety scammers from campaigns

AI Meets the 2024 Election: Automated Deception

For years, disinformation has focused on misleading text. In the 2024 election season, a spate of AI-generated audio and visual content will likely pollute the wires as well

Defense contractor and AI communications firm DeepMedia estimates that 500,000 video and voice deepfakes will be shared on social media this year.

Information Operations Weaponize Media

In 2016, 32 of 33 major American news outlets cited Russian troll accounts at least once in their coverage.

Responses: Technical

Prevention

- Content authenticity architectures
- Open standards, C2PA
- Partnerships between media and technical orgs

Protection

- Deepfake detectors (built into platforms)
- DARPA and NSF programs on ID’ing GANs

Responses: Policy

Principles:

- Prioritize authentic content online
- Clearly label modified or AI-generated content
- Guard against threats to elections

Legal Frameworks:

- *EU AI Act*: AI tools to sway voters are “high risk” requiring oversight
- *US*: State-level legislation on deepfakes against political candidates, harassment
- *China*: Registration and licensing requirements for AI that could sway public opinion; AI must adhere to “core socialist values”

What can we do -- now?

Adopt content provenance and authenticity technologies, such as in accordance with the C2PA standard for political communications.

Legislation such as the REAL Political Advertisements Act that requires disclosures of AI-generated text, images, video and audio in political content would provide a much-needed guardrail.

In the meantime, campaigns could commit to a voluntary pledge to label all AI-generated content.