



Enhancing Trust in Digital Spaces

APRIL 2025

Enhancing Trust in Digital Spaces

The United States has led the world in building an online ecosystem that has enabled growth, productivity and innovation across all sectors of the economy. Americans increasingly rely on digital technologies to conduct business, interact with the government and engage in civil society.

As artificial intelligence (AI) and other emerging technologies continue to transform the digital landscape, the public and private sectors have a crucial role to play in building and preserving trust in digital interactions, content and identities. The rise of AI-enabled deceptive content, such as deepfakes and unauthorized digital replicas of an individual's image or voice online, has introduced new avenues for online fraud and cybersecurity attacks. At the same time, the latest wave of AI innovation has the potential to revolutionize the way that the public and private sectors can identify and take action against these threats.

Business leaders and policymakers should work together to uphold collective trust and strengthen protections against fraud. The business community can build trust by creating and deploying technical tools to protect their customers and business operations, implementing effective governance approaches, and deepening and building new partnerships to share information and foster trust in digital spaces. Policymakers can also help to build trust by accelerating and enabling secure technologies, enacting safeguards for deceptive digital content and engaging with partners to stop malicious actors. Training and educational resources are also a critical part of building trust to help empower individuals and organizations to recognize and understand how to mitigate deceptive content.

Below are **best practices for businesses** and **recommendations for policymakers** to build trust online.

Building Trust through Digital Governance: Best Practices for Businesses

Businesses can develop and deploy new tools that improve digital trust.

- Embed or attach data characteristics to digital content that indicate when data has been tampered with, enabling users to verify the origin of images, videos or audio files.
- Replace knowledge-based approaches for verifying a person's identity (e.g., asking a series of questions only the account owner should know) with new approaches that are more secure against impersonation.
- Accelerate the use of phishing-resistant authentication (e.g., passkeys) that can defend against AI-enabled attacks.
- Use AI-powered fraud detection capabilities to enhance security of online transactions.
- Adopt controls to prevent brands from being spoofed or hijacked (e.g., Branded Caller ID, Domain-based Message Authentication, Reporting and Conformance for branded emails).
- Use secure, encrypted communication channels, data storage solutions and pre-established processes for sharing sensitive information or completing transactions.

Businesses can implement safeguards to prevent abusive or deceptive digital content.

- Implement policies for digital tools and services prohibiting their use in preparing or distributing fraud, scams and impersonation, along with clear processes for users to report violations of these terms.
- Create a formal notice and removal mechanism for unauthorized digital replicas and deepfakes, as well as a means to reinstate legitimate content.
- Where appropriate, implement automated and human mechanisms to evaluate content and address deceptive content.

Businesses can make education and training resources accessible to help individuals and organizations understand how to protect against deepfake-based attacks and scams.

- Provide regular training to employees on how to identify and respond to suspicious activities or communications.
- Make training resources available to clients, small businesses and other partner organizations, tailoring content as appropriate, to create a more secure ecosystem.

- Conduct tabletop exercises to validate governance processes while refining crisis management roles and procedures.
- Share best practices when using AI-enabled tools with images, videos or audio files that depict or include features of a recognizable person.
- Create public awareness materials to help people recognize deepfakes and how and when to report it.

Building Trust in Digital Spaces: Recommendations for Policymakers

Policymakers should enable and accelerate the adoption of more robust safeguards that enable trusted transactions online.

- Allow organizations to verify an individual's identity, with their consent, using authoritative government sources.
- Provide clear guidelines to minimize legal uncertainty around the use of new technologies such as mobile driver's licenses and passkeys.
- Prioritize U.S. participation in industry-led, voluntary and internationally accepted standards-setting bodies and regulatory forums, including those that are focused on identity, security and connectivity.
- Develop guidance and resources for states to launch new, interoperable tools for residents to better protect and assert their identities online (e.g., through mobile driver's licenses and other portable identity credentials).

Policymakers should enact safeguards against deceptive content (e.g., unauthorized representations of an individual's image, voice or visual likeness online).

- Clarify an individual's ability to control the public communication of their name, image or voice.
- Enact a new, comprehensive federal statute that prohibits a person or entity from intentionally and knowingly committing deceptive acts through the public communication of a representation of an individual's image, voice or visual likeness.
- Protect organizations' abilities to remove harmful synthetic content using a statutory complaint notice process.
- Protect permissible uses of synthetic digital content, such as parody, newsworthiness, comment and criticism, scholarship and private uses.

Policymakers should enforce existing laws to stop fraud, scams and deceptive impersonation perpetrated by malicious actors, including through the use of AI.

- Direct the Department of Justice to prosecute and seek penalties for digital impersonation cases where harm to the impersonated individual is established.
- Urge relevant federal independent regulators (e.g., Federal Communications Commission, Federal Trade Commission) to prioritize enforcement against malicious actors who use AI to commit fraud, scams and deceptive impersonation.
- Collaborate with global allies to investigate, prosecute and seek penalties for AI-enabled fraud and other crimes.

About Business Roundtable

Business Roundtable is an association of more than 200 chief executive officers (CEOs) of America's leading companies, representing every sector of the U.S. economy. Business Roundtable CEOs lead U.S.-based companies that support one in four American jobs and almost a quarter of U.S. GDP. Through CEO-led policy committees, Business Roundtable members develop and advocate directly for policies to promote a thriving U.S. economy and expanded opportunity for all Americans. Learn more at www.brt.org.