NAVIGATING THE NEW AI FRONTIER

Mitigating Risks and Safeguarding Reputation in an Evolving Landscape

Authors: Rhett Skelton, Michael McMenemy, Jonathan Newton

GAME CHANGERS

Ipsos

KEY TAKEAWAYS:

1. **A new threat to reputation and business**: AI presents a unique threat to companies trying to safeguard their reputation. Bad actors from around the world can leverage AI's capabilities in the areas of social engineering, image or video fabrication, and phishing/scams for personal gain, inflicting severe damage to a business' reputation along the way.
2. **Know who you are**: Understanding the potential impact of these threats requires knowing where your corporate reputation currently stands, and what key stakeholders expect. Having a baseline measurement program in place can help prioritize actions that have the greatest impact on corporate perceptions.
3. **Fight fire with fire**: In the ever-changing reputational landscape it is now vital for companies to employ a multifaceted, AI-driven strategy to stay ahead of threats. Both traditional research solutions combined with digital surveillance ensure your reputation is protected from threats both known and unknown.
4. **Planning for the future**: An internal task force comprised of experts in AI, data science, cybersecurity, policy, and communications will be central to the protection of a company's reputation. Improving AI literacy across the organization and identifying potential AI-driven risks will ensure the ability to react swiftly to AI-aided threats.

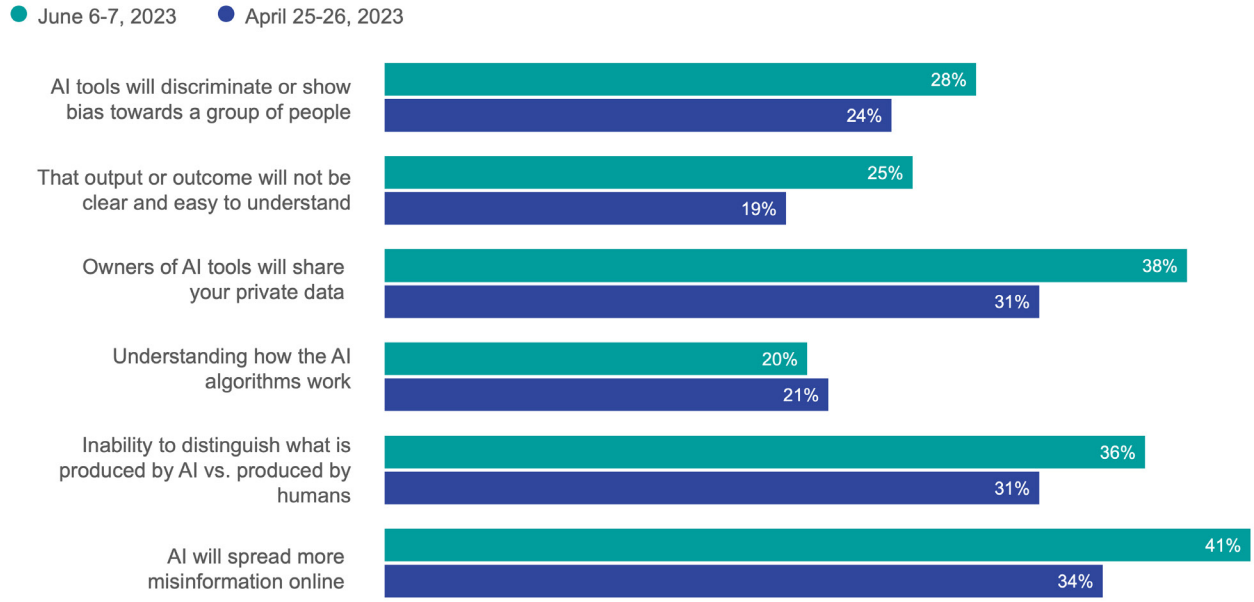
"Your identity is like your shadow: not always visible and yet always present" – *Stanislaw Lem, Solaris*

Artificial intelligence (AI) has emerged as a powerful force that shapes industries, transforms businesses and influences every aspect of our lives. Its proliferation and democratization will lead to unprecedented and rapid advancements, paving the way for innovative applications that improve efficiency and enhance customer experiences.

At the same time, AI anxiety is increasing, according to recent surveys from the Ipsos Consumer Tracker. Ipsos also finds that understanding of the technology hasn't kept pace, according to a recent Ipsos Global Views publication on AI. AI's unique challenges and the unprecedented risks it presents to large corporations seeking to protect their reputations and brand integrity haven't received much public fanfare.

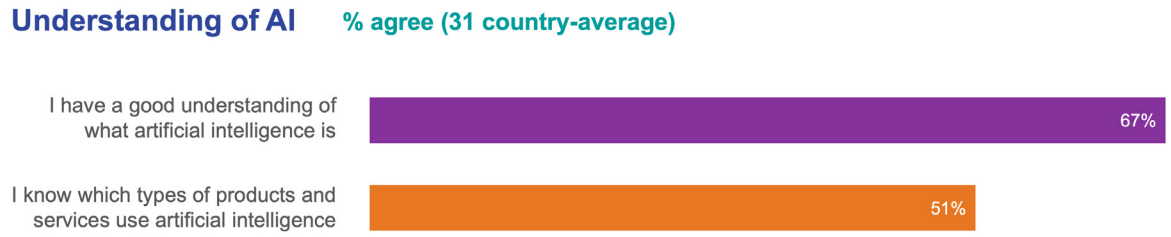
The degree of our worry about AI is increasing for some

Q: When thinking about possible uses for AI, how worried, if at all, are you about each of the following? - % Very worried



Source: Ipsos Consumer Tracker, fielded June 6 - 7, 2023 among 1,108 U.S. adults.

Understanding of AI is still lagging



Base: 22,816 adults under the age of 75 across 31 countries, interviewed May 26 – June 9, 2023 -- online only in all countries except India. The "Global Country Average" reflects the average result for all the countries where the survey was conducted. It has not been adjusted to the population size of each country or market and is not intended to suggest a total result.

Source: Ipsos | Global views on AI 2023

For example, generative AI, a subset of AI technology, enables the creation of synthetic media and brings immense potential for positive contributions, especially for creative industries. At the same time, synthetic media introduces significant risks for all businesses. Anyone, even the least tech-savvy fraudsters, with the assistance of AI, can now create realistic, fake audio and video content in sophisticated schemes. Bad actors can further exploit generative AI to create fraudulent content used in scams, phishing attempts, or even attributed to corporations, maligning their reputation.

How do companies address emerging risks and safeguard their brand in this new AI-driven era? The key steps are to:

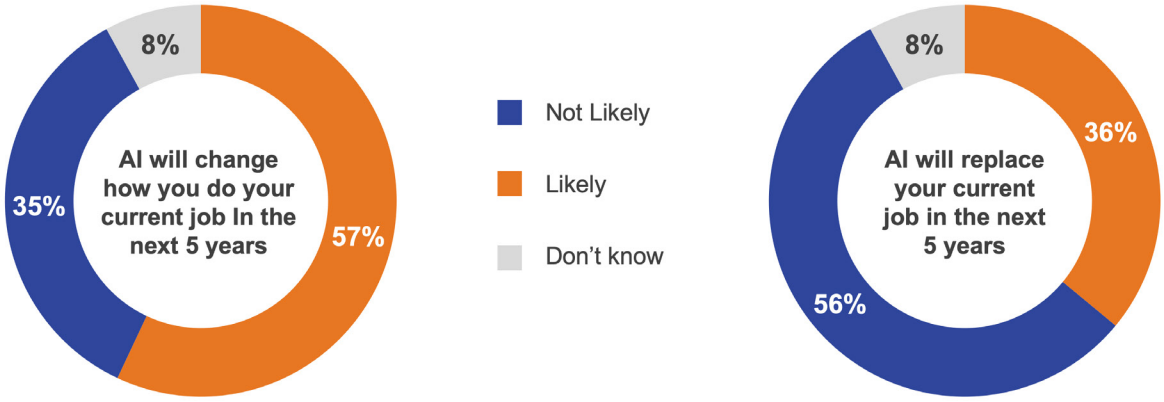
1. Consider the perils of AI proliferation, or various ways that bad actors may use the technology
2. Assess your organization's risks and reputational impacts
3. Monitor the key impact areas for potential new threats
4. Plan how to respond to any threats known or unknown

Consider the Perils of AI Proliferation

The democratization of AI opens the door to potential threats, as individuals with limited coding experience and bad intentions can exploit the technology for their gain. Much has been written about how AI-powered products and services are anticipated to impact individuals. Recent Ipsos research even shows that 57% of workers expect AI to change the way they work and 36% expect it to replace them completely (Ipsos Global Views on AI).

Impact of AI on Current Job

Q. How likely, if at all, do you think it is that… ***(31-country average)***



Base: 22,816 adults under the age of 75 across 31 countries, interviewed May 26 – June 9, 2023 -- online only in all countries except India.

The "Global Country Average" reflects the average result for all the countries where the survey was conducted. It has not been adjusted to the population size of each country or market and is not intended to suggest a total result.

The samples in Brazil, Chile, Colombia, India, Indonesia, Ireland, Malaysia, Mexico, Peru, Romania, Singapore, South Africa, Thailand, and Turkey are more urban, more educated, and/or more affluent than the general population

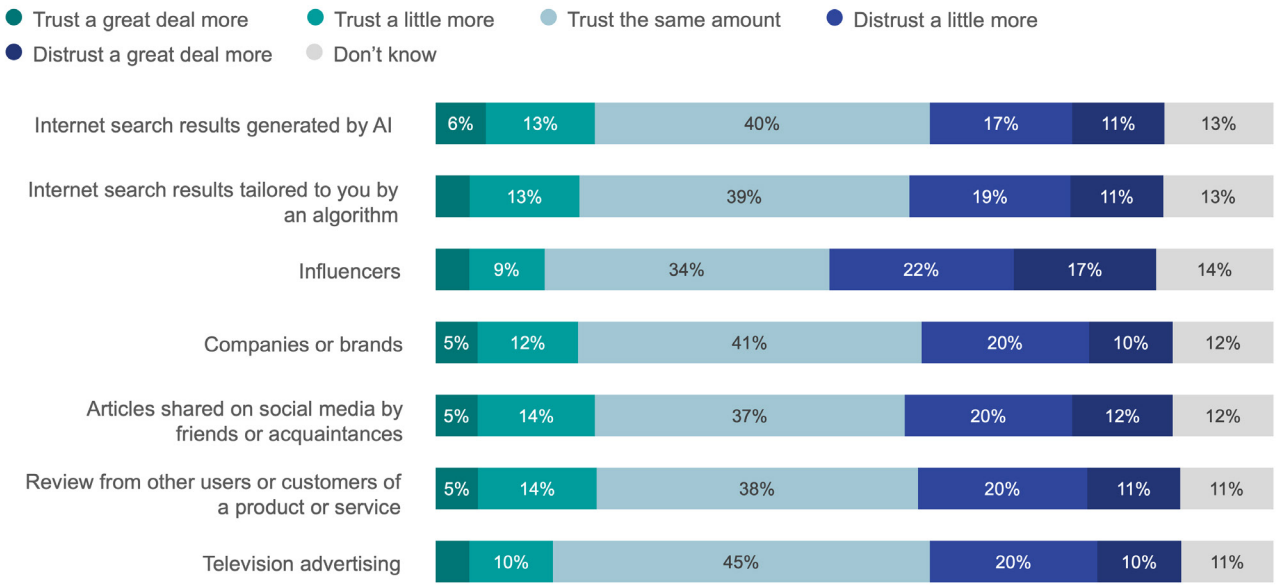
Less commonly discussed, however, are the potential negative consequences that these advancements will have for businesses and how the impact on a business' reputation could be devastating. For example:

- **Social engineering attacks** can leverage AI-generated artificial voices that are indistinguishable from a real human's voice enable frauds to create scams that mimic the voices of corporate executives to deceive employees into providing sensitive information or initiate fraudulent financial transactions.
- **Image fabrication**, which is the ability for scammers to develop photorealistic videos and images that portray fictitious scenarios involving a company's executives, operations, or internal communications. This emerging threat can then severely damage a company's reputation by creating negative perceptions and leading to significant financial losses.
- **Phishing and scams** will be enhanced with tools like WormGPT which aid in launching sophisticated business email compromise (BEC) attacks. These events are no longer confined to traditional means either as AI-driven techniques make it easier for criminals to create more convincing and personalized deceptions using voice and video masking, making detection difficult.

Internally, attacks with generative AI tools can deceive employees and spread harmful and incorrect information, cause panic or unrest within a company and impact response times when dealing with a corporate crisis. Externally, such intrusions can undermine trust in corporate communications, leading to financial losses and irreparable damage to a brand's reputation.

People are likely to distrust AI-created content

Q: Now, if AI were to be more widely used by the following, would that make you trust them more, less or the same?



Source: Ipsos Consumer Tracker, fielded February 14 – February 15, 2023 among 1,109 U.S. adults

Assess Your Organization's Risks and Reputational Impacts

To effectively mitigate the risks associated with AI-generated threats, companies must first identify and prioritize potential impacts on their business and reputation. A comprehensive risk assessment is crucial to understand where vulnerabilities lie and to develop tailored strategies for mitigation.

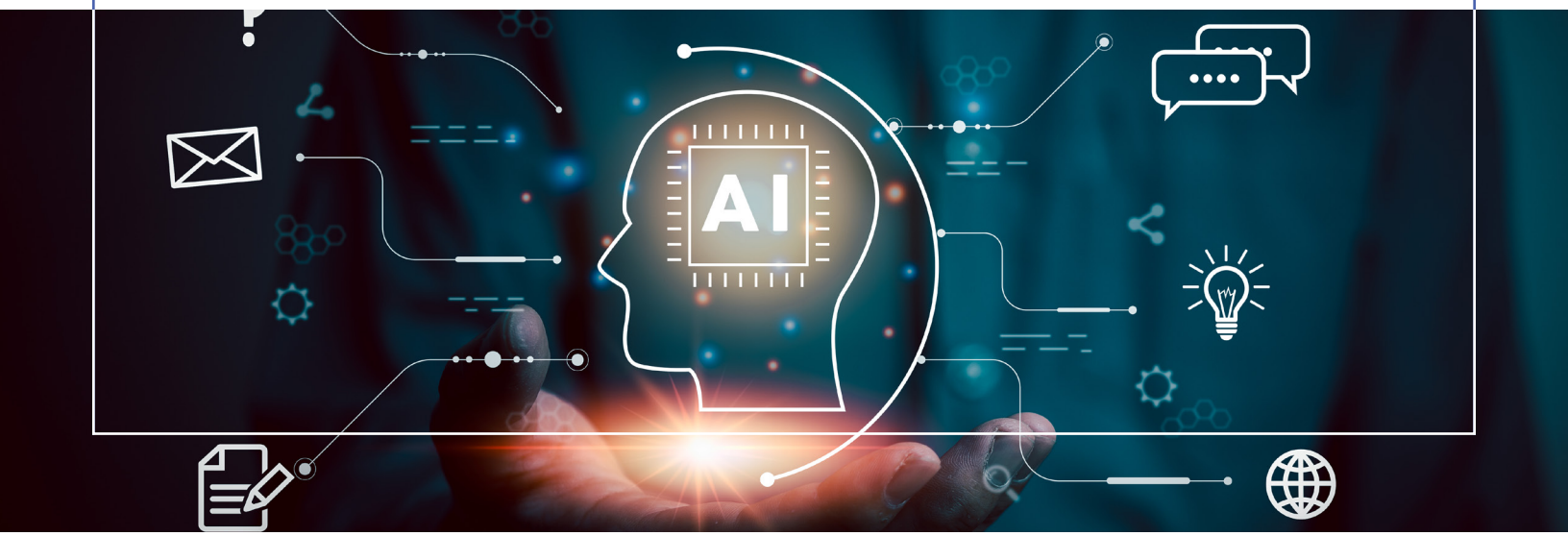
- **Identify Vulnerabilities:** Companies should conduct in-depth assessments of their current technological landscape, data security protocols, and communication channels. Identifying potential points of vulnerability will allow organizations to implement targeted defenses against AI-driven risks.
- **Understand AI Misuse:** By understanding how generative AI can be misused, corporations can better anticipate and combat potential threats. Staying up to date on the latest developments in AI technology, and its potential risks, is vital to developing proactive risk management strategies.
- **Predicting Future Threats:** Companies must continue to think ahead and anticipate how AI technologies are evolving and could be exploited in the future. Adopting a forward-thinking approach enables organizations to stay ahead of potential threats and be better prepared to respond.

Monitor the Key Impact Areas

Having identified potential risks, corporations should establish a comprehensive toolkit to continuously monitor these AI-driven threats over time. This toolkit should consist of three essential components.

- **AI-Based Threat Detection:** Leverage AI technology for defense. Organizations need to identify data that can help monitor reputational shifts, set up near real-time data feeds to monitoring tools, then train AI or large-language models that monitor abnormal events, especially in key metrics.
- **Human Oversight:** While AI can be effective in detecting certain risks or shifts in key metrics, human oversight remains critical. A team of experts should monitor multiple data streams and verify AI-generated content, differentiating between legitimate and malicious material.
- **Collaborative Partnerships:** Engage in collaborations with AI research institutions, cybersecurity experts, and reputation and technology leaders. Such partnerships foster knowledge-sharing and collective efforts to address emerging risks.

Given the multi-faceted challenges now facing companies, one-dimensional approaches to safeguarding reputation are no longer adequate. Staying ahead of threats means adopting a surveillance program such as Ipsos' Reputation Intelligence for Strategic Evaluation (RISE) platform that leverages multiple insights streams including traditional survey data as well as AI-curated social listening data, media information, and other non-survey sources.



Plan How to Respond

To tackle AI-related risks and opportunities effectively, corporations should establish a dedicated internal task force. This team should comprise individuals with expertise in AI, data science, cybersecurity, policy, and communications. The AI task force's key responsibilities include:

- **Risk Management:** Identify, analyze, and prioritize potential AI-driven risks, formulating strategies to mitigate these threats effectively.
- **Education and Training:** Foster a culture of AI literacy across the organization. Provide training to employees to recognize and respond to AI-generated threats.
- **Crisis Response:** Develop and rehearse crisis response plans to handle AI-related reputation emergencies promptly.

What's Next

Generative AI is forcing business leaders and regulators to reimagine the role technology plays in our lives, leaving the tech industry, policymakers, and Americans writ large scrambling for what is to come.

Right now, no one has answers. Even the questions we should be asking are unclear. Even so, it is vital that decisions be made with the public's opinion in mind. By keeping these three points in mind, executives can better read the room on artificial intelligence—and make better decisions in the future.

1. Americans are feeling a wide range of emotions towards AI. Most do not see AI as disruptive.
2. The public would rather have companies developing AI to regulate AI themselves rather than the government—but Americans hold reservations with private-sector regulation, too.
3. AI might not be an exception in our partisan times. The closer the technology or business model is to polarization, the greater the reputational and regulatory risks.

Authors:

Rhett Skelton
SVP, Ipsos Corporate Reputation
Rhett.Skelton@Ipsos.com

Michael McMenemy
Director, Ipsos Corporate Reputation
Michael.Mcmenemy@Ipsos.com

Jonathan Newton
Account Manager, Ipsos Corporate Reputation
Jonathan.Newton@Ipsos.com

About Ipsos

At Ipsos we are passionately curious about people, markets, brands, and society. We deliver information and analysis that makes our complex world easier and faster to navigate and inspires our clients to make smarter decisions. With a strong presence in 90 countries, Ipsos employs more than 18,000 people and conducts research programs in more than 100 countries. Founded in France in 1975, Ipsos is controlled and managed by research professionals.