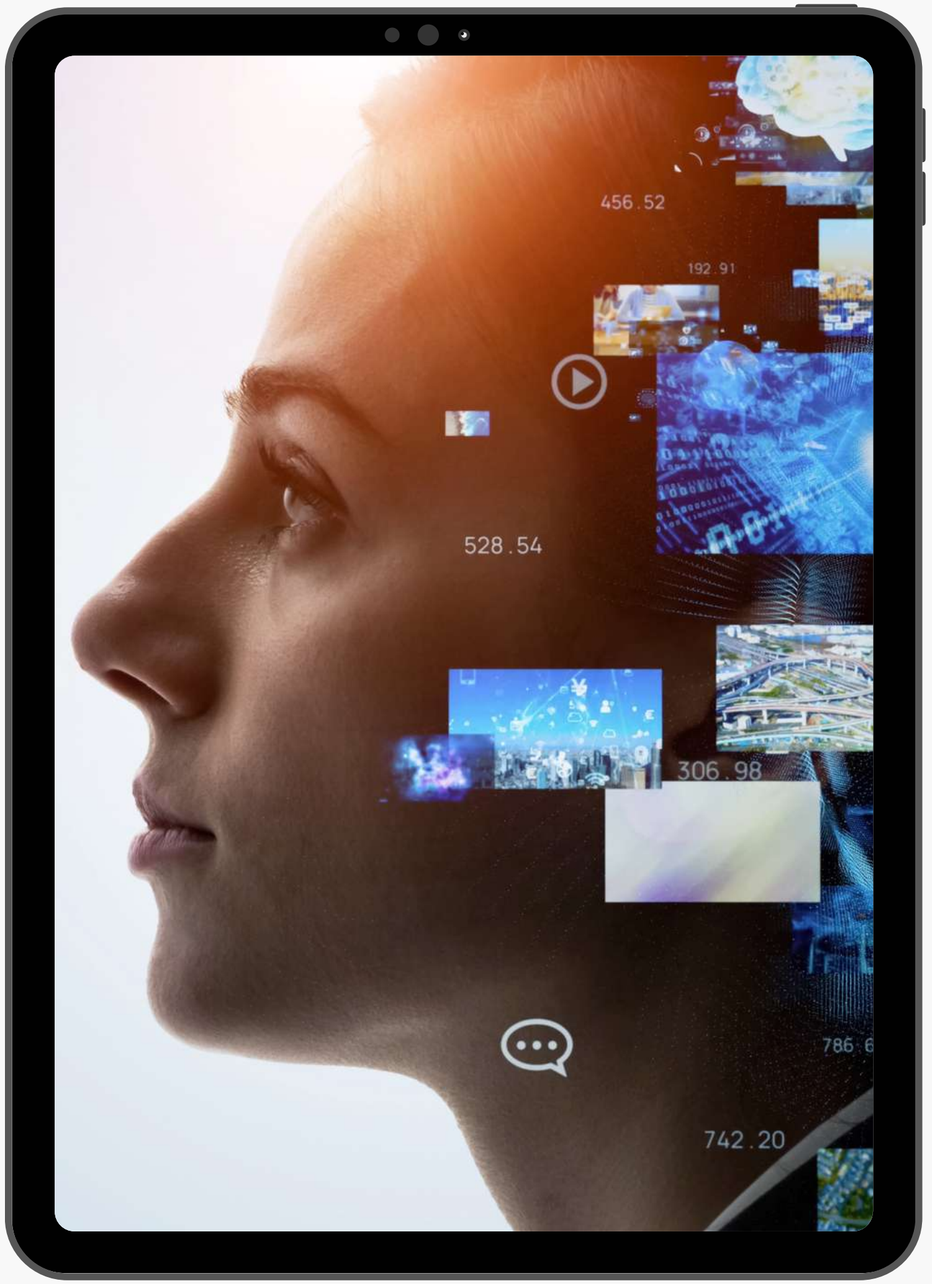
AI in the Enterprise: Preparing for the Future of Cybersecurity and Data Privacy

November 3, 2023



Debbie Reynolds

Founder, CEO, and Chief Data Privacy Officer, Debbie Reynolds Consulting, LLC

- A leading voice in Data Privacy and Emerging Technology
- Hosts award-winning #1“The Data Diva” Talks Privacy Podcast
- Featured by media outlets like PBS, New York Times, Wired, Business Insider, Protocol, USA Today, New Statesman, Dark Reading, Morning Brew, Lifewire, CMSWire, Bloomberg, Digiday
- Recognized as one of the Global Top Eight Privacy Experts by Identity Review
- Named one of the Global Top 30 CyberRisk Communicators by The European Risk Policy Institute in 2020 and 2021
- Appointed to the U.S. Department of Commerce's IoT Advisory Board in 2022
- Serves as the IEEE Committee Chair for Cyber Security for Next Generation Connectivity Systems at IEEE for Human Control & Flow

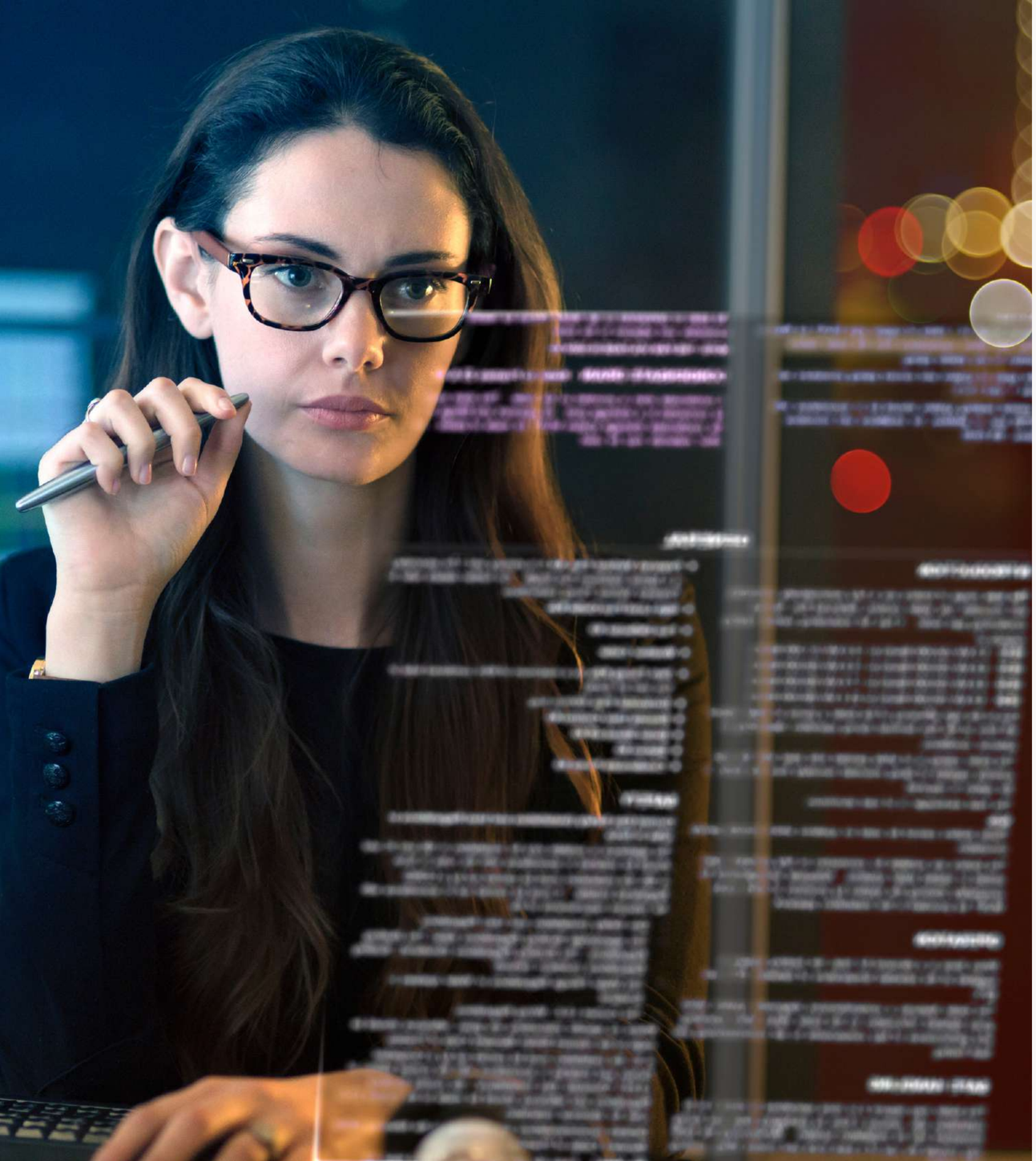
AGENDA

- Statistics
- Harnessing Real-Time Insights
- Navigating the Velocity of Change
- Combating Unauthorized Access
- Addressing AI Risk Drift
- Cultivating a Culture of Rapid Learning

STATISTICS

- 9 in 10 organizations back AI to give them a competitive edge over rivals.

(MIT Sloan Management)



- 40% of the global workforce will have to learn new skills over the next three years due to AI implementation.

(IBM Institute for Business Value (IBV) Research, 2023)

- 57% of CEOs surveyed are concerned about the data security of AI.

(IBM Institute for Business Value (IBV) Research, 2023)

HARNESSING REAL-TIME INSIGHTS

Harnessing Real-Time Insights

- Access to up-to-date information allows for more informed and timely decision-making
- Businesses can respond quickly to market changes, customer behaviors, and operational challenges
- Real-time data analysis can identify bottlenecks, inefficiencies, and opportunities for optimization in various business processes, leading to improved productivity and reduced costs

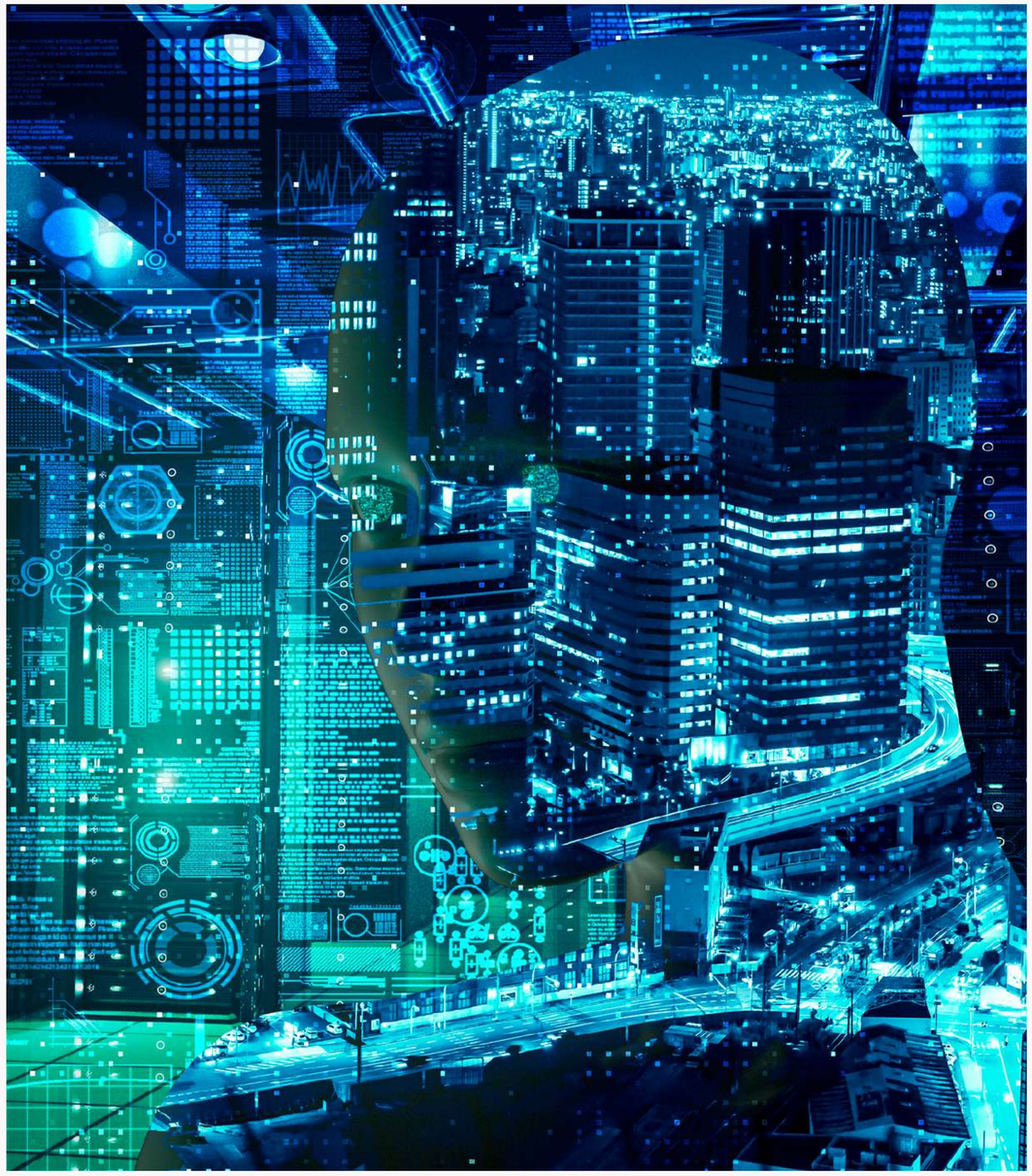
NAVIGATING THE VELOCITY OF CHANGE

Navigating the Velocity of Change

- Rapid changes in job roles and functions
- Expectation to leverage AI to boost productivity
- Creating a short feedback loop for fine-tuning and interactions

COMBATING UNAUTHORIZED ACCESS

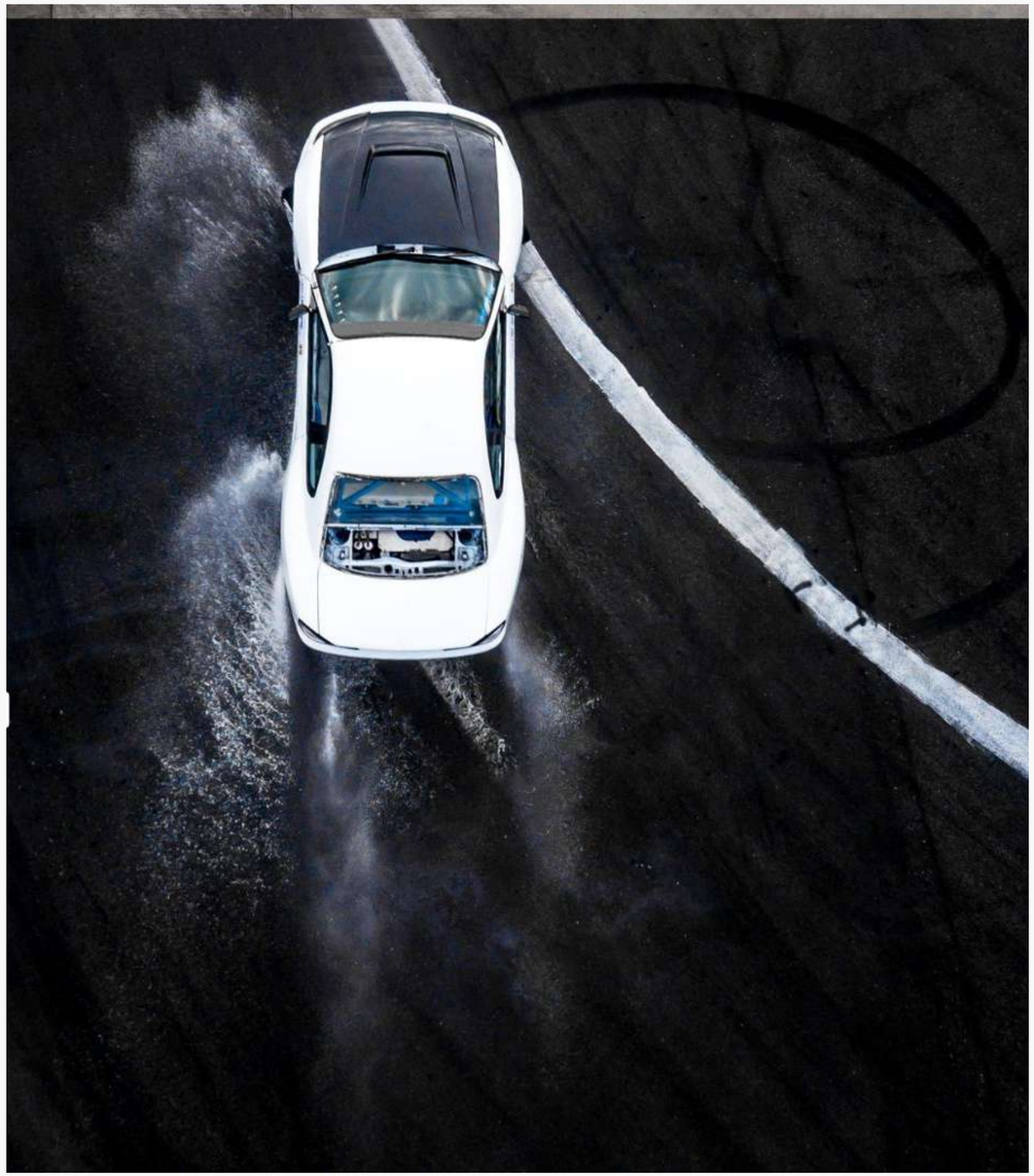
Combating Unauthorized Access



- Unauthorized Access to Human Data
- Unauthorized Access to Company Data
- Unauthorized Access to Model Data
- Data Lineage will be vital to AI use in the future

ADDRESSING AI RISK DRIFT

Addressing AI Risk Drift



- Drift from Using AI as a Helper to Automated Decision-Making
- Drift from Low Stakes to High Stakes Use Cases
- Drift from Correlation into Inference

CULTIVATING A CULTURE OF RAPID LEARNING

Cultivating a Culture of Rapid Learning

- Rapid advances in AI capabilities and Use Cases
- Finding Opportunities to leverage AI in new ways
- Continuous Training of AI features

Takeaways

- AI as a Competitive Necessity
- Workforce Transformation
- Security and Privacy Challenges
- AI's Evolution in Decision-Making
- Necessity of Continuous Learning

Resources

- House, The White. “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.” The White House, 30 Oct. 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

- “AI Risk Management Framework.” NIST, July 2021. www.nist.gov, https://www.nist.gov/itl/ai-risk-management-framework

- “Blueprint for an AI Bill of Rights | OSTP.” The White House, https://www.whitehouse.gov/ostp/ai-bill-of-rights/

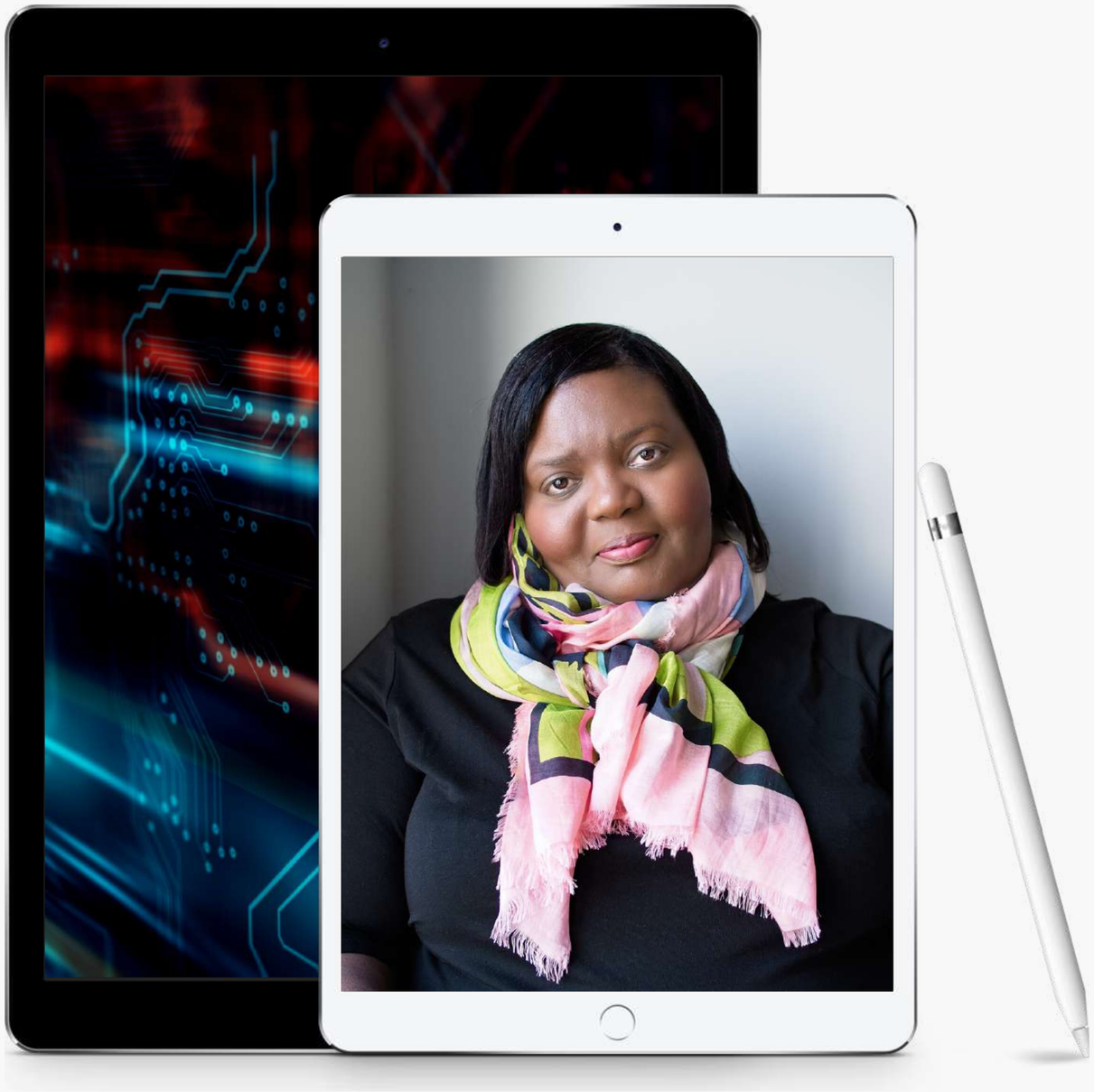
- House, The White. “FACT SHEET: Biden-Harris Administration Announces National Standards Strategy for Critical and Emerging Technology.” The White House, 4 May 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-national-standards-strategy-for-critical-and-emerging-technology/.

Resources

“The AI Risk Drift and Its Impact on Data Privacy for Organizations.” Debbie Reynolds Consulting LLC, https://www.debbiereynoldsconsulting.com/data-privacy-advantage/the-ai-risk-drift-and-its-impact-on-data-privacy-for-organizations

“How Generative AI Amplifies Unauthorized Access Privacy Risks with Enterprise LLMs.” Debbie Reynolds Consulting LLC, https://www.debbiereynoldsconsulting.com/data-privacy-advantage/how-generative-ai-amplifies-unauthorized-access-privacy-risks-with-enterprise-llms

“Data Privacy in the AI Era: Five Challenges Raising the Stakes for Businesses.” Debbie Reynolds Consulting LLC, https://www.debbiereynoldsconsulting.com/data-privacy-advantage/data-privacy-in-the-ai-era-five-challenges-raising-the-stakes-for-businesses



CONTACT US

DEBBIE REYNOLDS

DEBBIE REYNOLDS CONSULTING, LLC
HTTPS://WWW.DEBBIEREYNOLDSCONSULTING.COM
DATADIVA@DEBBIEREYNOLDSCONSULTING.COM
+1-(312) 513-3665