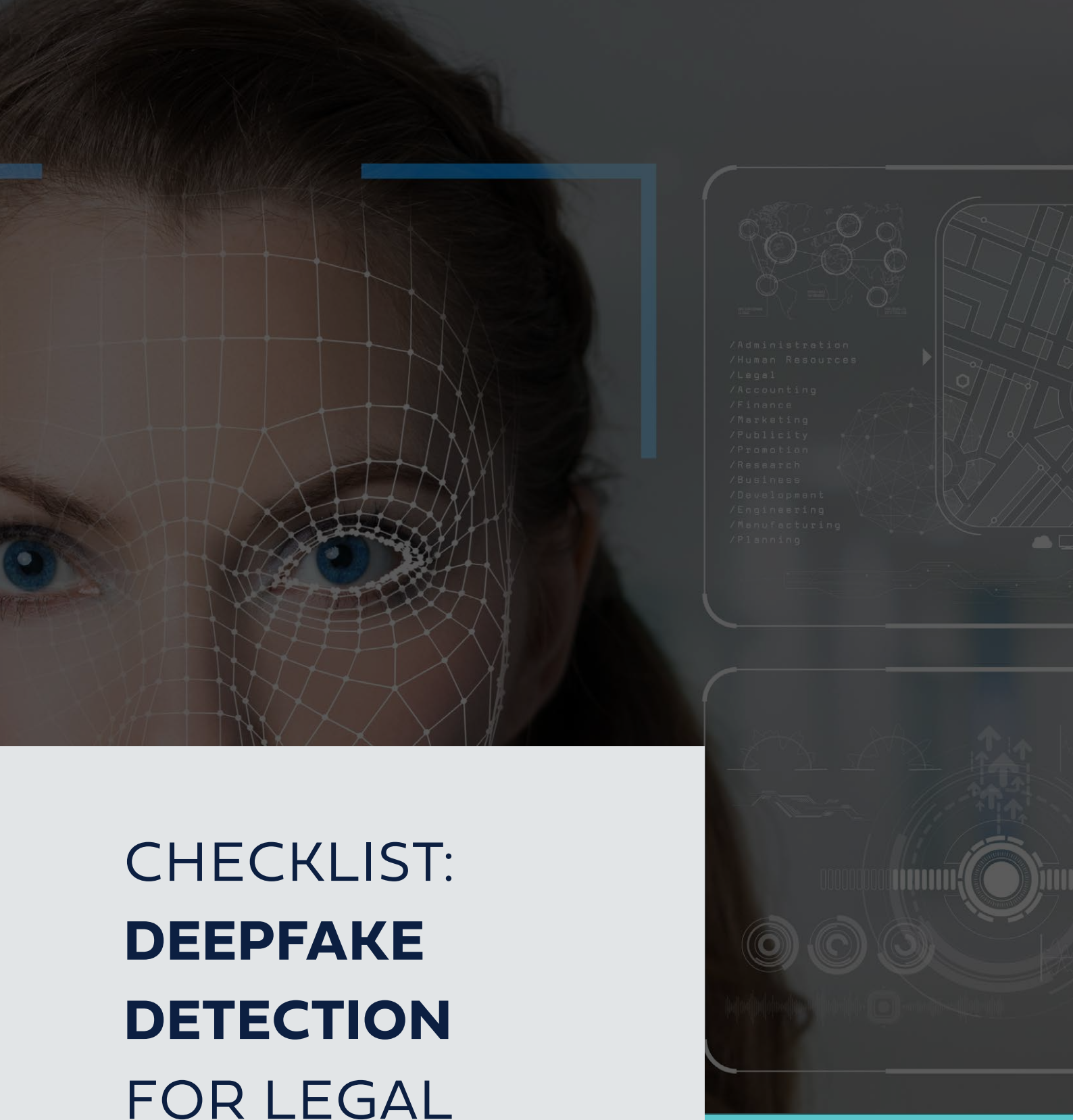

CHECKLIST: **DEEPFAKE DETECTION** FOR LEGAL PROFESSIONALS

consultwebs

Welcome to a critical juncture in legal technology.

Deepfakes – AI-generated videos indistinguishable from reality – are rapidly emerging as a new frontier in legal challenges. Understanding and detecting them is no longer optional; it's imperative.

This checklist equips you with essential knowledge and tools.

Get Familiarized with Deepfake Technology

- Understand the basics of AI and machine learning used in deepfakes. Here are some articles and article listings worth checking out:
  - **Deepfakes, explained**
  - **Deepfakes: The Ugly, and the Good**
  - **Article Collection on Deepfakes (The Conversation)**
  - **Subscribe to Key Publications for Updated Info**
- Share findings with the team regularly, or have a dedicated team member/team for AI research in umbrellas like Deepfake.

Examples of Deepfake Attacks

Below are highly sophisticated deepfake attacks that can deceive people.

Zoombombing

This is when an uninvited guest joins a Zoom meeting to hijack, spy, or disrupt the meeting. Sometimes the attacker even impersonates a team member or authorized employee. This scenario happened recently when a **hacker tricked a group of investors and crypto developers** by impersonating a Binance executive using a hologram in a Zoom call.

Vishing

A type of attack using a combination of email and voice-based phishing (or vishing) to breach a corporate network, e.g., attackers posing as tech support.

Biometrics Attack

A type of attack where the hacker uses voice or face recognition by imitating the victim's face or voice.

Ways to Mitigate the Risk of Deepfakes

- The best way to learn how to fight and prevent deepfakes is to see them first-hand — exposure.
- Provide training that will help everyone in the company to fully understand deepfake threats.
- Run a series of tests or drills to check who will fall into deepfake attacks.
- Adjust and revise the company's threat protocols based on the result.

Invest in Detection Software

- Acquire AI-based detection tools.
  - **Deepware**
  - **Sensity**
  - **Truepic**
- Train staff in using these tools.

DEEPFAKE DETECTION FOR LEGAL PROFESSIONALS

Review Visual and Audio Cues

- Check for inconsistencies in lighting, facial expressions, or lip sync.
- Listen for irregularities in voice patterns or audio quality.

Implement Verification Protocols

- Establish firm-wide guidelines for media verification.
- Double-check sources and cross-verify information.

Encourage Vigilance and Reporting

- Promote a culture of awareness and responsibility.
- Set up a system for reporting suspected deepfakes.

DEEPFAKE DETECTION FOR LEGAL PROFESSIONALS

Consult Experts
When Needed

- Reach out to tech experts for complex cases.
- Collaborate with IT security for enhanced protection.

Review
Legal Implications

- Stay informed about legal aspects related to deepfakes.
- Update policies as per evolving legal standards.

Educate
Clients

- Inform clients about the risks of deepfakes.
- Provide guidance on how to identify potential deepfakes.

If you'd like to learn more about protecting and managing your firm's branding with a team of experts–

we're here to help!