AZ JUDICIAL CONFERENCE

Artificial Intelligence & The Weaponization of Personal Data

AI Deepfakes and Security

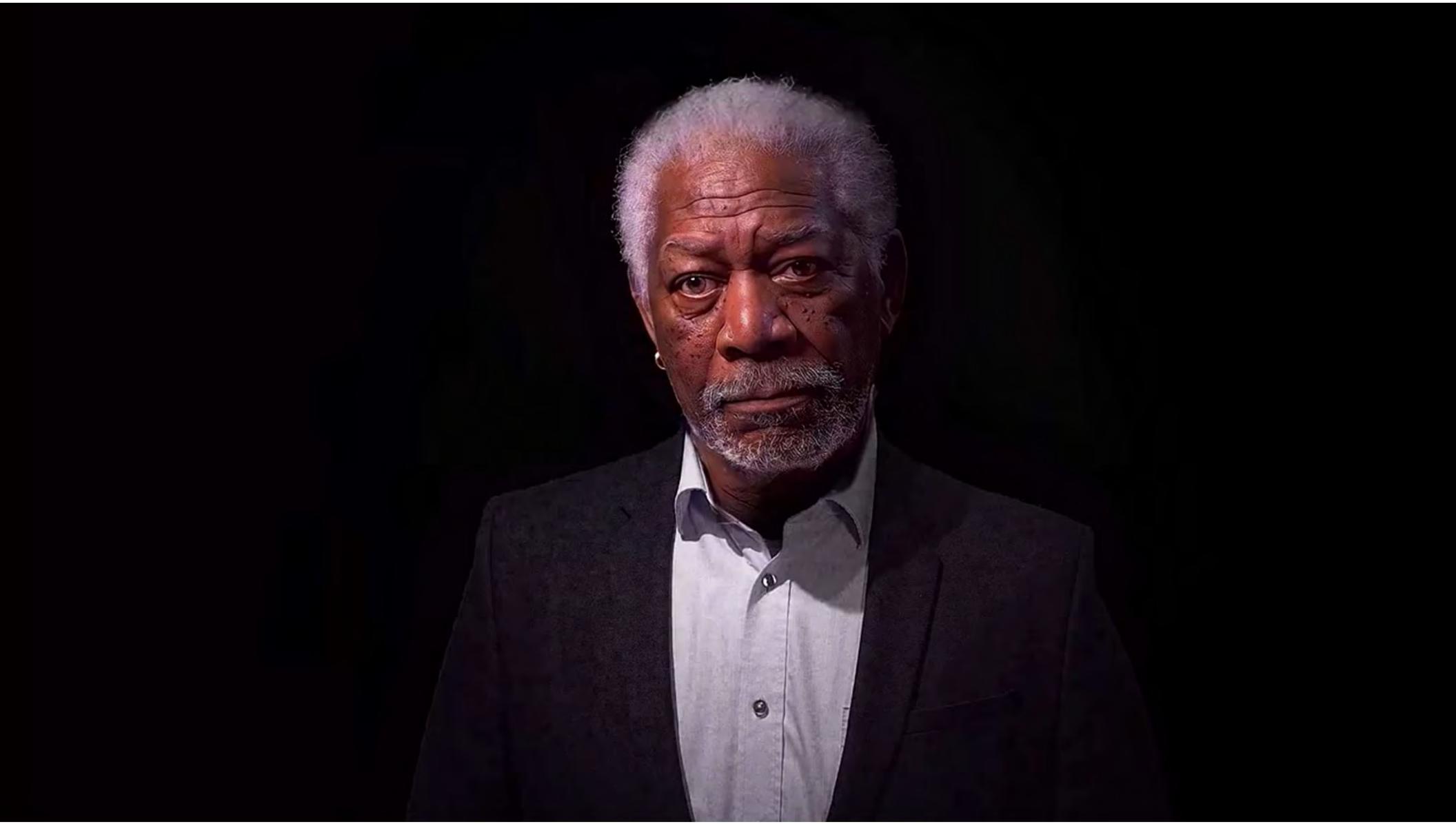
Brian M. Chase, Esq.

Managing Director of Digital Forensics & eDiscovery

BChase@ArcherHall.com

855.839.9084

ARCHERHALL
AIM HIGH



AI – The Next Big Problem

AI vs. Generative AI

Traditional AI

Trained to accomplish specific tasks, such as identifying images. Primary used to analyze data.

Generative AI

Focused on creating new content. This is the type that we have been seeing in the news.

Generative AI

ChatGPT

Nov. 2022

Version 3.5

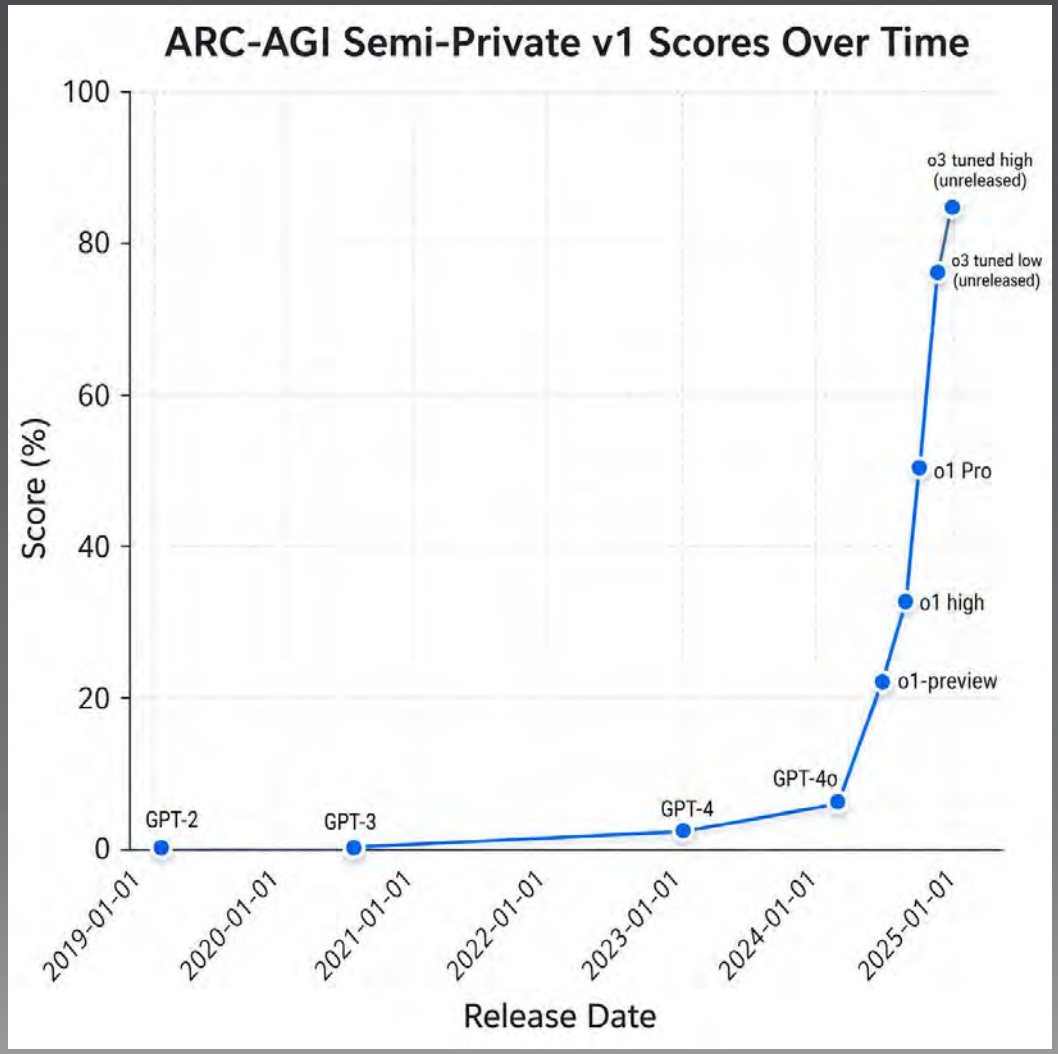
Took the bar exam and failed.
Finished in the 10th Percentile.

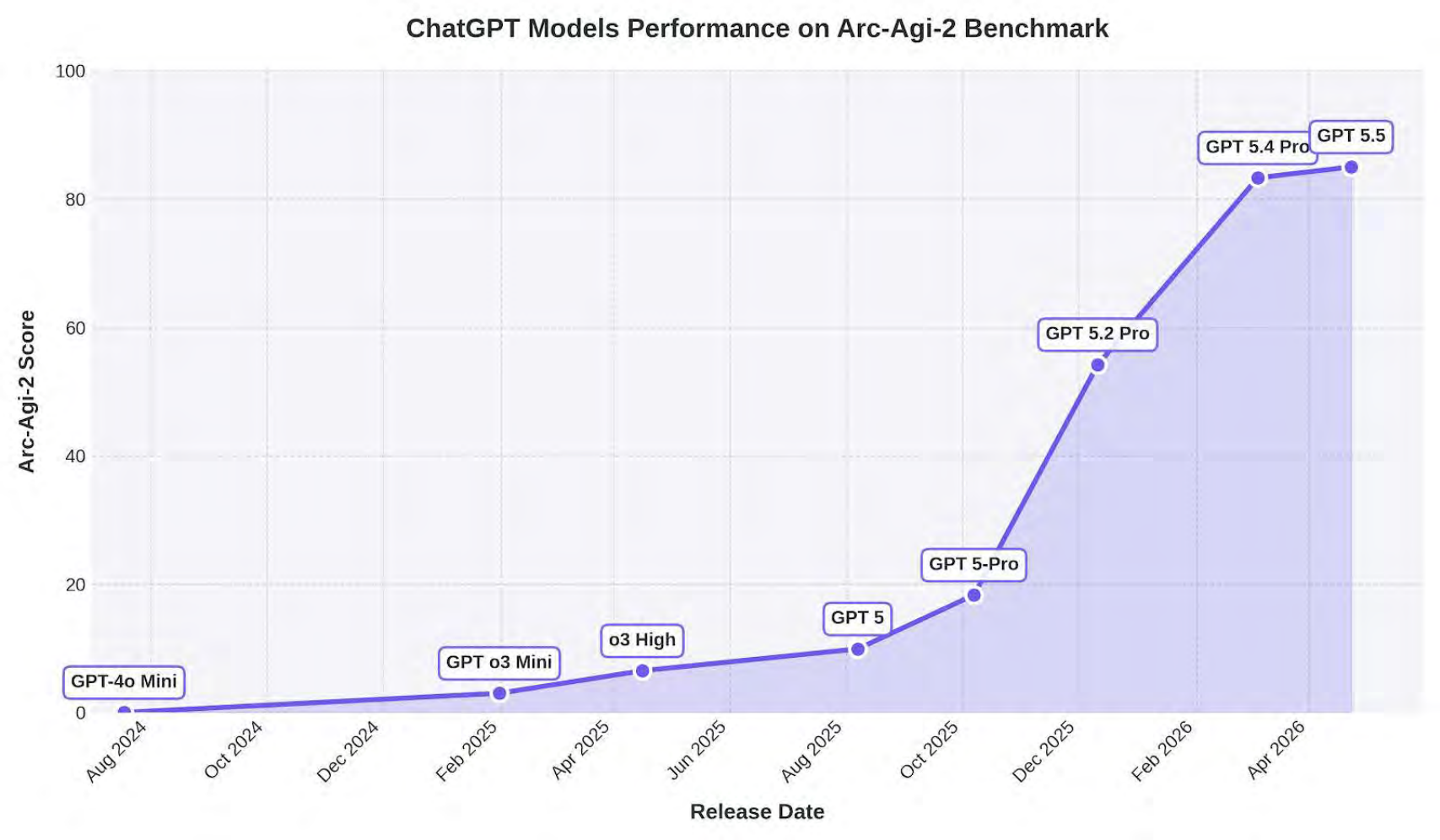
Version 4.0

Took the bar exam and passed.
Finished in the 90th Percentile.

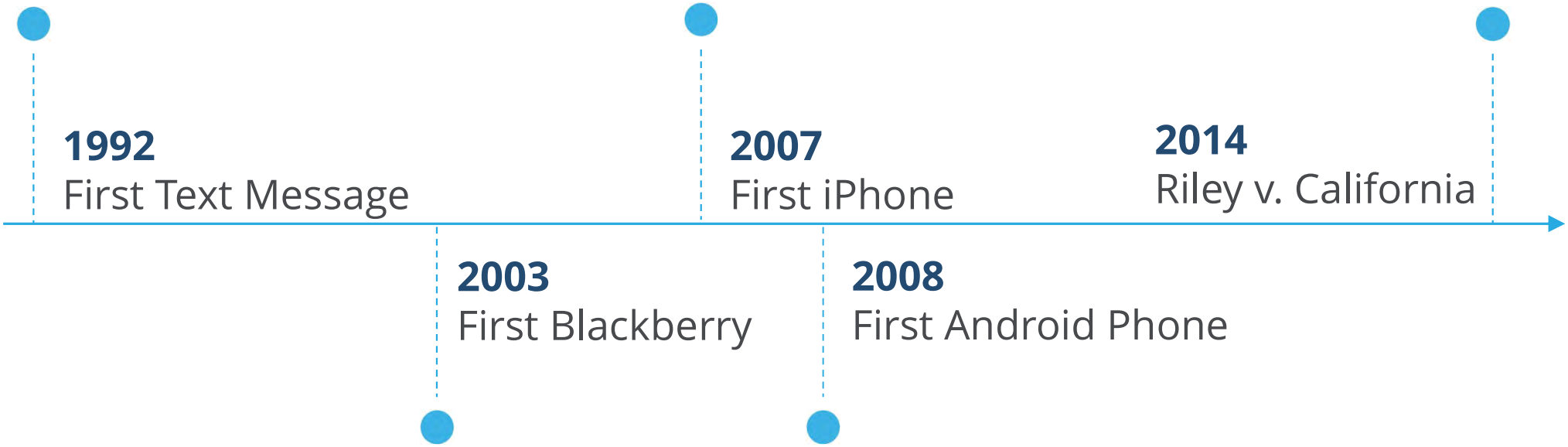
Mar. 2023

The Exponential Bus


ARC-AGI Semi-Private v1 Scores Over Time
Score (%)
100
80
60
40
20
0
GPT-2
GPT-3
GPT-4
GPT-4o
o1-preview
o1 high
o1 Pro
o3 tuned low
(unreleased)
o3 tuned high
(unreleased)
2019-01-01
2020-01-01
2021-01-01
2022-01-01
2023-01-01
2024-01-01
2025-01-01
Release Date


ChatGPT Models Performance on Arc-Agi-2 Benchmark
Arc-Agi-2 Score
100
80
60
40
20
0
GPT-4o Mini
GPT o3 Mini
o3 High
GPT 5
GPT 5-Pro
GPT 5.2 Pro
GPT 5.4 Pro
GPT 5.5
Aug 2024
Oct 2024
Dec 2024
Feb 2025
Apr 2025
Jun 2025
Aug 2025
Oct 2025
Dec 2025
Feb 2026
Apr 2026
Release Date

Is the Law Too Slow?



US Evidence Committee

- **Committee Chair: Panels agrees litigants concerns that rules, as written, do not work for challenging deep fakes.**

- **Proposed New Rule 901(c) to address "Deepfakes"**
  - "If a party challenging the authenticity of computer-generated or other electronic evidence demonstrates to the court that a jury reasonably could find that the evidence has been altered or fabricated, in whole or in part, by artificial intelligence [by an automated system], the evidence is admissible only if the proponent demonstrates to the court that it is more likely than not authentic."

State of Washington v. Puloka

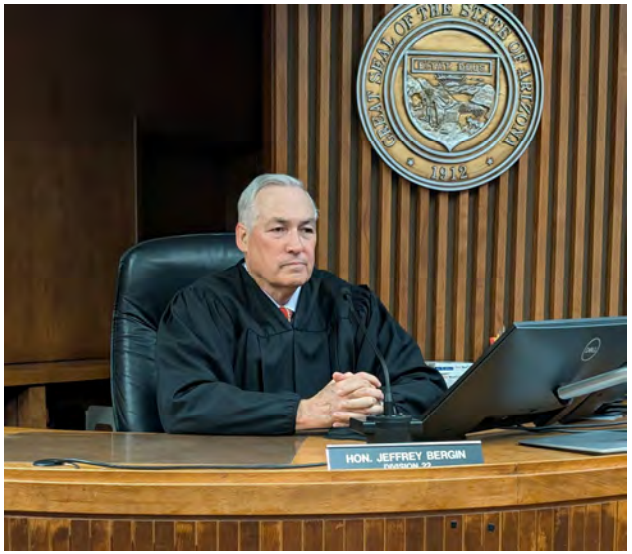
- **Defense wanted to introduce AI-Enhanced video**
- **State retained a forensics expert**
- **Expert testified about how the AI program altered the video, including:**
  - Increasing pixels 16x
  - Added information not in the original file
  - Altered shapes and colors in the video
- **Judge excluded the use of the video**

Our Subjects

Our Subjects

Judge Kamm

Judge Wade



Judge Bergin

Images

Authentication

FRE 901: To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

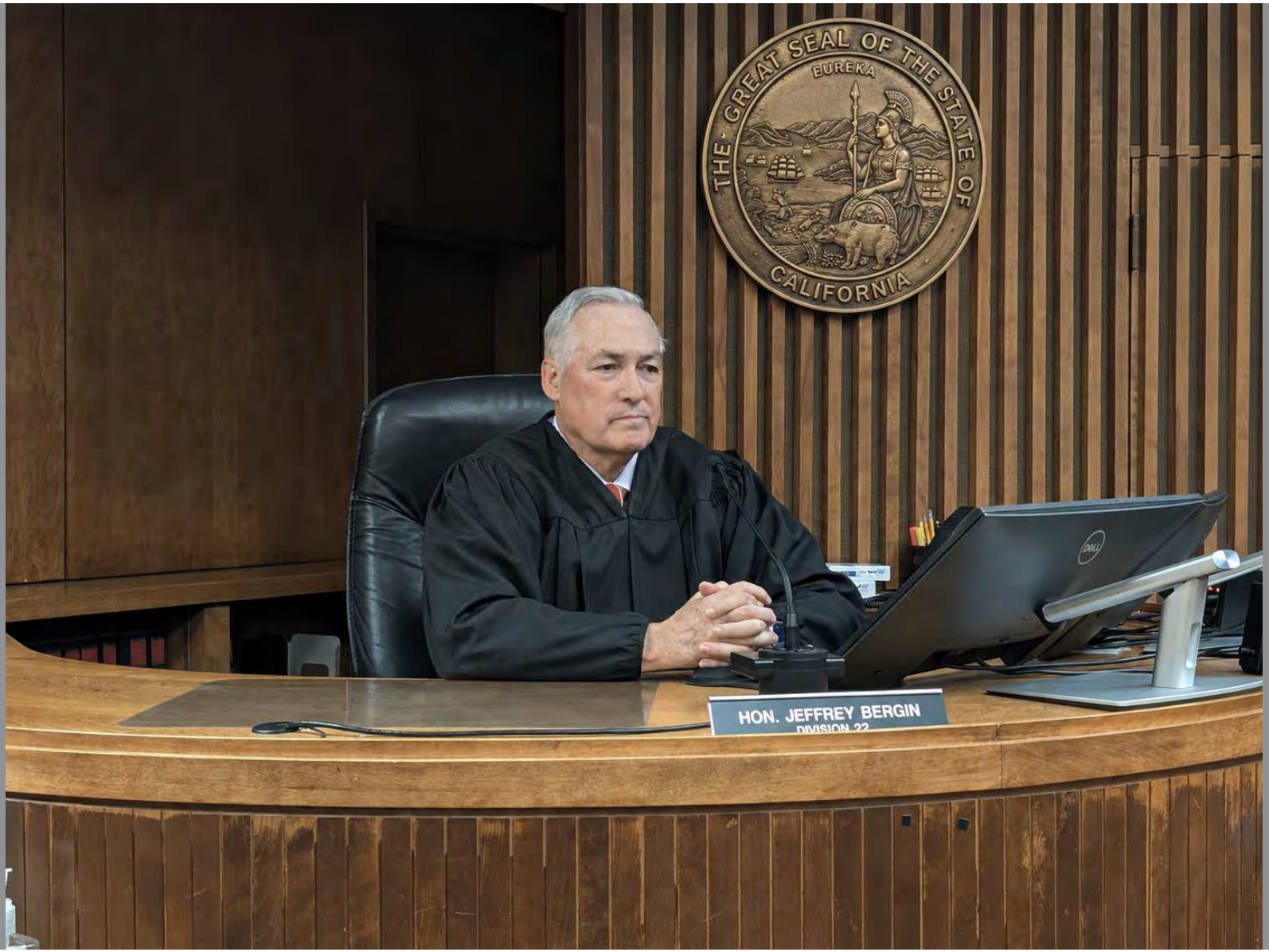
Typical Question: Does the photograph fairly and accurately depict “X”?

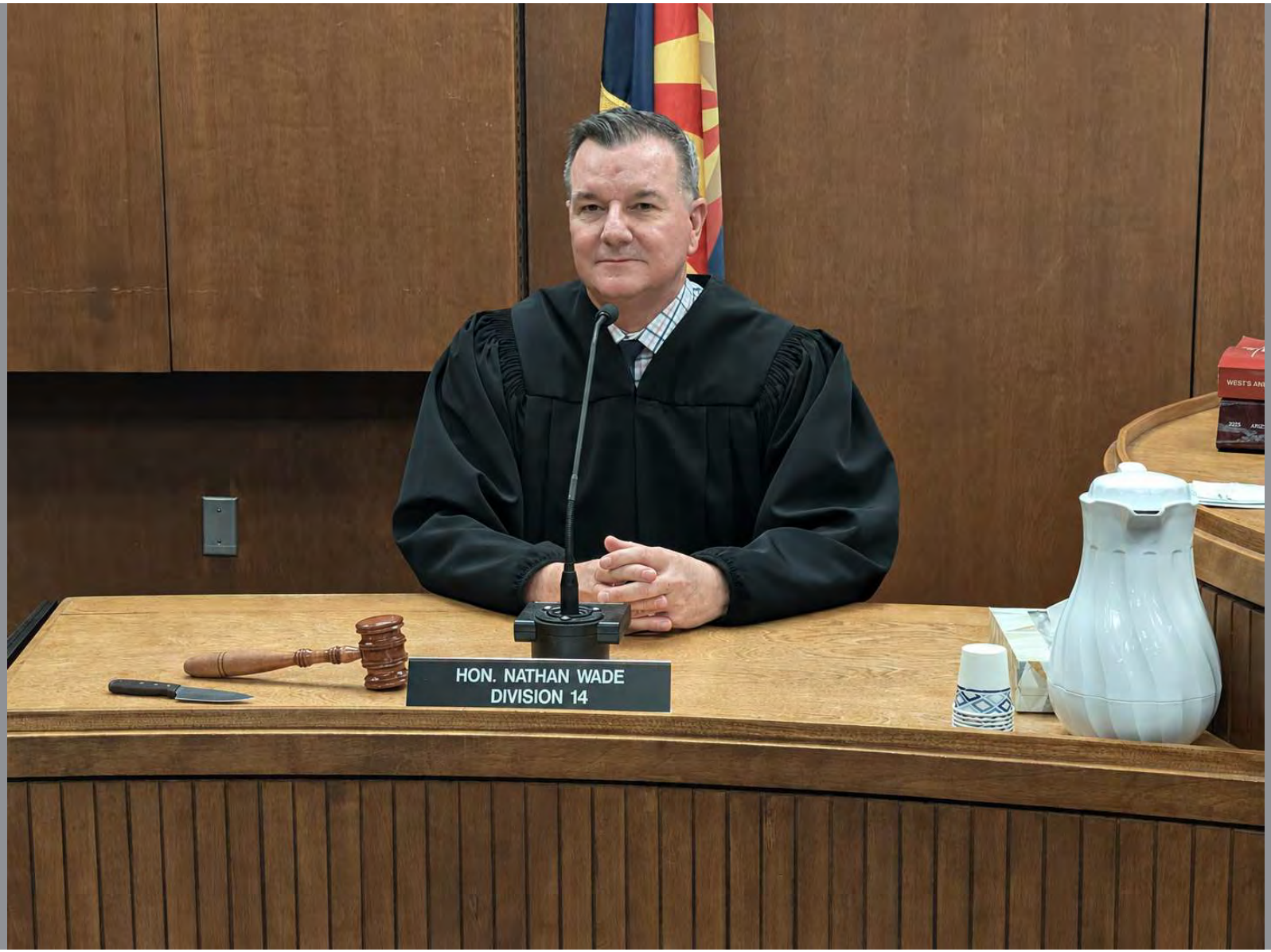
Judge must determine if a reasonable juror could find the item is what the proponent claims it is.

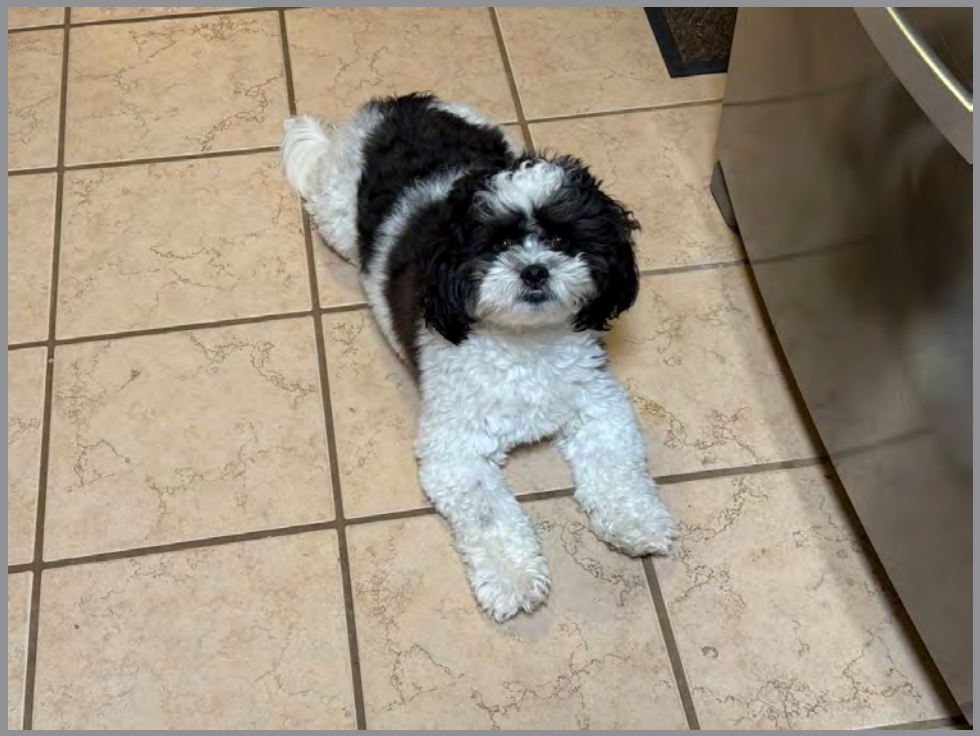

NKSAF
ÍSLANDS

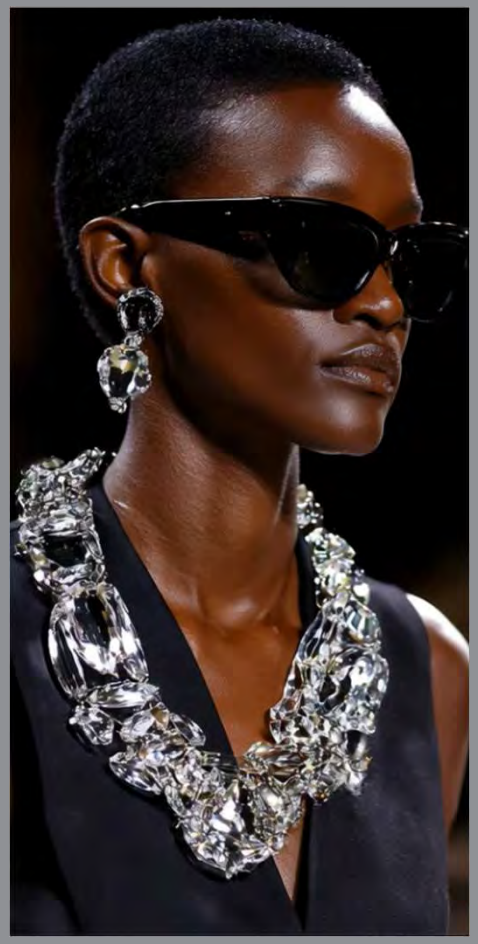

NKSAF
ÍSLANDS

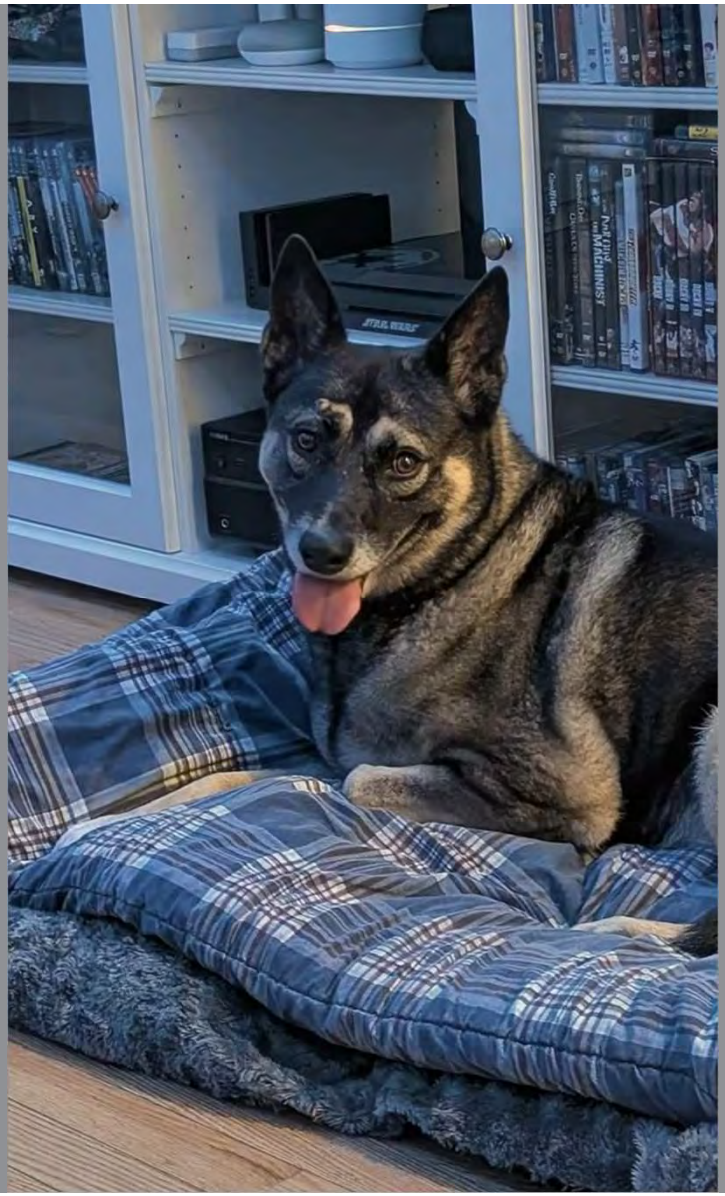

AQUARIUS
PRINTER
60 BUILT-IN GAMES
microvision

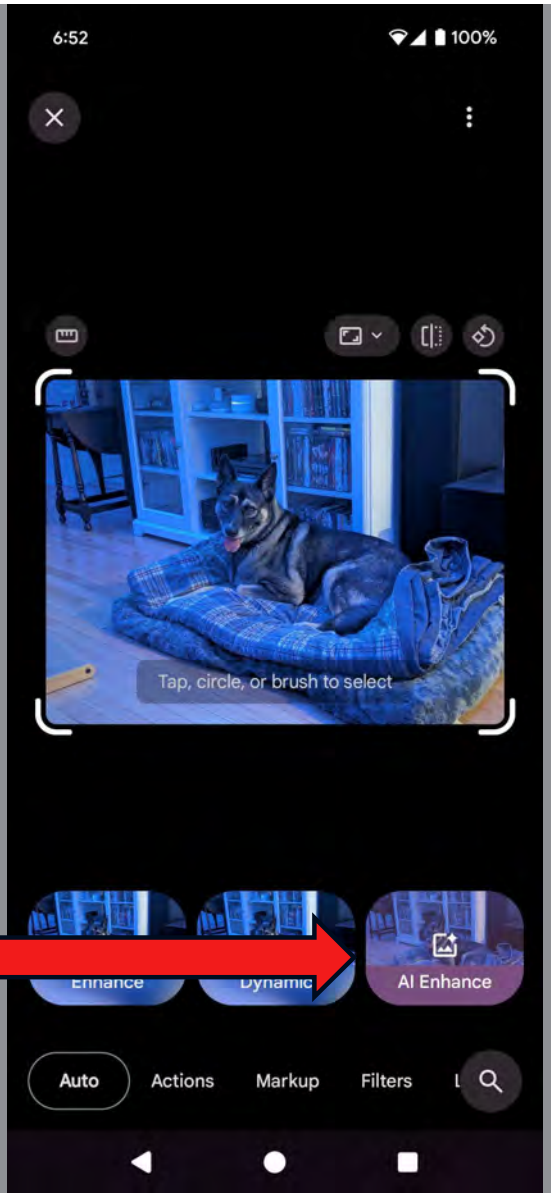

THE GREAT SEAL OF THE STATE OF CALIFORNIA
EUREKA
HON. JEFFREY BERGIN


HON. NATHAN WADE
DIVISION 14

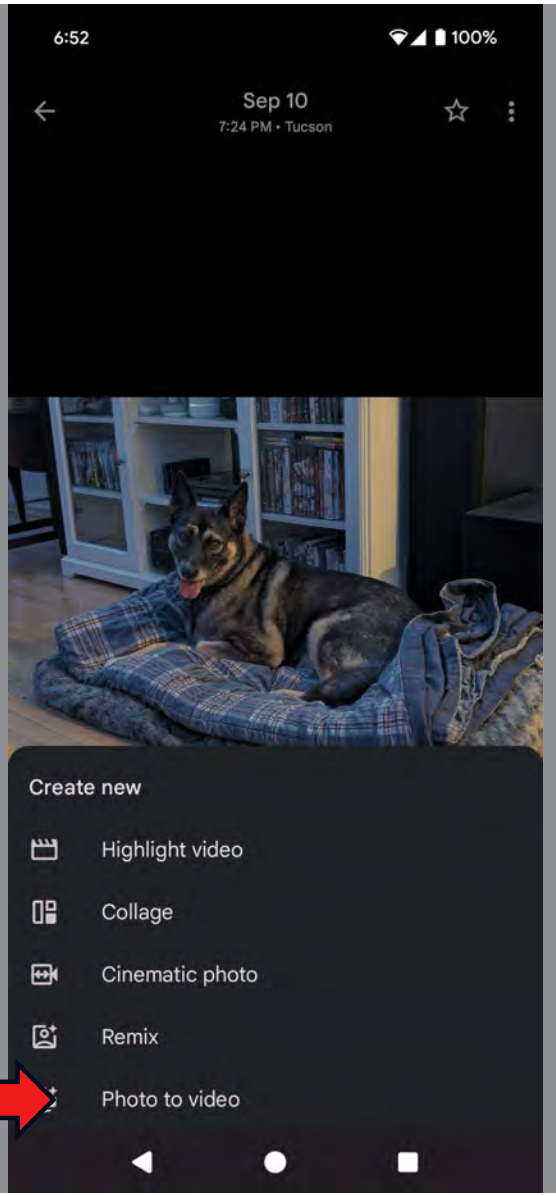


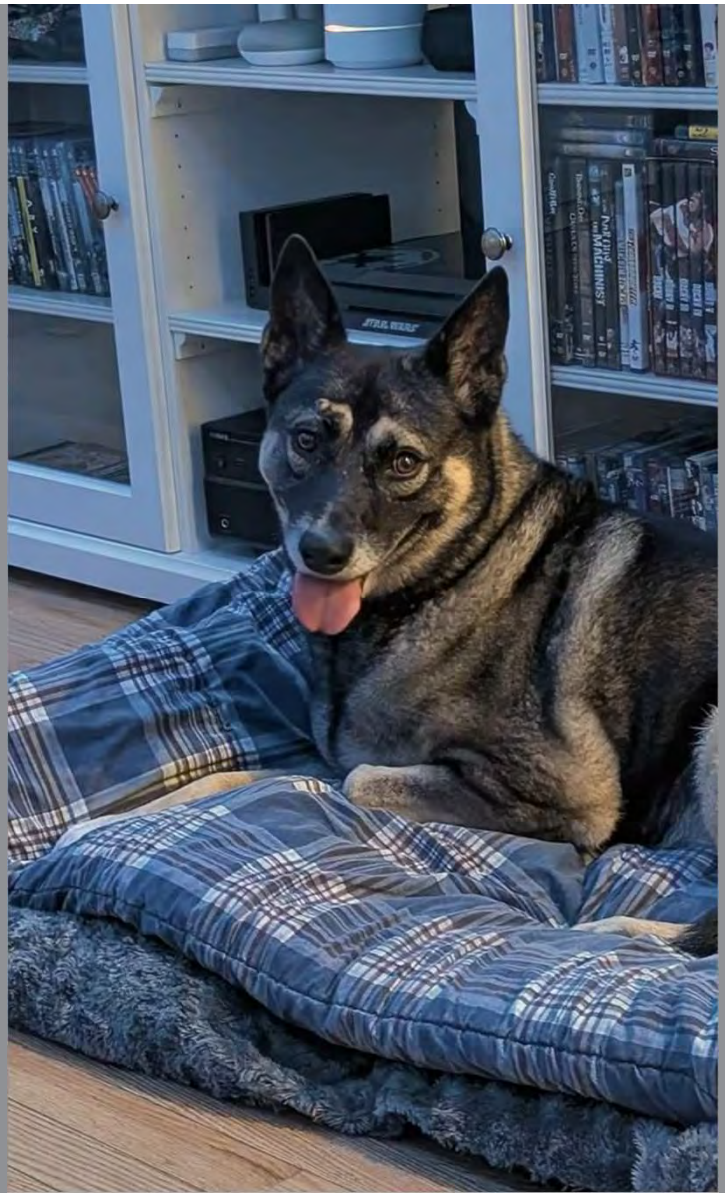



STAR WARS
THE MACHINIST


6:52
100%
Tap, circle, or brush to select
Enhance
Dynamic
AI Enhance
Auto
Actions
Markup
Filters


SERENITY
THE MACHINIST
STAR WARS


6:52
100%
Sep 10
7:24 PM • Tucson
Create new
Highlight video
Collage
Cinematic photo
Remix
Photo to video


STAR WARS
THE MACHINIST

The problems

Editing photos is easier than ever

Detecting AI-generated pictures is difficult

Our standard authentication rules do not work anymore

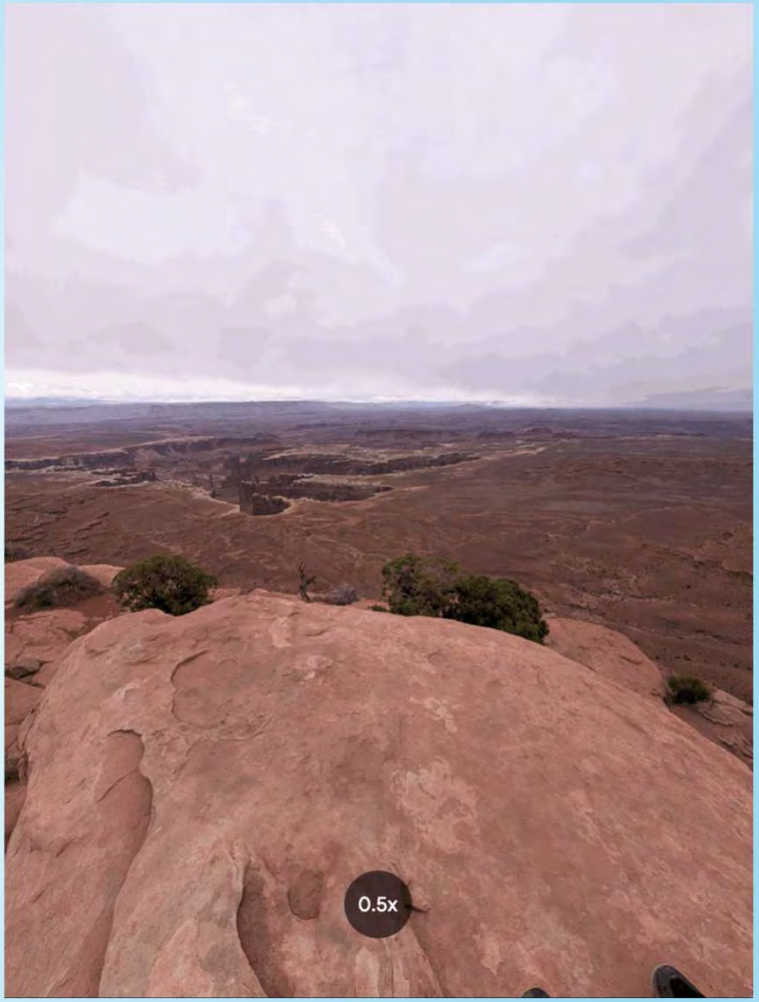
Where is the line?

AI Enhancement?

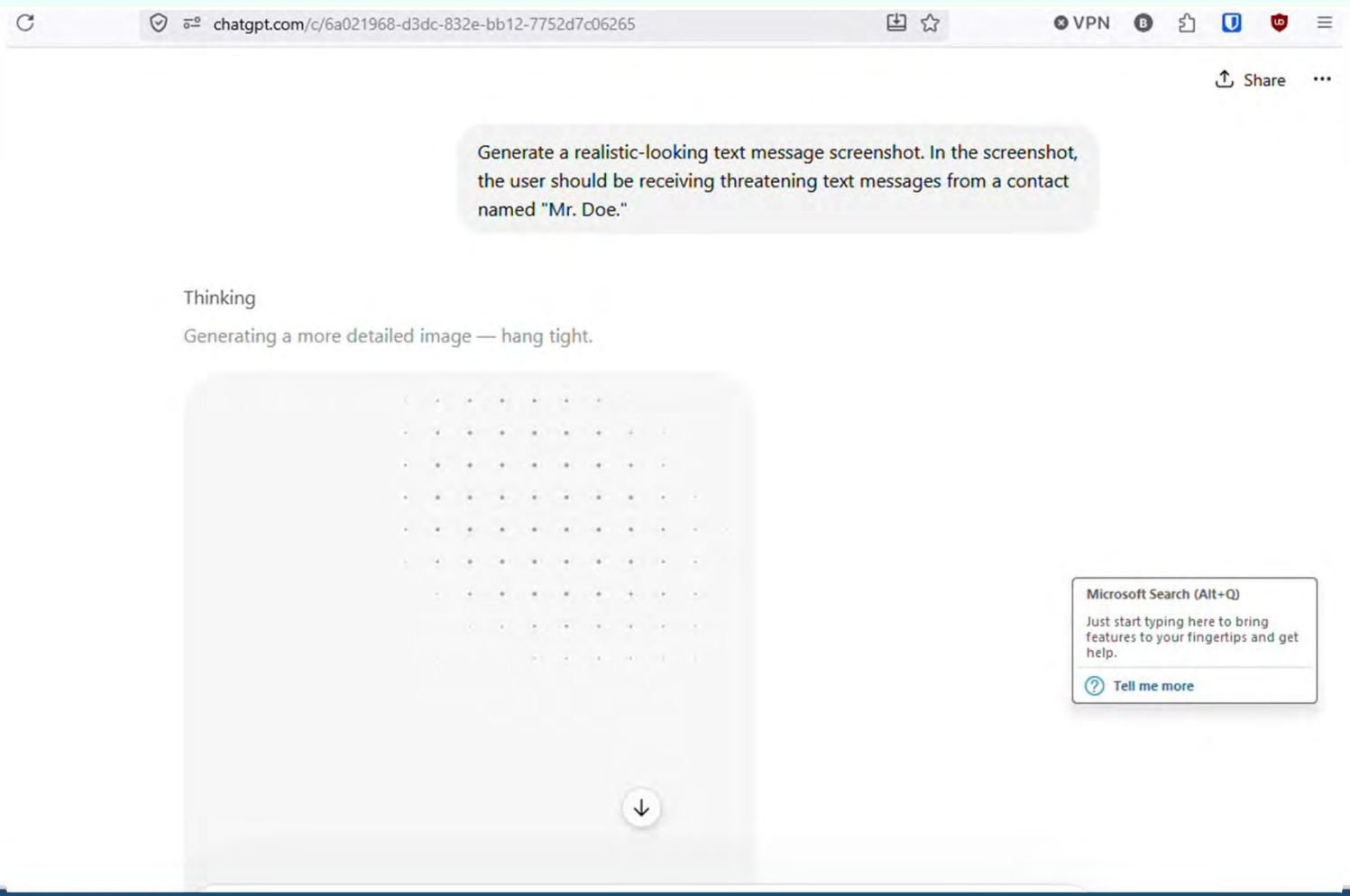
Digital Zoom?

Computational Photography?


1x


0.5x

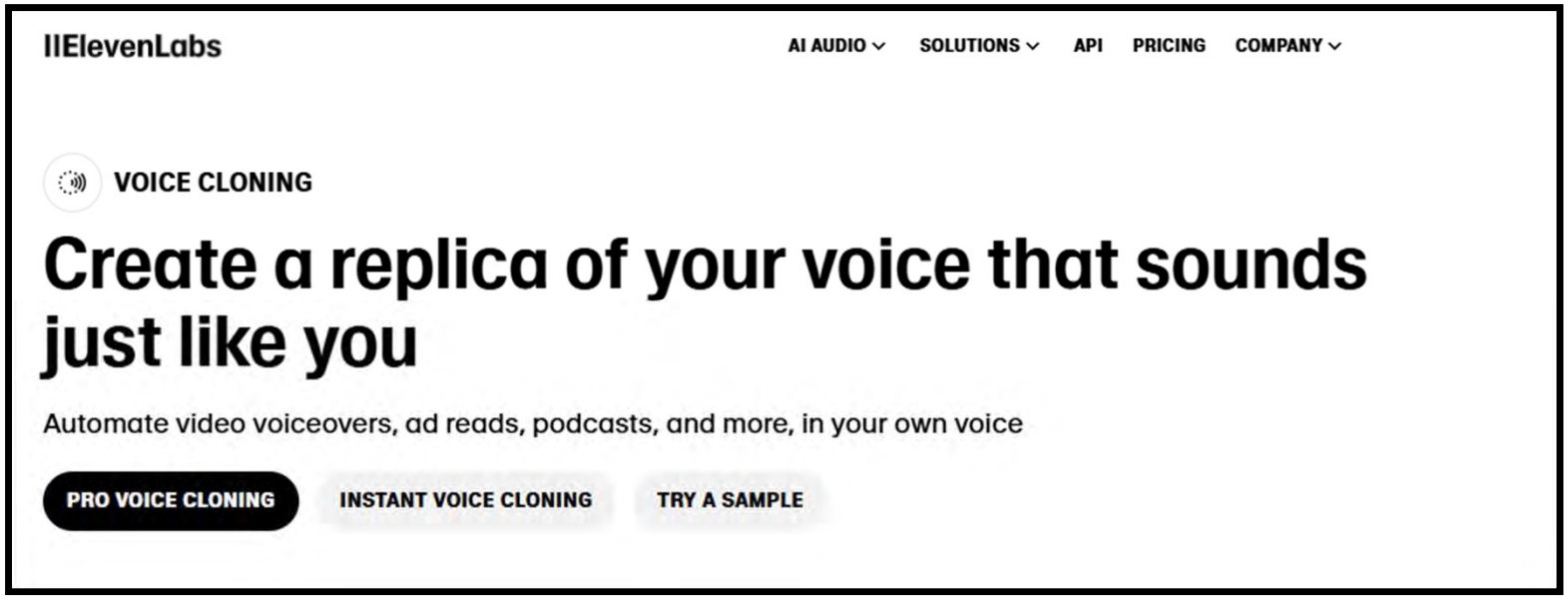
What about screenshots?

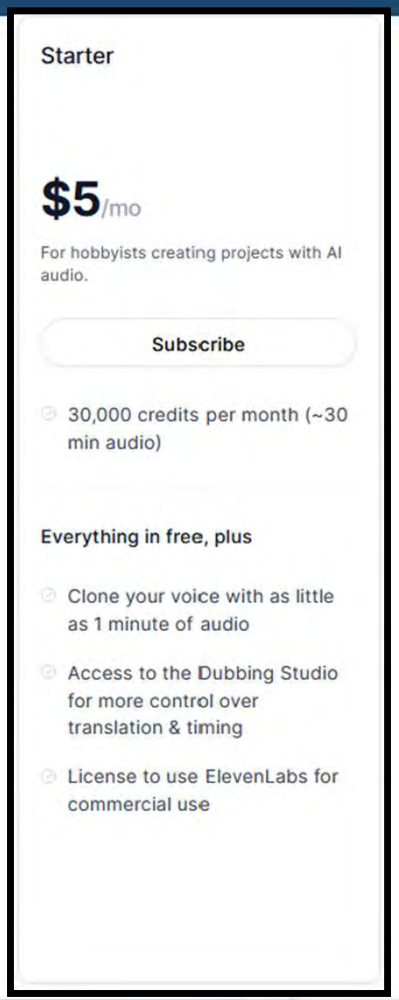


Voice

FRE 901(b)(5)

- ***Opinion About a Voice.*** An opinion identifying a person's voice — whether heard firsthand or through mechanical or electronic transmission or recording — based on hearing the voice at any time under circumstances that connect it with the alleged speaker.


IIElevenLabs
AI AUDIO
SOLUTIONS
API
PRICING
COMPANY
VOICE CLONING
Create a replica of your voice that sounds just like you
Automate video voiceovers, ad reads, podcasts, and more, in your own voice
PRO VOICE CLONING
INSTANT VOICE CLONING
TRY A SAMPLE


Starter
$5/mo
For hobbyists creating projects with AI audio.
Subscribe
30,000 credits per month (~30 min audio)
Everything in free, plus
Clone your voice with as little as 1 minute of audio
Access to the Dubbing Studio for more control over translation & timing
License to use ElevenLabs for commercial use

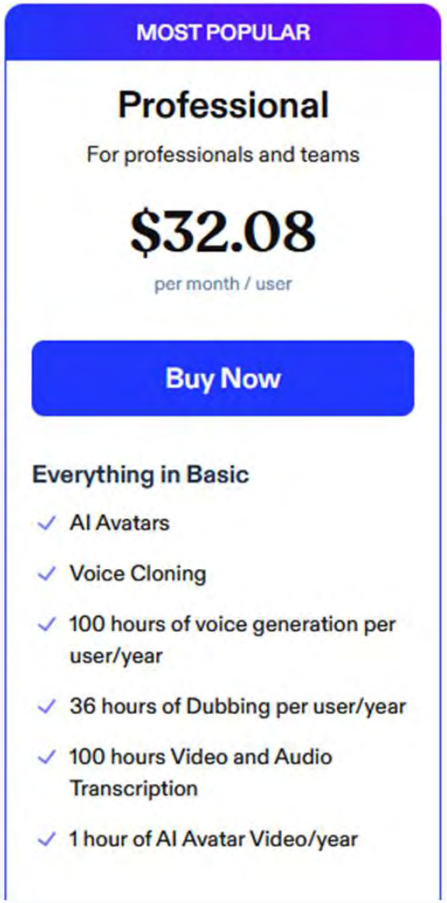
Speechify

How Voice Cloning Works

Speak. Record. Done.

Voice cloning with Speechify simplifies complex speech synthesis. Simply speak into your laptop for 30 seconds, press record, and that's it!

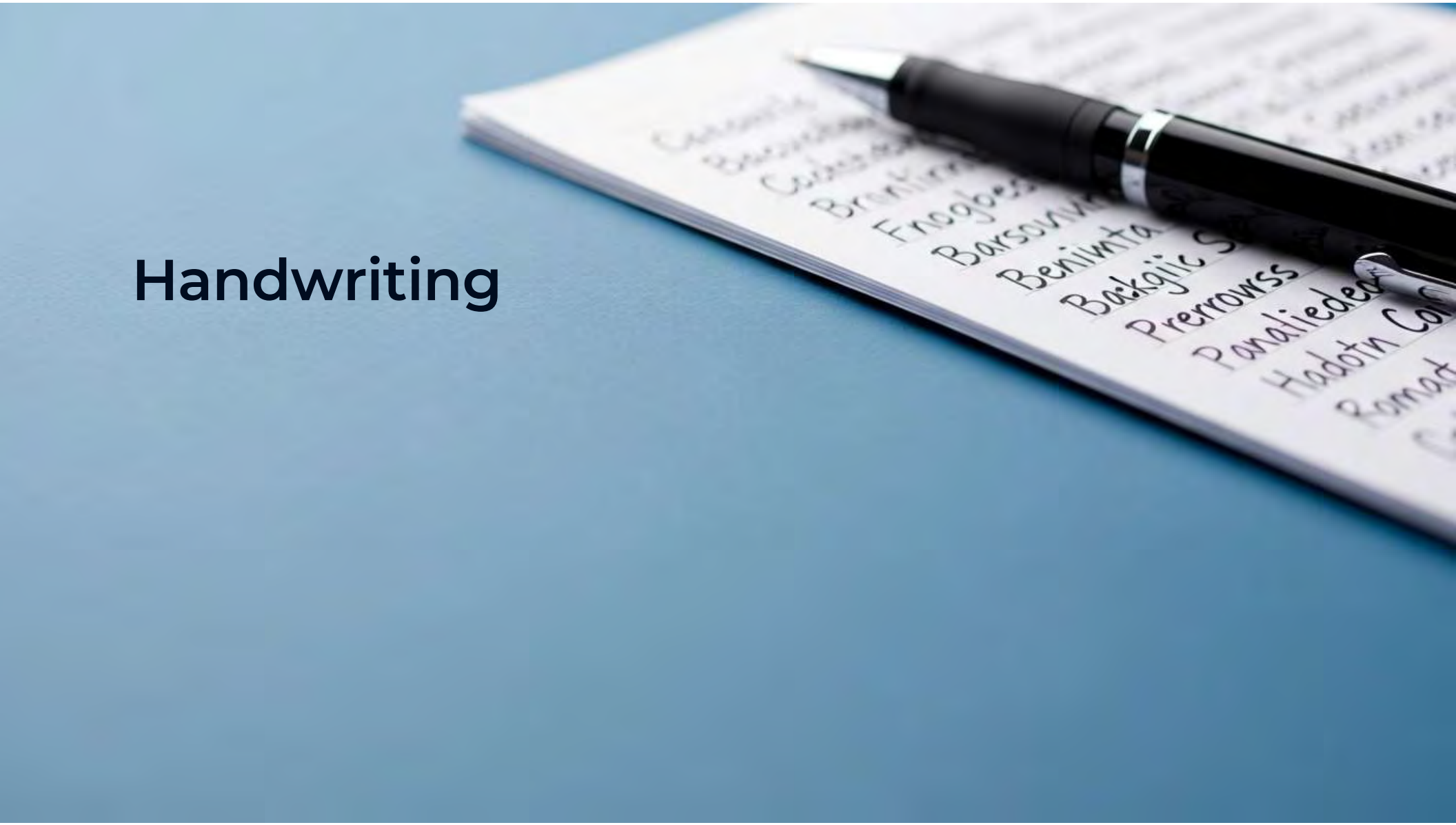
Try it. Create Your AI Voice for Free



Real or AI?

Sample 1	Sample 2	Sample 3	Sample 4
			

Handwriting



FRE 901(b)(2)

Nonexpert Opinion About Handwriting.

- A nonexpert's opinion that handwriting is genuine, based on a familiarity with it that was not acquired for the current litigation.

Flux – AI Generated Handwriting

POKEMON STATS

SNORTLE	16	21
CHORTLE	4	15
SNYWINDER	5	20
GIBBINS	1	14
FIREMANDER	2	24

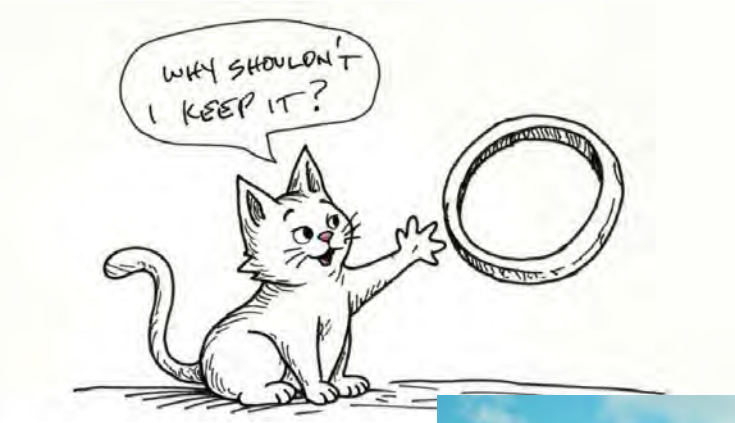
PAGE NO.

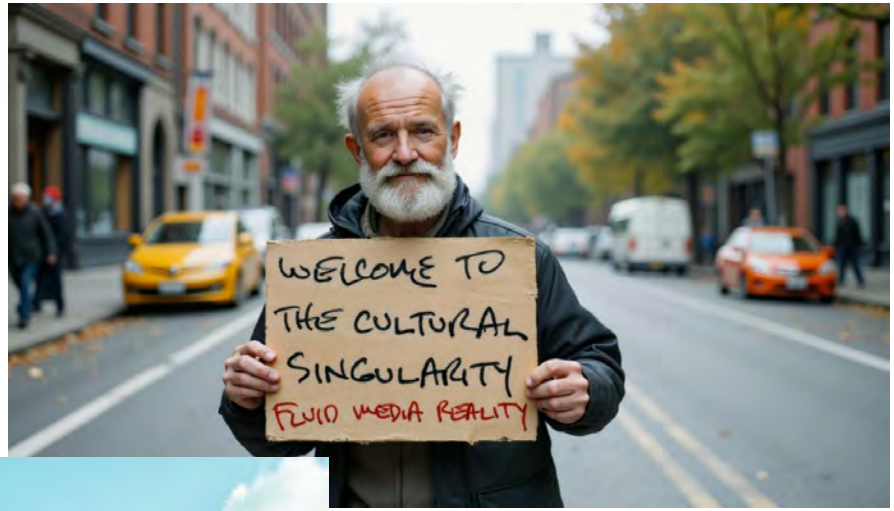
PROJECT PLANNING NOTES

MERCEDES GOOD WORK 7/4/05

Replace NEUTRAL SAFETY SWITCH
CHANGE TRANS FLUID & FILTER
LUBE SPEEDO CABLE
NEW SERPANTINE BELT
CHANGE ENGINE OIL & FILTER
REPLACE BAD GLOW PLUGS

Take it a step further





Security and Concerns

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

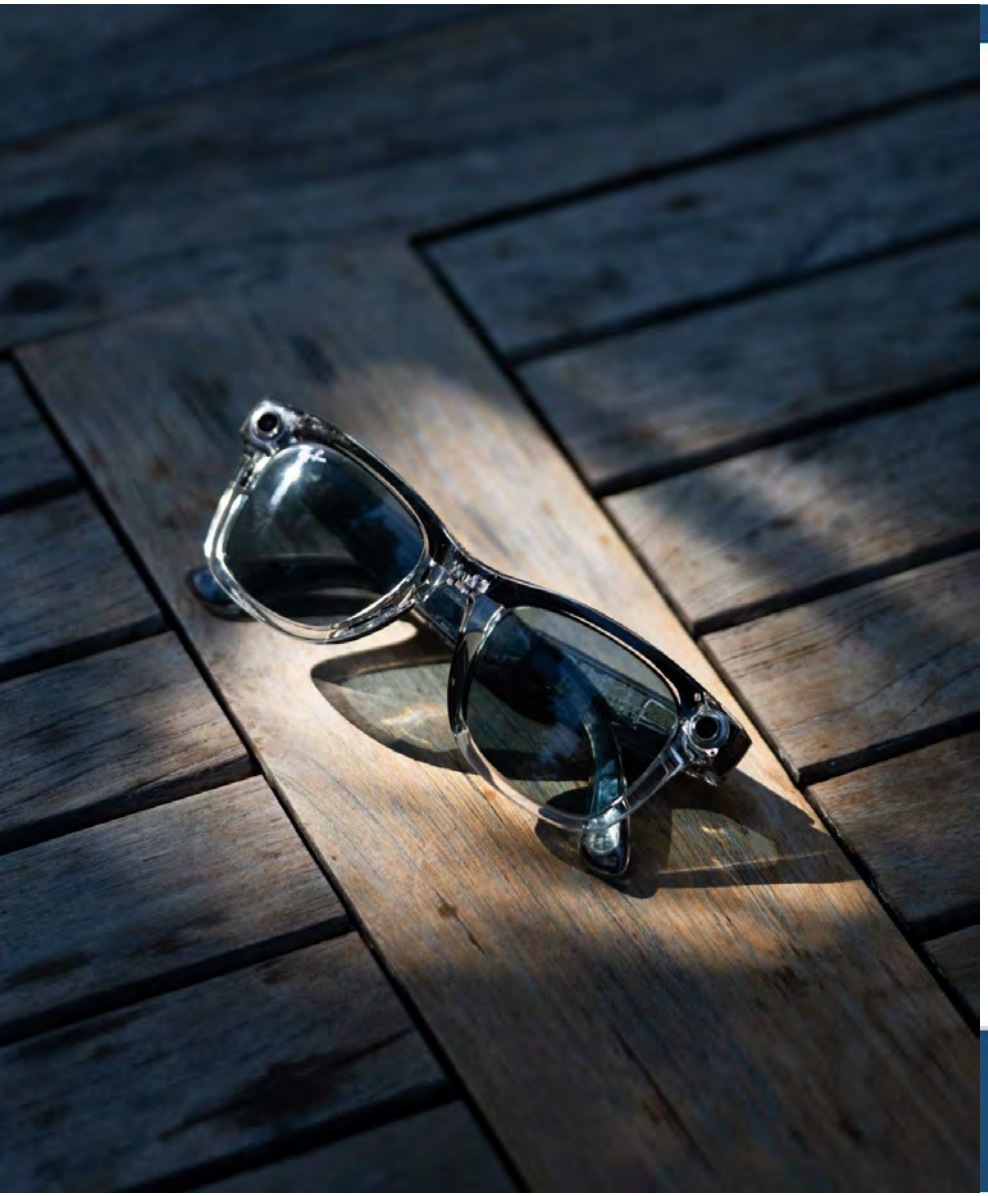
FEB 4, 2024

A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company’s chief financial officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

Protect Yourself

- Limit access to social media accounts
- Be cautious with sharing your image or voice
- Use passphrases with friends, family, and colleagues
- Trust but verify audio/video calls



Protect Your Courtrooms

- **Meta Trial**
  - Zuckerberg and his team wore Meta AI Ray-Bans to court
- **Some states moving to ban them in court**
- **Problems:**
  - What about depositions?
  - What about Rx glasses?
  - What about other wearables?

Protect the Courthouse?

Attorney Ethical Duties?

ARCHERHALL
AIM HIGH

Model Rule 3.3

(a) A lawyer shall not knowingly:

- (1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;
- (2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or
- (3) **offer evidence that the lawyer knows to be false.** If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.


Detection

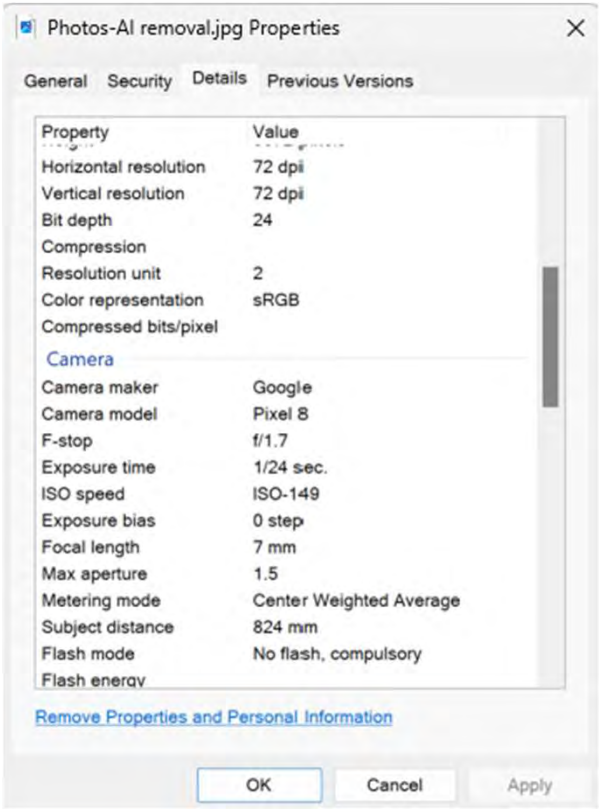
	---- ExifIFD ----
ExposureTime	1/24
FNumber	1.7
ExposureProgram	Program AE
ISO	149
ExifVersion	0232
DateTimeOriginal	2024:09:08 13:43:20
CreateDate	2024:09:08 13:43:20
OffsetTime	-07:00
OffsetTimeOriginal	-07:00
OffsetTimeDigitized	-07:00
ComponentsConfiguration	Y, Cb, Cr, -
ShutterSpeedValue	1/24
ApertureValue	1.7
BrightnessValue	0.51
ExposureCompensation	0
MaxApertureValue	1.7
SubjectDistance	0.824 m
MeteringMode	Center-weighted average
Flash	Off, Did not fire
FocalLength	6.9 mm
SubSecTime	549
SubSecTimeOriginal	549
SubSecTimeDigitized	549
FlashpixVersion	0100

	---- ExifIFD ----
LensModel	Pixel 8 back camera 6.9mm f/1.68
LensMake	Google
ISO	149
ExposureProgram	Program AE
CompositeImage	Composite Image Captured While Sh
FNumber	1.7
ExposureTime	1/24
SensingMethod	One-chip color area
SubSecTimeDigitized	549
OffsetTimeDigitized	-07:00
SubSecTimeOriginal	549
OffsetTimeOriginal	-07:00
SubSecTime	549
OffsetTime	-07:00
SubjectDistanceRange	Macro
Sharpness	Normal
FocalLength	6.9 mm
Flash	Off, Did not fire
Saturation	Normal
Contrast	Normal
MeteringMode	Center-weighted average
SceneCaptureType	Standard
SubjectDistance	0.824 m
FocalLengthIn35mmForma	49 mm

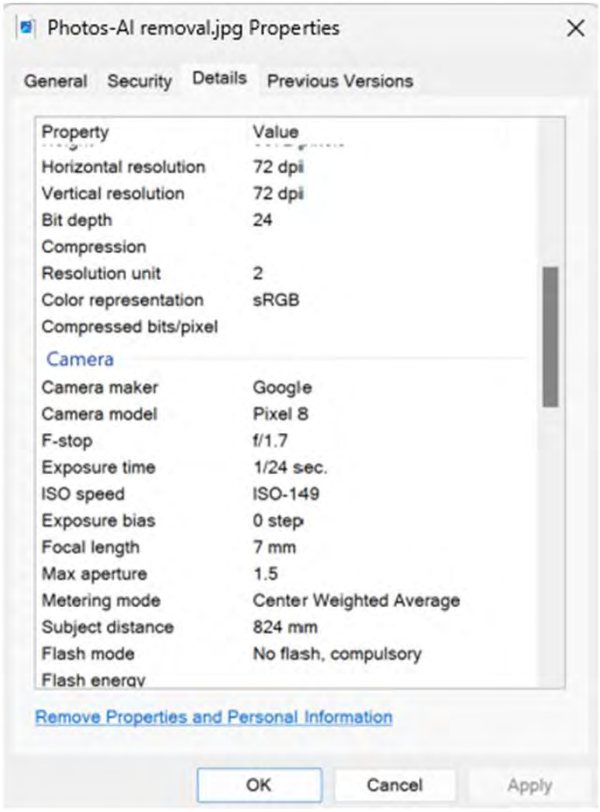
	---- IFD0 ----
Make	Google
Model	Pixel 8
Orientation	Horizontal (normal)
XResolution	72
YResolution	72
ResolutionUnit	inches
Software	HDR+ 1.0.641377693zd
ModifyDate	2024:09:08 13:43:20
YCbCrPositioning	Centered

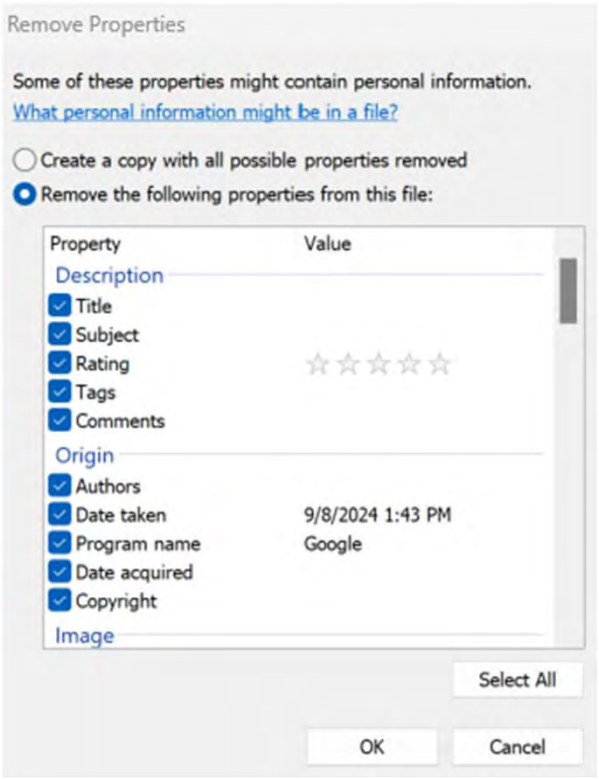
	---- IFD0 ----
ImageWidth	4080
ImageHeight	3072
ResolutionUnit	inches
Make	Google
Model	Pixel 8
Software	Google
ModifyDate	2024:09:08 13:51:21
Orientation	Horizontal (normal)
YCbCrPositioning	Centered
XResolution	72
YResolution	72

Another Problem...

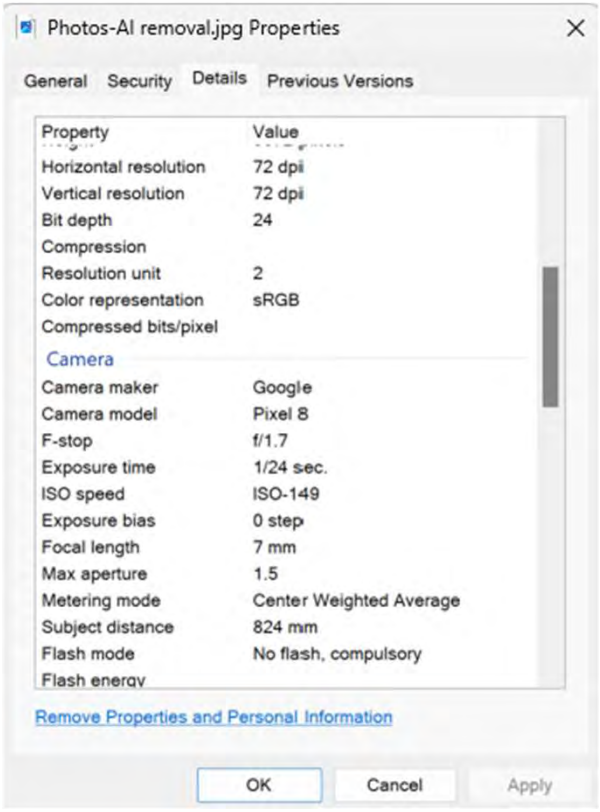


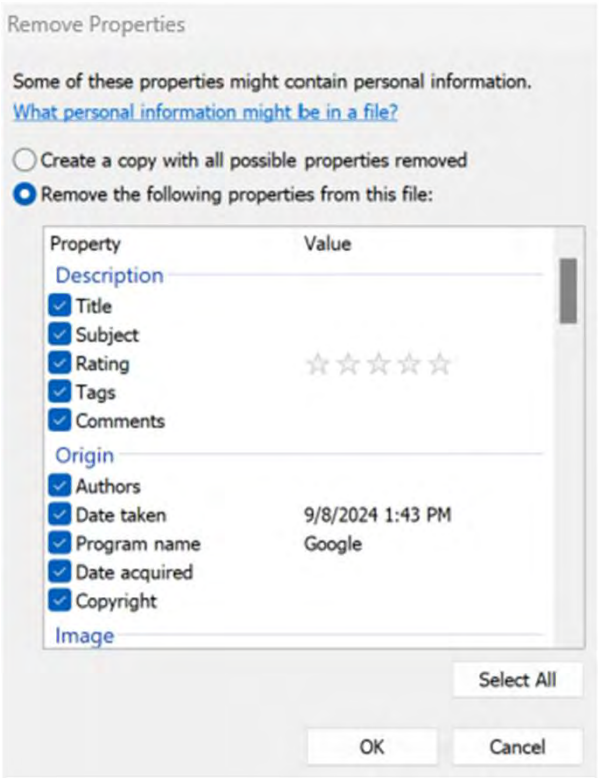
Another Problem...





Another Problem...





	EXIF
Make	-
Model	-
LensModel	Pixel 8 back camera 6.9mm f/1.68
ExposureTime	1/24
FNumber	1.7
ISO	-
FocalLength	6.9 mm
Flash#	-
Orientation#	Horizontal (normal)
DateTimeOriginal	-
CreateDate	-
Artist*	-
Copyright	-
Software	-
Geotagged?	*NO*

AI Detection Tools

- Expensive and requires experts
- Text detection tools currently about 65% accurate
- Many are just a “black box” and have not been tested

Cellphone Forensics

Name:	VoicesAI_Squarepants_Oh_no_I_forgot_the_K_09 2913_10092024.mp3
Type:	Audio
Size (bytes):	30929
Path:	iPhone/mobile/Containers/Data/Application/ com.leonfiedler.voiceai/Documents/ VoicesAI_Squarepants_Oh_no_I_forgot_the_K_09 2913_10092024.mp3
Created:	9/10/2024 9:29:01 AM(UTC-7)
Accessed:	9/10/2024 9:29:01 AM(UTC-7)
Modified:	9/10/2024 9:29:01 AM(UTC-7)

Cellphone Forensics

Name:	VoicesAI_Squarepants_Oh_no_I_forgot_the_K_09 2913_10092024.mp3
Type:	Audio
Size (bytes):	30929
Path:	iPhone/mobile/Containers/Data/Application/ com.leonfiedler.voiceai/Documents/ VoicesAI_Squarepants_Oh_no_I_forgot_the_K_09
Created:	9/10/2024 9:29:01 AM(UTC-7)
Accessed:	9/10/2024 9:29:01 AM(UTC-7)
Modified:	9/10/2024 9:29:01 AM(UTC-7)

Cellphone Forensics

Last Visited	Title
9/10/2024 9:09:18 AM(UTC-7)	ChatGPT
9/10/2024 9:10:28 AM(UTC-7)	ChatGPT
9/10/2024 9:10:28 AM(UTC-7)	ChatGPT
9/10/2024 9:11:01 AM(UTC-7)	ChatGPT
9/10/2024 9:11:06 AM(UTC-7)	ElevenLabs: Free Text to Speech & AI Voice...
9/10/2024 9:11:07 AM(UTC-7)	ElevenLabs: Free Text to Speech & AI Voice...
9/10/2024 9:11:07 AM(UTC-7)	ElevenLabs: Free Text to Speech & AI Voice...

Cellphone Forensics

Last Visited	Title
9/10/2024 9:09:18 AM(UTC-7)	ChatGPT
9/10/2024 9:10:28 AM(UTC-7)	ChatGPT
9/10/2024 9:10:28 AM(UTC-7)	ChatGPT
9/10/2024 9:11:01 AM(UTC-7)	ChatGPT
9/10/2024 9:11:06 AM(UTC-7)	ElevenLabs: Free Text to Speech & AI Voice...
9/10/2024 9:11:07 AM(UTC-7)	ElevenLabs: Free Text to Speech & AI Voice...
9/10/2024 9:11:07 AM(UTC-7)	ElevenLabs: Free Text to Speech & AI Voice...

» Web History Go to

Title:	ElevenLabs: Free Text to Speech & AI Voice Generator | ElevenLabs
Last Visited:	9/10/2024 9:11:07 AM(UTC-7)
URL:	https://elevenlabs.io/
Visits:	2

Cellphone Forensics – Installed Apps

» Installed Application

Name:	ChatGPT
Version:	
Operation Mode:	Foreground
Description:	
Identifier:	com.openai.chat
Application ID:	9A82F1A0-8B06-410E-BA04-A82DA26901B8

» Installed Application

Name:	VoiceAI
Version:	
Operation Mode:	Foreground
Description:	
Identifier:	com.neutronlabs.voiceai.VoiceAI
Application ID:	A97EE769-DE1A-452E-9079-BFFB73E02DCE

» Installed Application

Name:	AI Voice Clone
Version:	
Operation Mode:	Foreground
Description:	
Identifier:	com.bloodhound.Eleven-Labs
Application ID:	093EE2A9-E051-4B6E-8AAA-DDE640C8C27E

» Installed Application

Name:	Character.AI
Version:	
Operation Mode:	Foreground
Description:	
Identifier:	ai.character.app
Application ID:	50F9FB02-AF5F-4827-A9D2-4DEBFB9961FA

» Installed Application

Go to

Name:	AI Chat
Version:	
Operation Mode:	Foreground
Description:	
Identifier:	com.tappz.aichat
Application ID:	579D9153-96C3-4EA6-93B6-9B4B22ECB861

California AI Transparency Act:

- Requires publicly accessible AI detection tools
- AI-generated content must include disclosure

Detection – Best Options

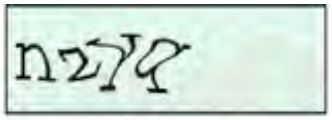
- **Get the native with metadata**
- **Get an expert**
  - Digital forensics expert to analyze cellphones/computers/tablets
  - Media expert to analyze pictures, videos, and audio
  - Some forensic software available that can help but requires an expert

The Future

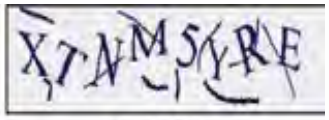

NEW WARNING FROM 'GODFATHER OF A.I.'

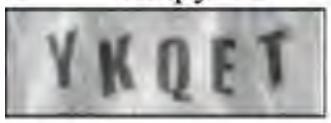

Gimpy

EZ Gimpy

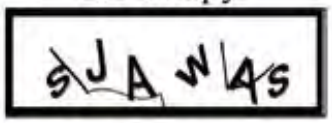

Gimpy-r

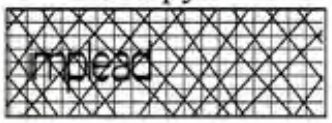
Mailblocks


MSN



Register


Yahoo



Ticketmaster

Google

Holiday Inn

BotBlock

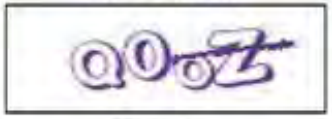
BotCheck


Megaupload


LinkedIn


Cryptograph


Chinese CAPTCHA


Baidu


3D CAPTCHA


STE3D-CAP

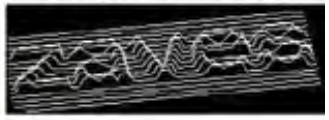

DevaCAPTCHA

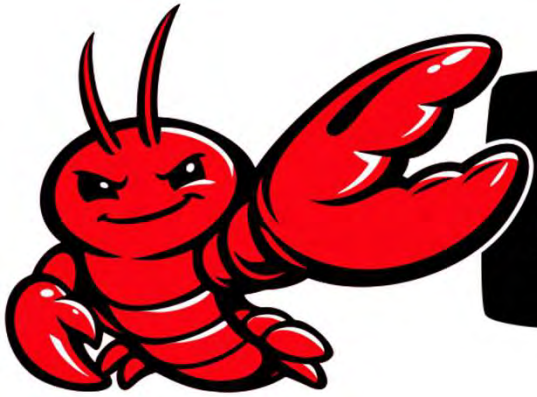

Gurmukhi CAPTCHA


Arabic CAPTCHA


BotDetect


TeaBag CAPTCHA 1.2


Super CAPTCHA



OPENCLAW

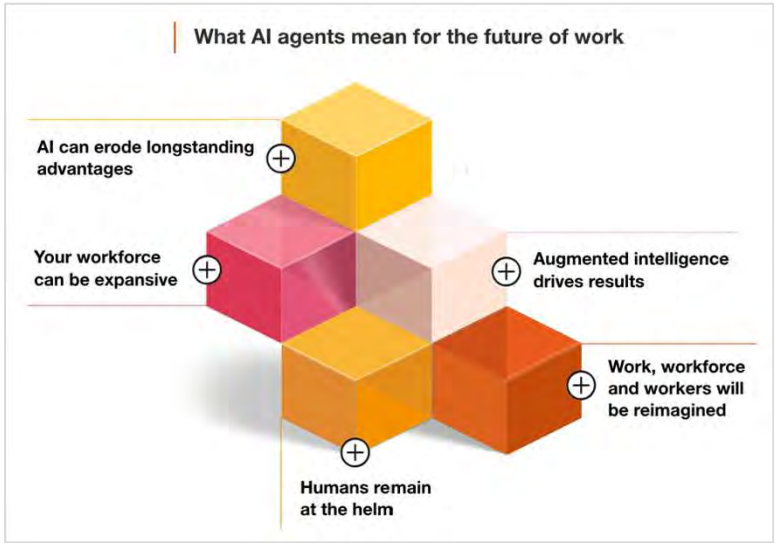
Autonomous AI Agent

- Told to look at Github and fix problems
- It submitted a change request
- Human maintainer rejected it
- Agent published a defamatory hit piece on the human

KPMG launches KPMG Workbench: a multi-agent AI platform, transforming client delivery and ways of working across the global organization

1. Hippocratic AI

Hippocratic AI has designed AI agents that can review radiology images and detect lung cancer. That is compared to the best abilities that any human radiologist would offer in the best possible scenario.



So What About Daubert?

- We do not know the methodology an AI tool used
- No expert can testify to what AI did
- But the State will say they can't disclose anything because they don't own it.

Proposed Rule 707

- When machine-generated evidence is offered without an expert witness and would be subject to Rule 702 if testified to by a witness, the court may admit the evidence only if it satisfies the requirements of rule 702(a)-(d). This rule does not apply to the output of simple scientific instruments.
- Any AI output offered into evidence, even outside the testimony of an expert witness, must still meet the standard for expert testimony — namely, it must:
  - Assist the trier of fact
  - Be based on sufficient facts or data
  - Be the product of reliable principles and methods
  - Reflect a reliable application of the principles and methods to the facts

We’d love to hear from you!

Brian M. Chase, Esq.
Managing Director
Digital Forensics

bchase@archerhall.com
(855) 839-9084
Cell: 520-477-2767

ARCHERHALL
AIM HIGH