

TechCheck slide

- Live-Demonstrations Running?
- Audio Sharing activated? *
- Microphone checked?
- Camera checked?
- Light Conditions checked?

* essential for virtual conferences

Pushing Deepfakes to the Limit

Fake Video Calls with AI

TNG  TECHNOLOGY
CONSULTING





When a new technology like this comes along, the most dangerous period is when the technology is out there but the public isn't aware of it. That's when it can be used most effectively.



Carl Bergstrom
University of Washington

Speakers



Thomas Endres

Partner

Oracle® JavaOne Rockstar
Intel® Black Belt Software Developer
Intel® Software Innovator
Intel® Top Innovator 2014 - 2019



Martin Förtsch

Principal Consultant

Oracle® JavaOne Rockstar
Intel® Black Belt Software Developer
Intel® Software Innovator
Intel® Top Innovator 2014 - 2019



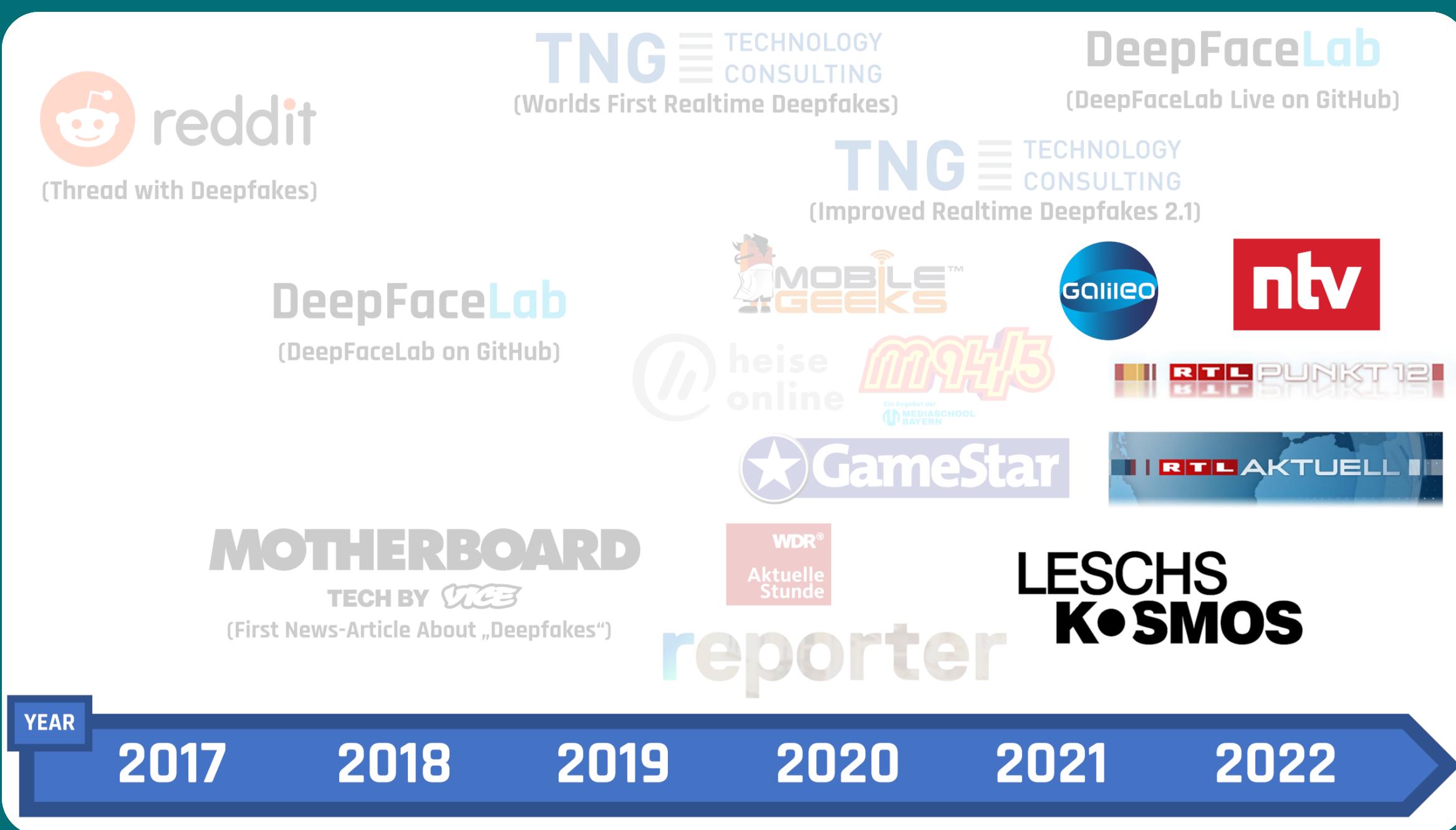
Jonas Mayer

Senior Consultant

Bedroom DJ
Teakwondo Black Belt
GameStar Certified Hacker
Intel® Software Innovator

Our Story

The Evolution of Deepfakes



Evolution of Deepfakes

First Deepfake Videos Were Published on Reddit in Autumn 2017



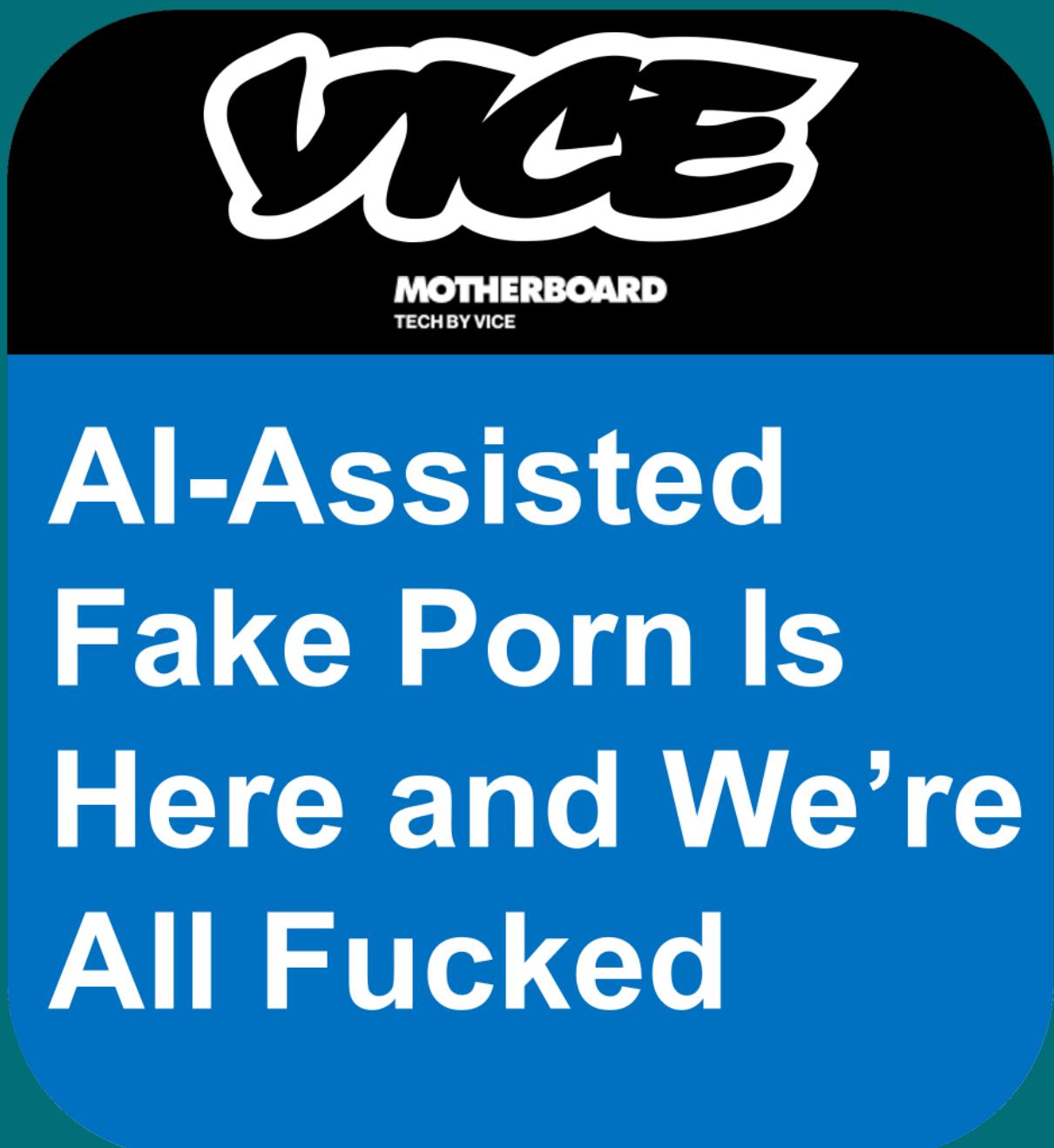
Evolution of Deepfakes

First Deepfake Videos Were Used for NSFW-Videos

Deep **Fakes**

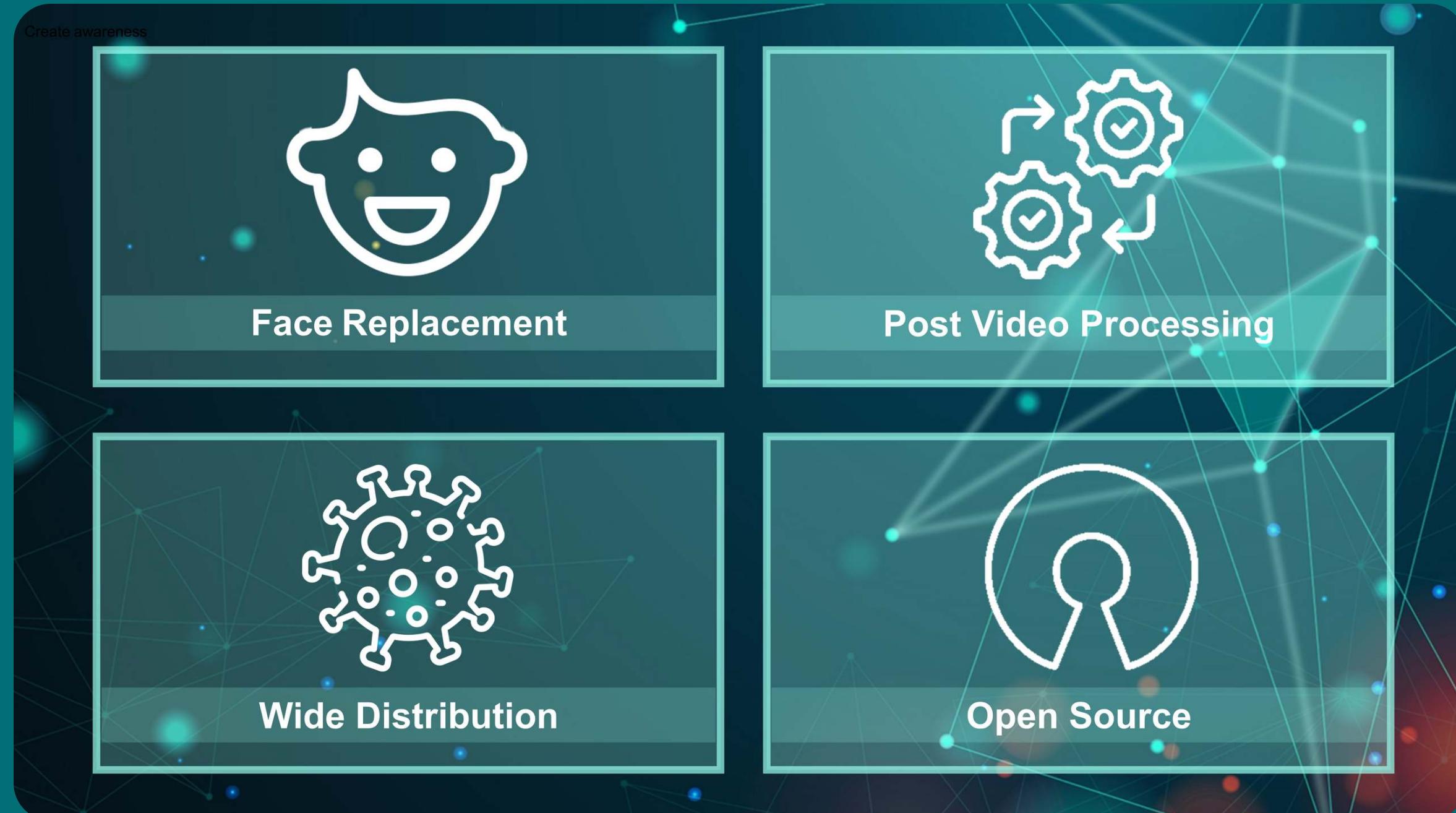
Evolution of Deepfakes

First News Article on Deepfakes at VICE Motherboard in Spring 2018



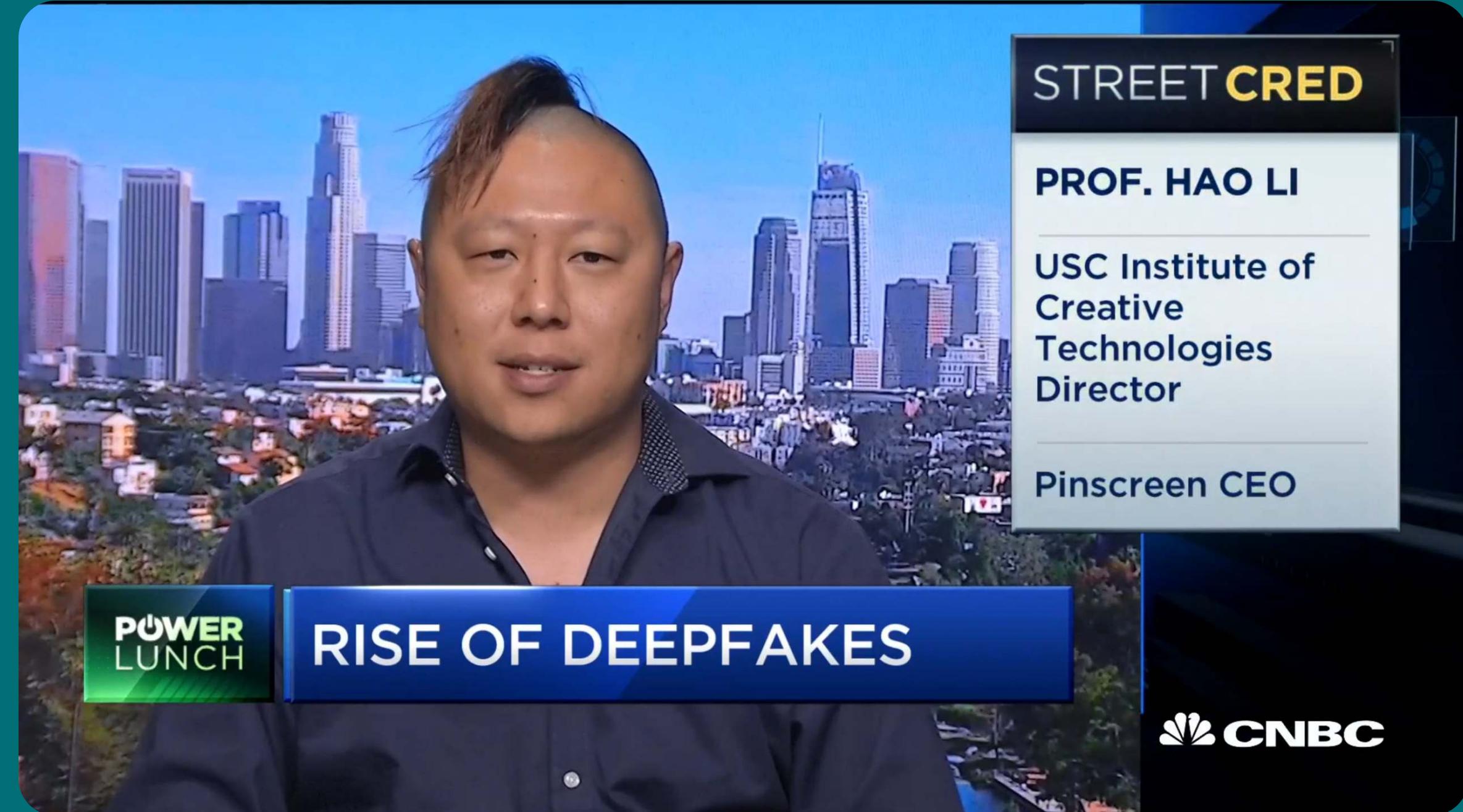
Evolution of Deepfakes

DeepFaceLab Published on GitHub (2018)



Evolution of Deepfakes

"Perfectly Real" Deepfakes Will Arrive in 6 Months to a Year (2019)



Realtime Deepfakes

The Motivation behind Deepfakes 2.0 (2019)



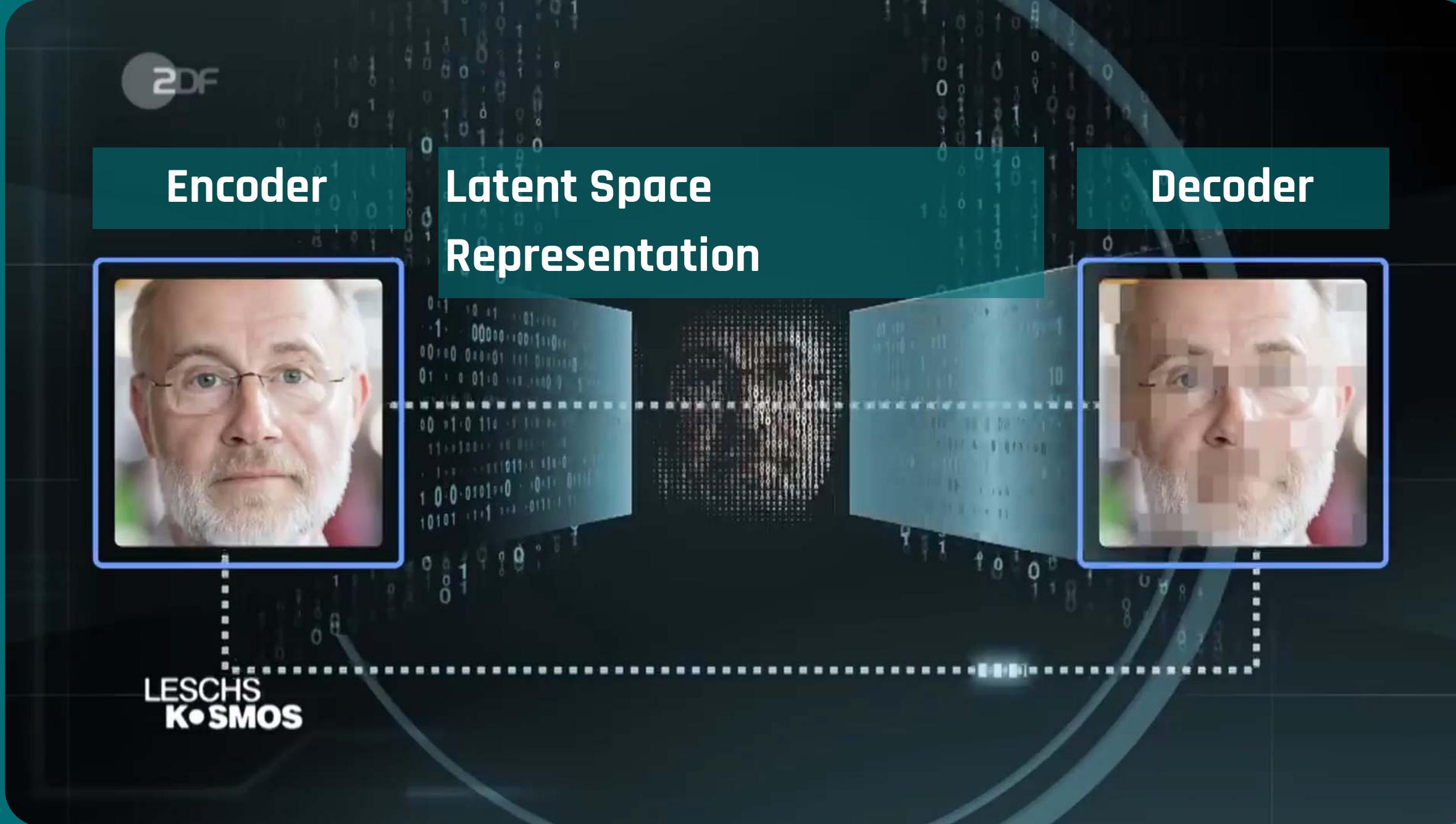
Agenda

- ▶ Deepfakes in a Nutshell
- ▶ Realtime Deepfakes
- ▶ Pushing Deepfakes to the Limit
- ▶ Videocalls with Deepfakes
- ▶ Conclusion



Deepfakes in a Nutshell

Training Encoder and Decoder on Harald Lesch



Deepfakes in a Nutshell

Loss Function Helps to Improve Generated Decoder Results

Encoder

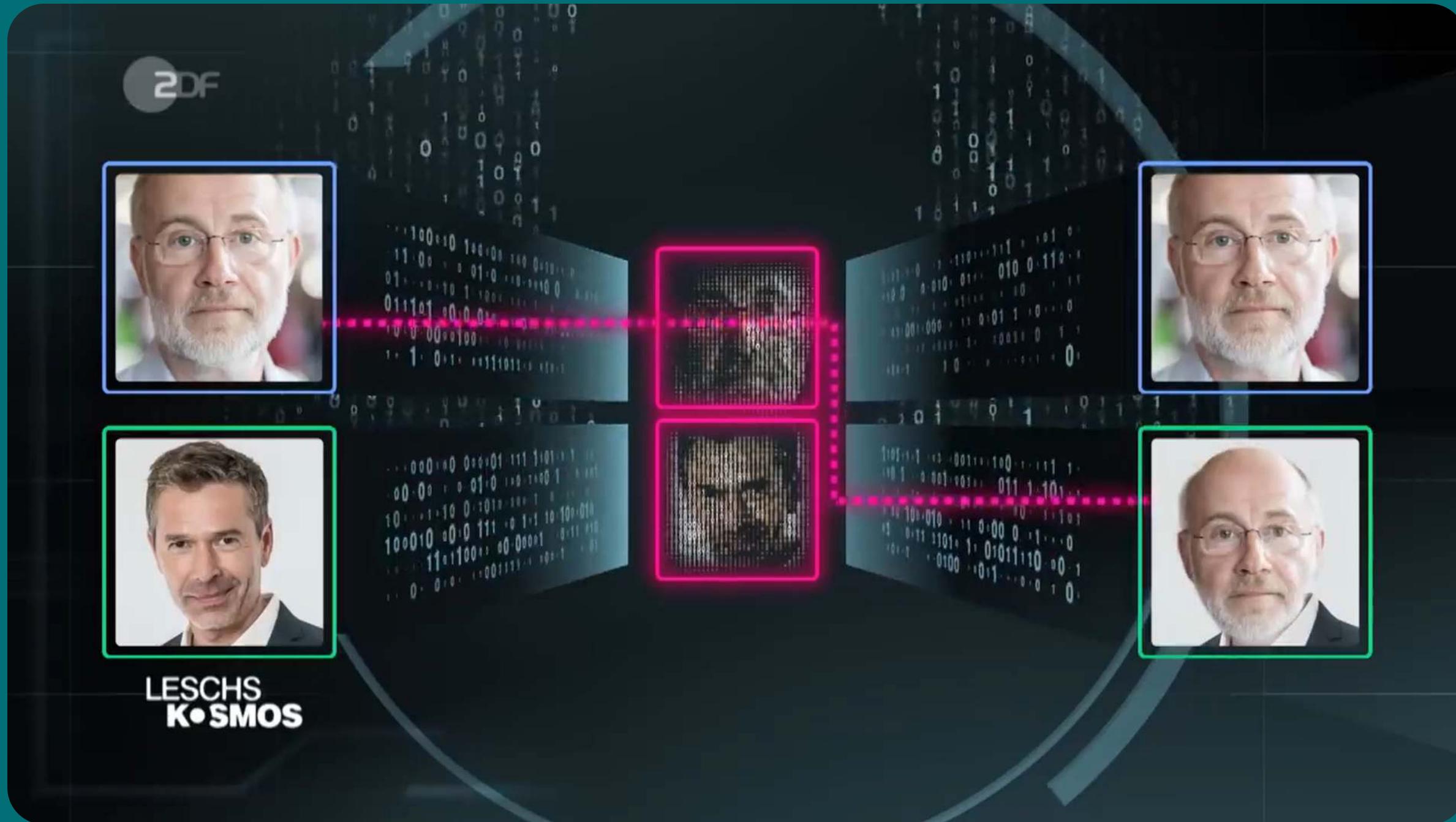
Latent Space
Representation

Decoder

Loss

Deepfakes in a Nutshell

Use Face Encoder but Different Face Decoder



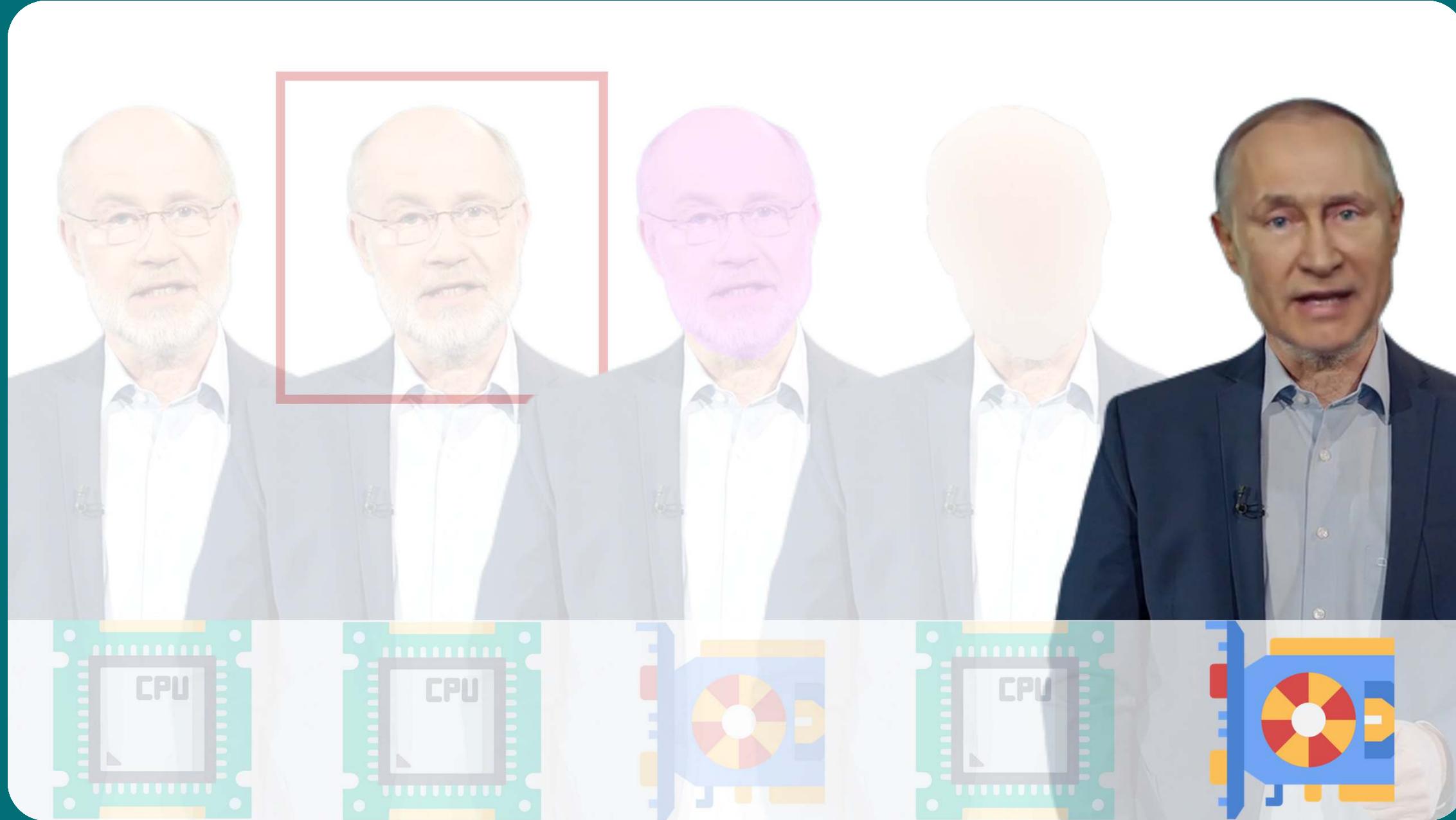
Agenda

- ▶ Deepfakes in a Nutshell
- ▶ Realtime Deepfakes
- ▶ Pushing Deepfakes to the Limit
- ▶ Videocalls with Deepfakes
- ▶ Conclusion



Realtime Deepfakes

Inference Workflow with TNG Realtime Deepfakes 2.0



Realtime Deepfakes

Fast Face Detection Demo



Realtime Deepfakes

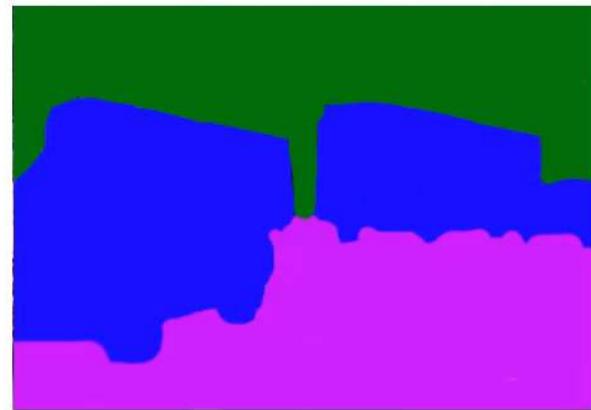
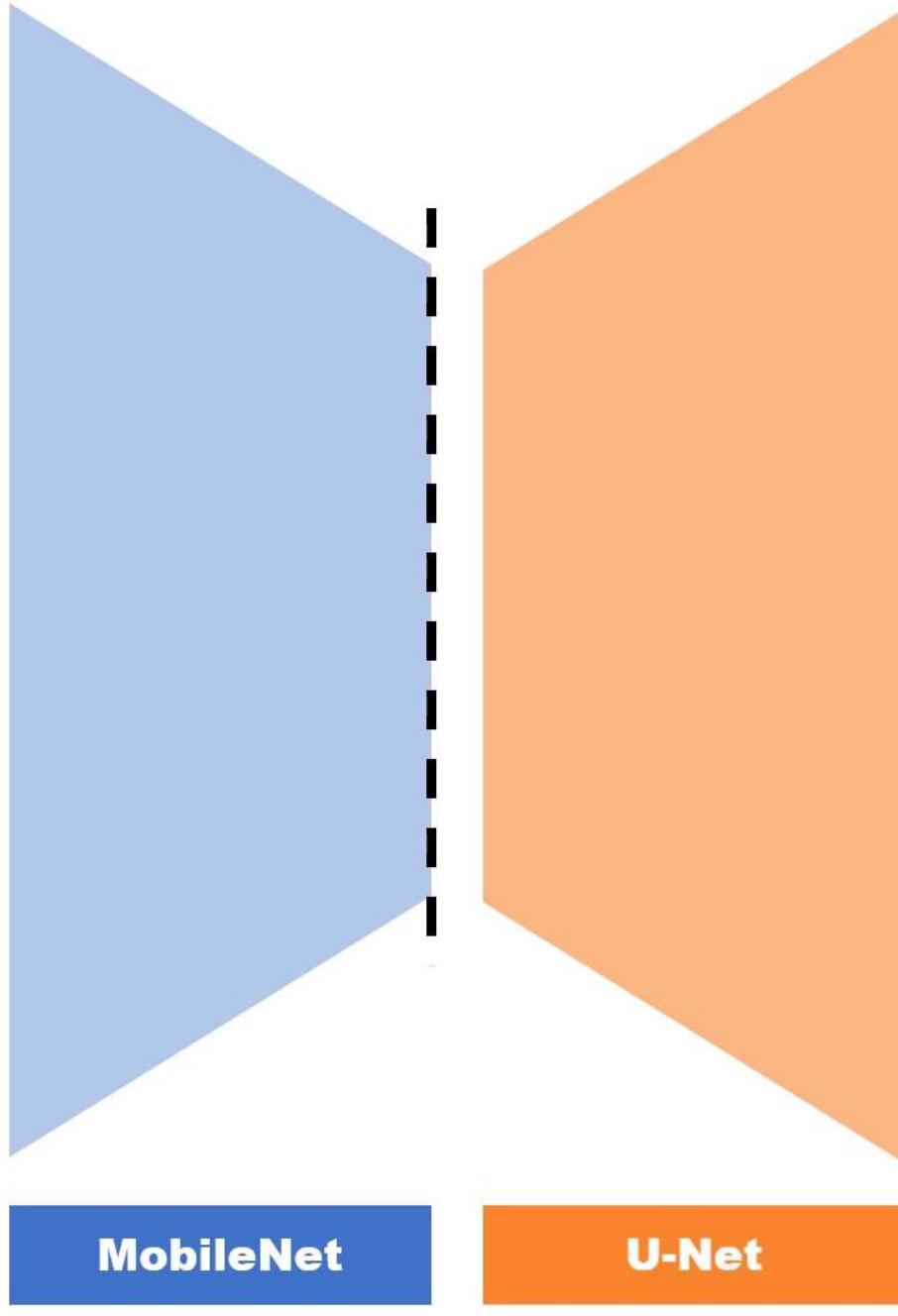
Face Segmentation Demo





Realtime Deepfakes

Transfer Learning for Face Segmentation



Realtime Deepfakes

Segmentation Dataset: CelebAMaskHQ



<https://github.com/switchablenorms/CelebAMask-HQ>

Realtime Deepfakes

Segmentation Dataset: CelebAMaskHQ



Eyeglasses



Hat



Earring



Necklace



Cloth



Hair

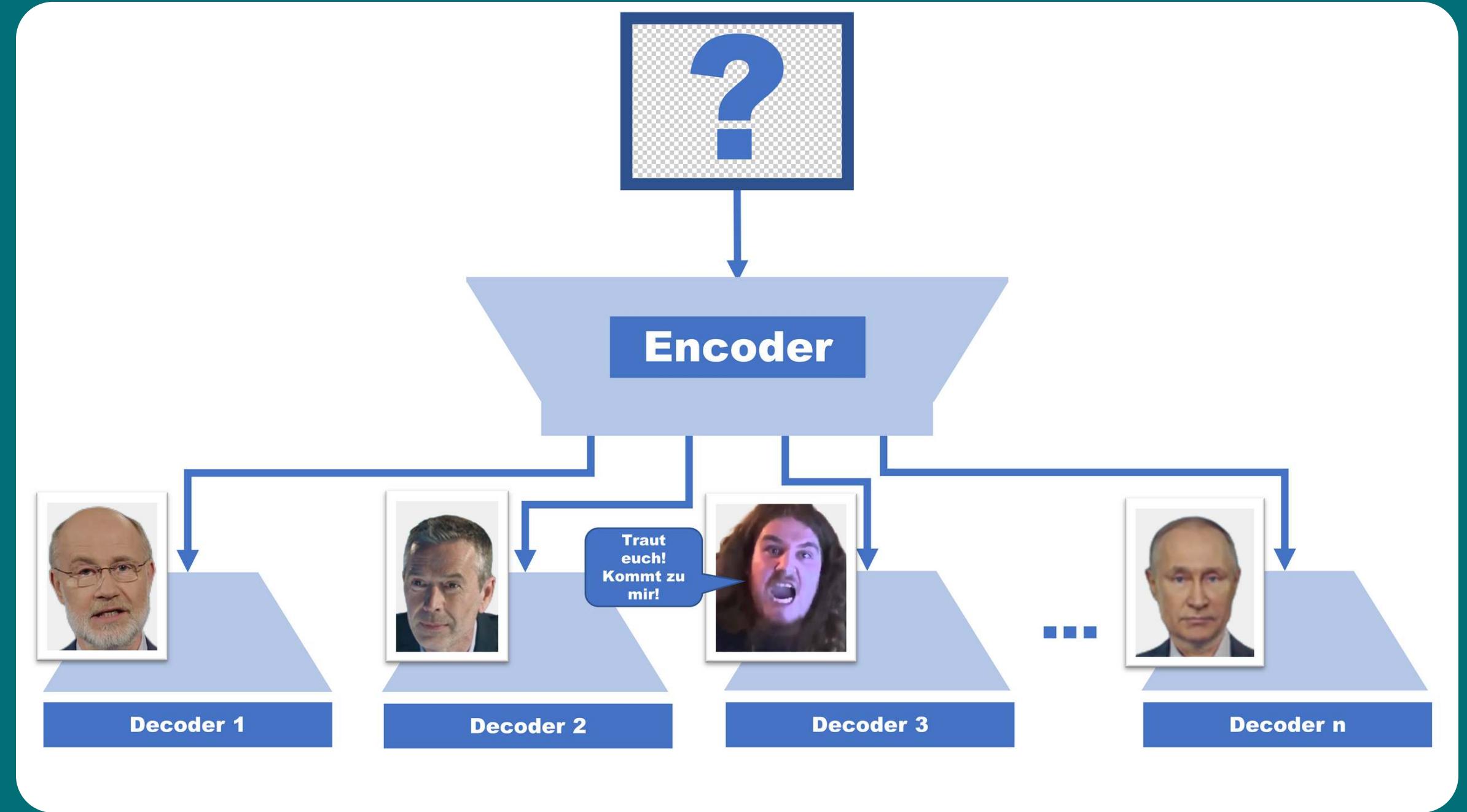
Realtime Deepfakes

OpenCV Inpainting Demo



Realtime Deepfakes

Multi-Decoder





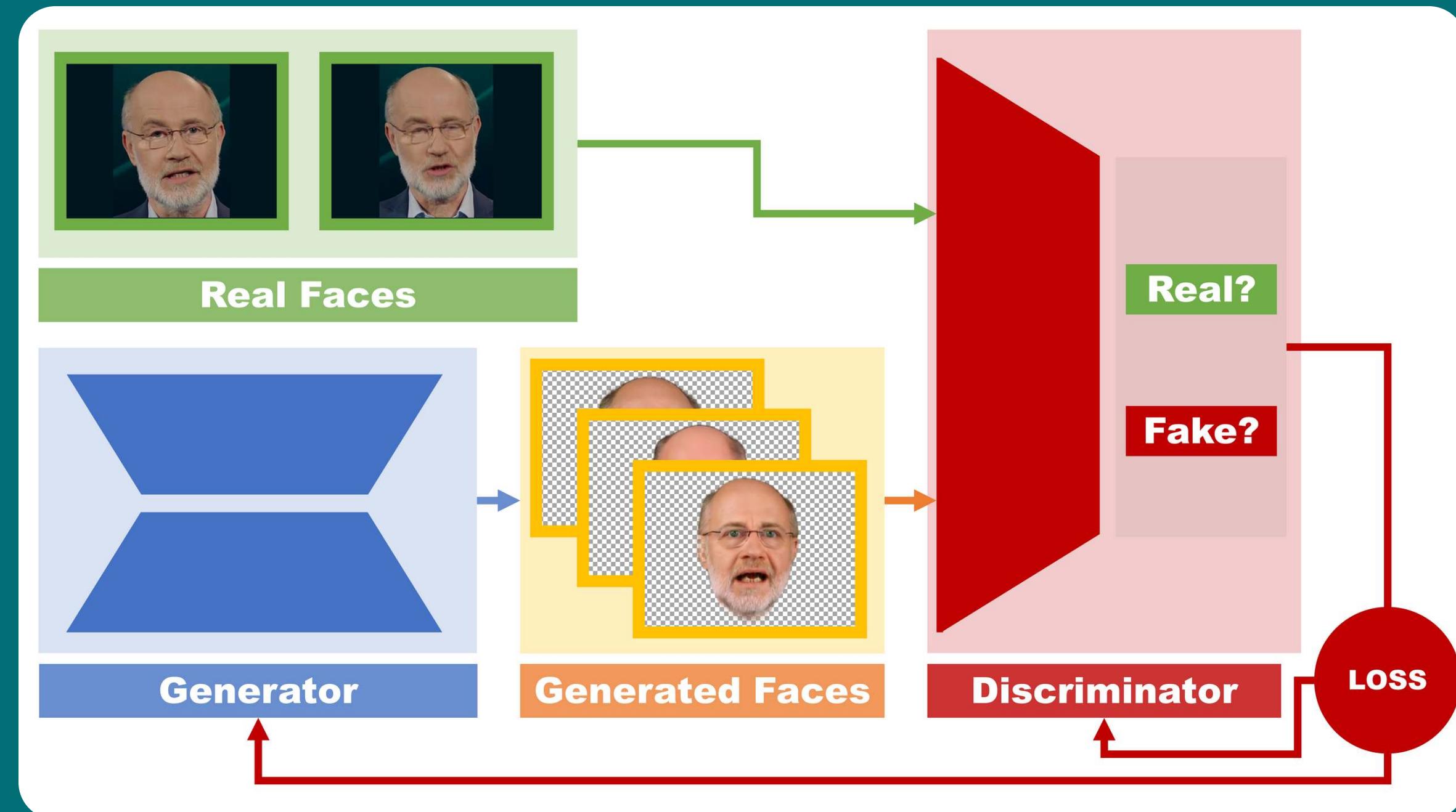
Realtime Deepfakes

First Results



Realtime Deepfakes

GAN (Generative Adversarial Networks) Training



Realtime Deepfakes

Full Demo

A large, red, rectangular stamp with a double-line border. The word "DEMO" is written in a bold, sans-serif font, centered within the stamp. The stamp has a slightly distressed, high-contrast appearance, giving it a printed or stamped look.

Realtime Deepfakes

Breaking News

Software ermöglicht Deep Fakes in Echtzeit
(heise.de)

ANGST VOR FAKE-VIDEOS

Deutsche Software schafft Deepfakes in Echtzeit
(mobilegeeks.de)

BREAKING NEWS

Deep-Fake-KI: Forscher tauschen Gesichter in Webcam-Aufnahmen in Echtzeit
(GameStar)

A



Realtime Deepfakes

Talks! Talks! Talks!



Realtime Deepfakes

Leschs Kosmos (ZDF) Wants to Report on Realtime Deepfakes



Realtime Deepfakes

Challenges: Blurry Details



Realtime Deepfakes

Challenges: Disappearing Hair



Realtime Deepfakes

The "Hair Trick"

Agenda

- ▶ Deepfakes in a Nutshell
- ▶ Realtime Deepfakes
- ▶ Pushing Deepfakes to the Limit
- ▶ Videocalls with Deepfakes
- ▶ Conclusion



Deepfakes 2.1

Introducing Tensorflow 2



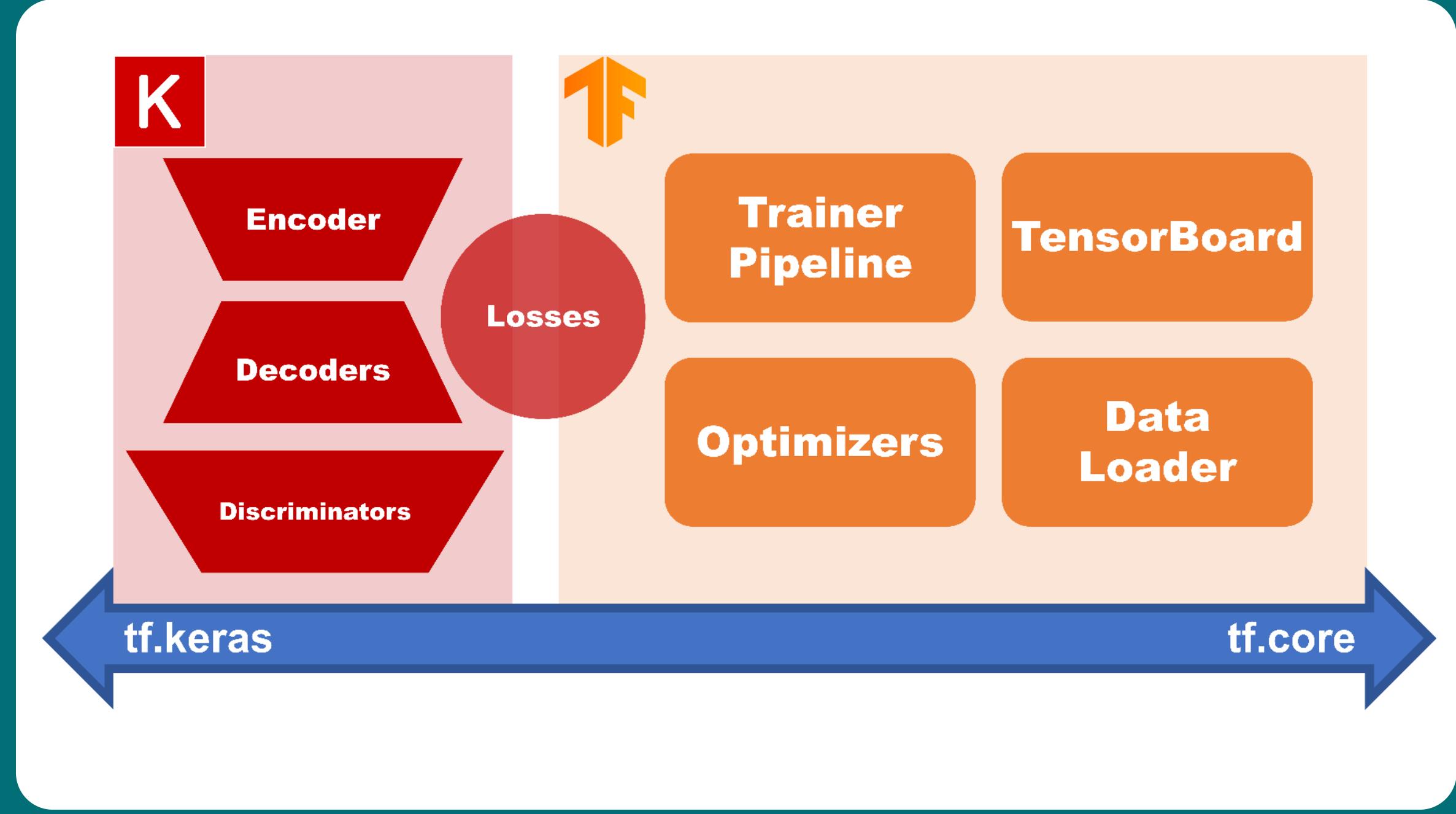
Deepfakes 2.1

Tensorflow ❤️ Keras



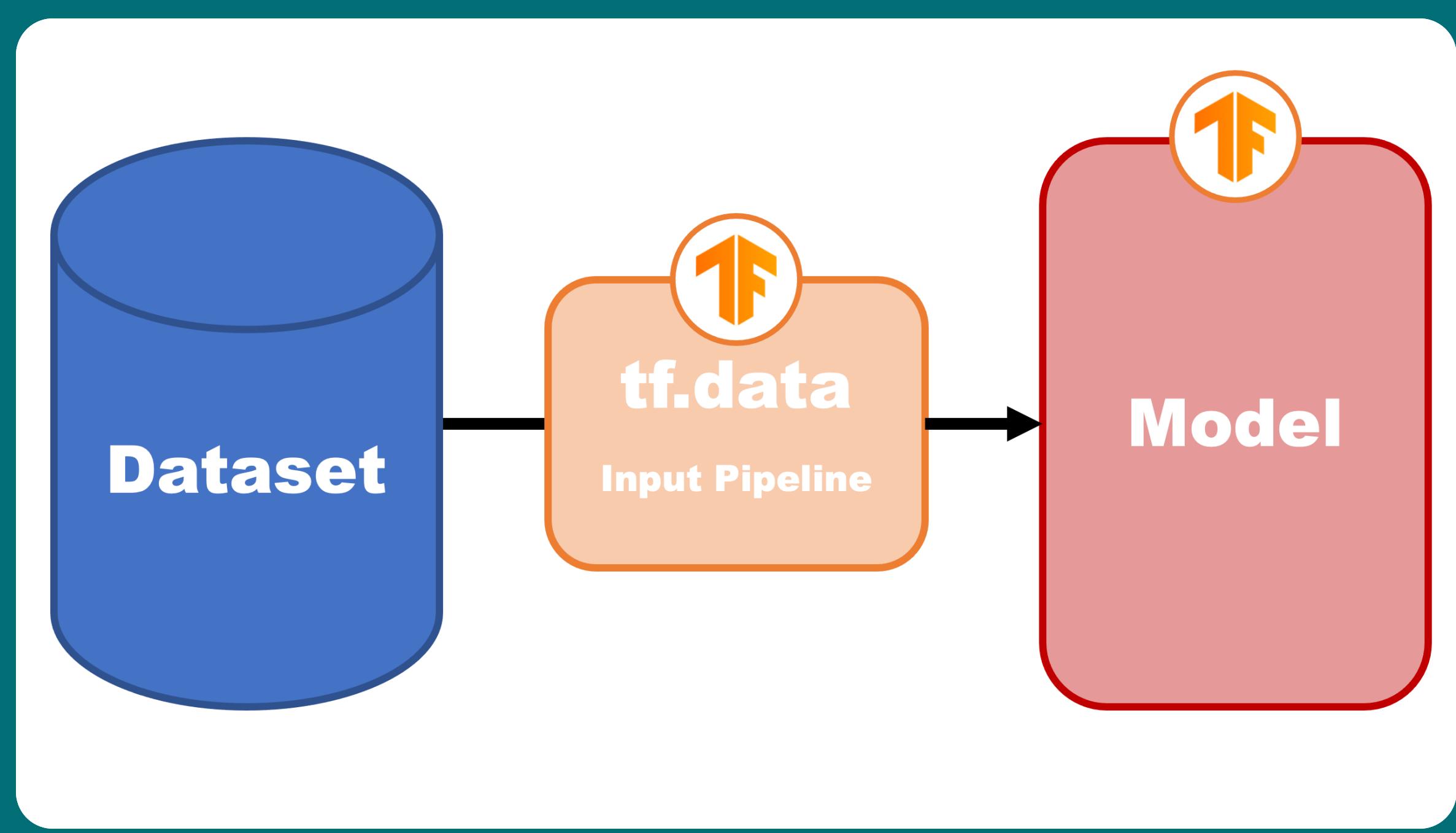
Deepfakes 2.1

Rewrite Trainer in Tensorflow 2



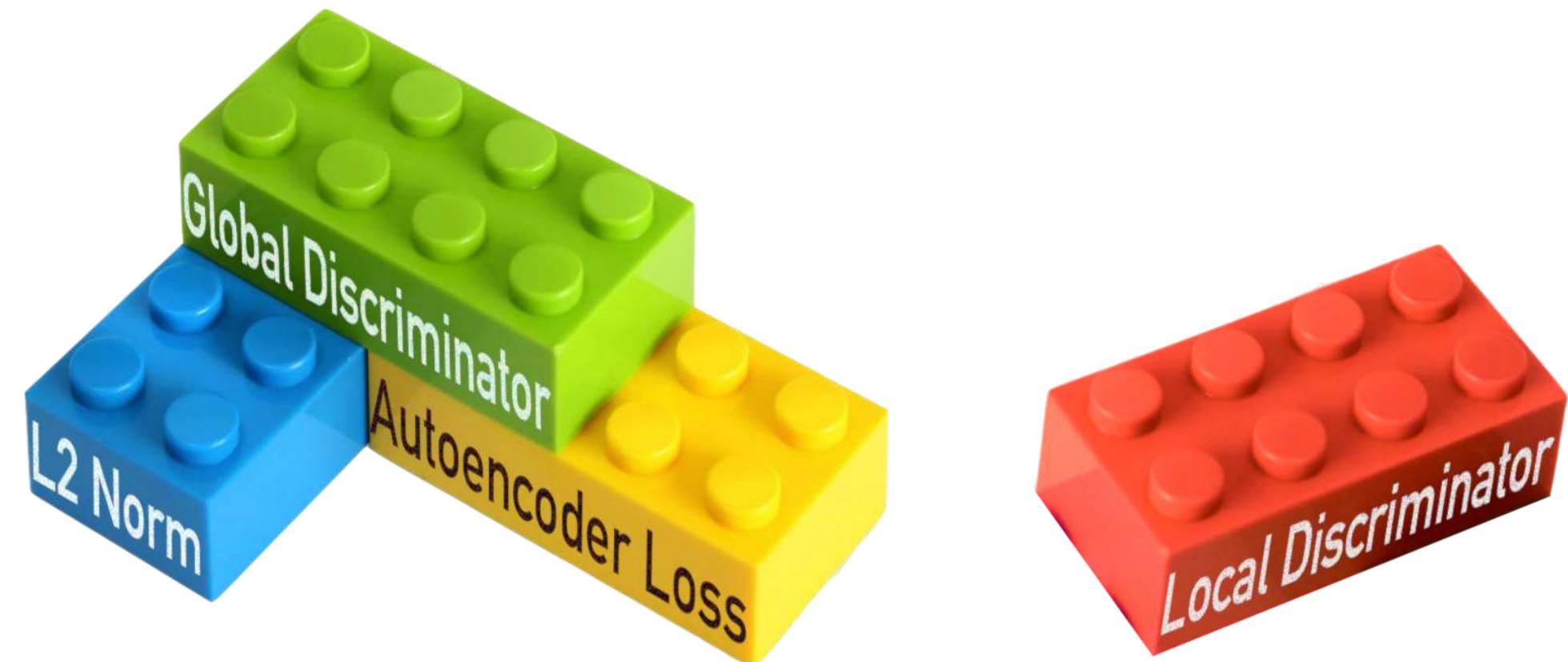
Deepfakes 2.1

`tf.data`: Faster loading of larger Datasets



Deepfakes 2.1

Modular Training Pipeline



Deepfakes 2.1

Remaining Issues

Realtime Deepfakes 2.0 - Challenges



1

Distortions

2

Alignment Problems

3

Centering Issues

4

Improveable Performance

Deepfakes 2.1

Remaining Issues: Speed

Deepfakes 2.1

Introducing MediaPipe (2021)



MediaPipe

Deepfakes 2.1

Introducing MediaPipe (2021)



Ready-to-use solutions



Build once, deploy anywhere



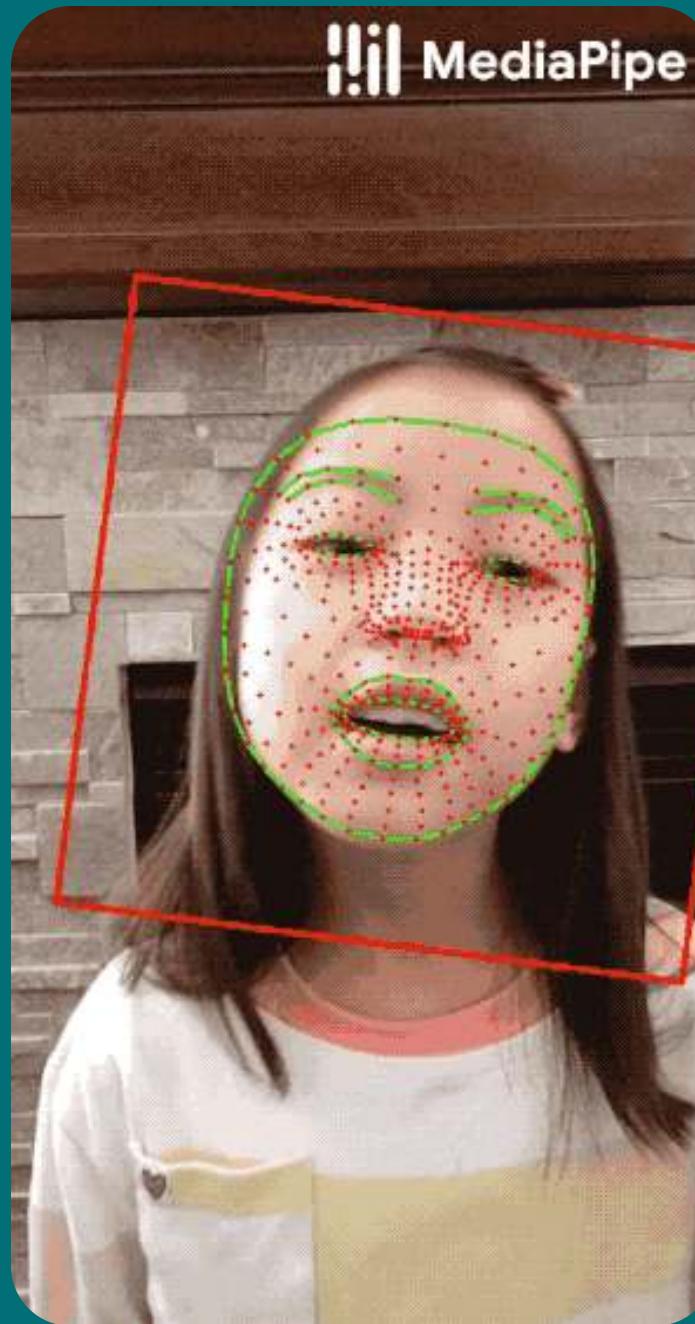
End-to-End acceleration



Free and open source

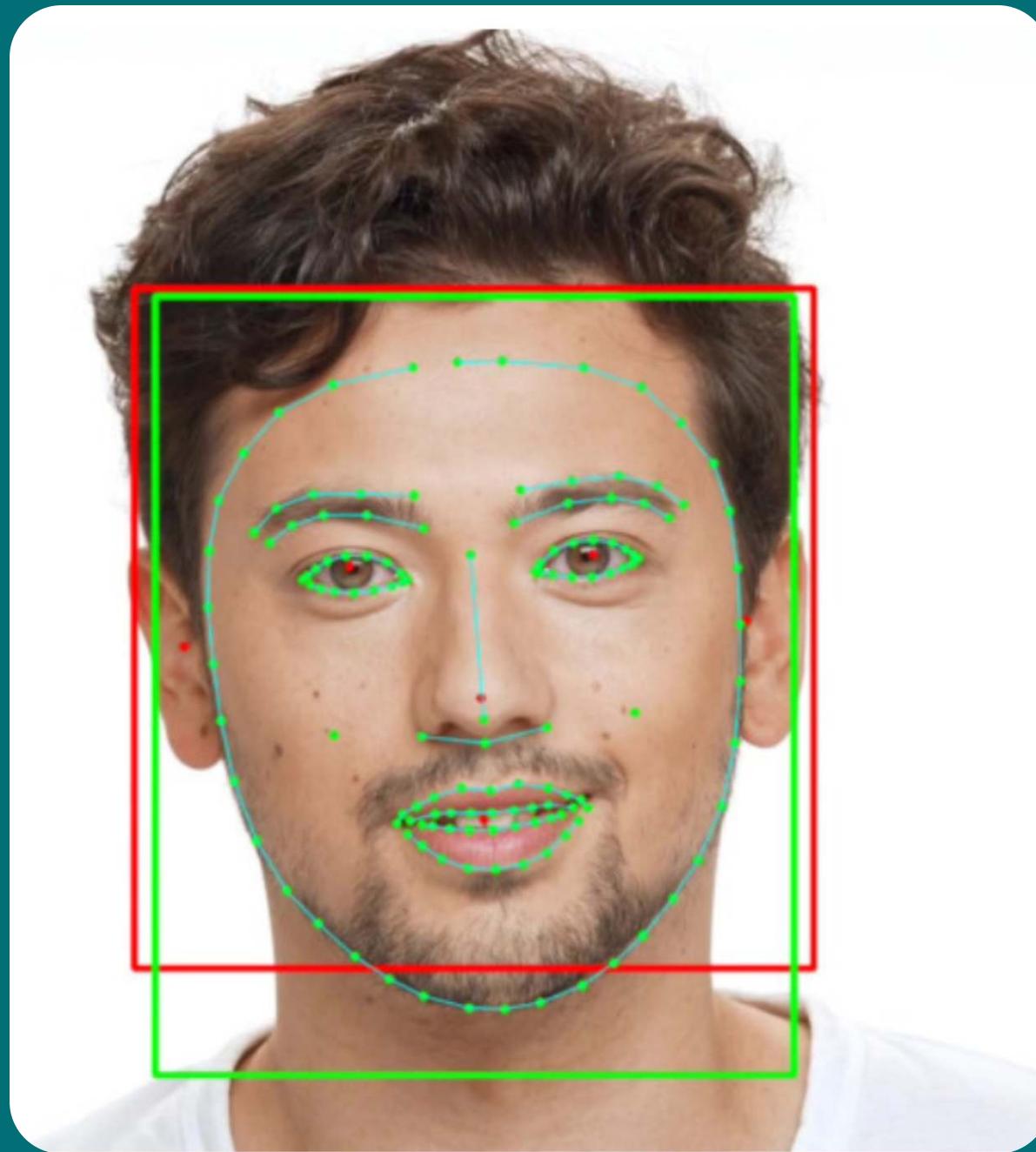
Deepfakes 2.1

Face Mesh for Fast Face Landmark Detection



Deepfakes 2.1

FaceMesh Is Based on BlazeFace Face Detection



Deepfakes 2.1

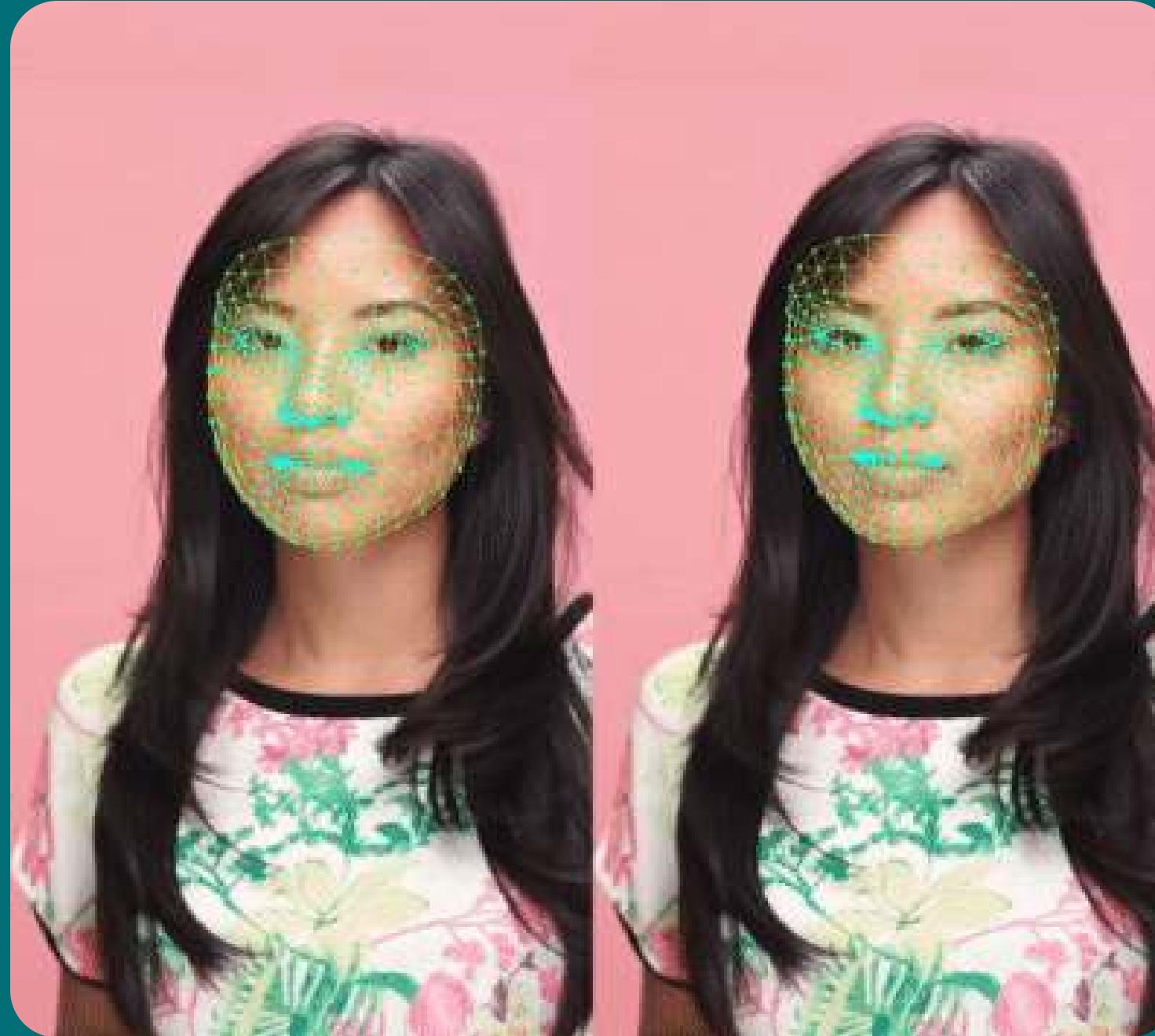
From Face Mesh with 468 Landmark Points to Facial Surface



SCAN ME

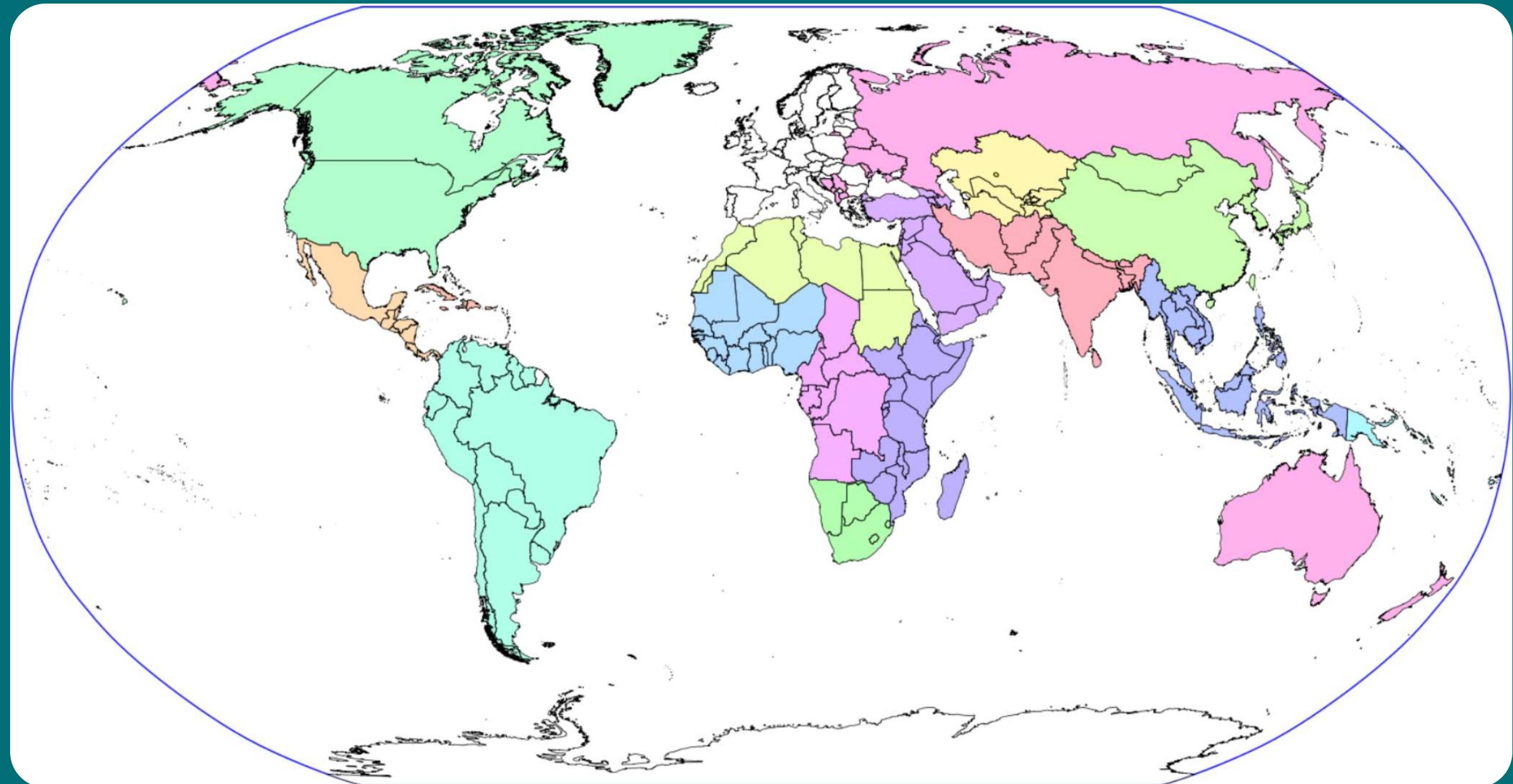
Deepfakes 2.1

Temporal Consistency



Deepfakes 2.1

FaceMesh Fairness Evaluation



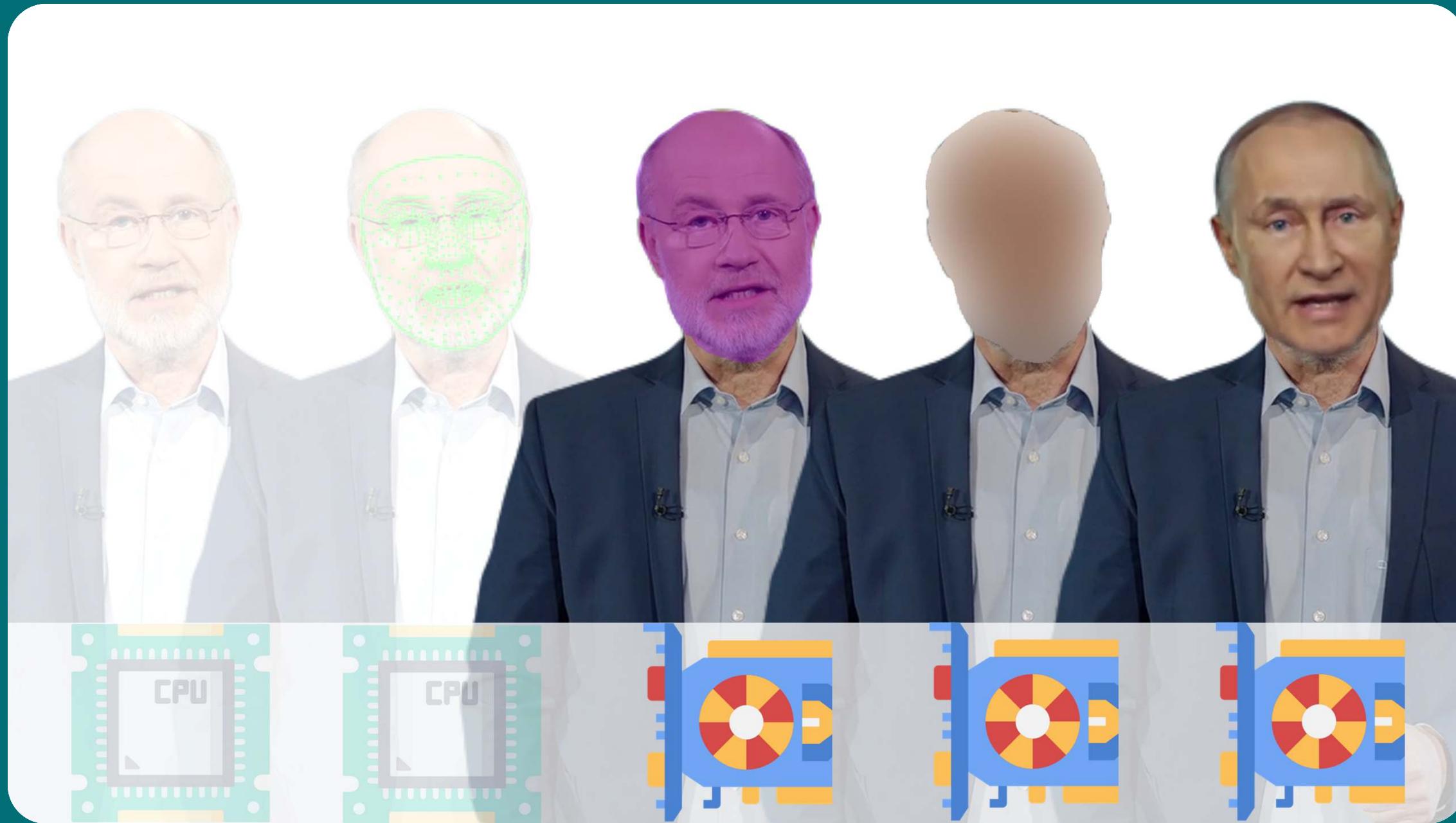
MediaPipe Demo

FaceMesh Demo

DEMO

Realtime Deepfakes 2.1

Inference Workflow



Deepfakes 2.1

Full Demo

A large, red, rectangular stamp with a double-line border. The word "DEMO" is written in a bold, sans-serif font, oriented diagonally from the top-left corner to the bottom-right corner of the stamp.

Agenda

- ▶ Deepfakes in a Nutshell
- ▶ Realtime Deepfakes
- ▶ Pushing Deepfakes to the Limit
- ▶ Videocalls with Deepfakes
- ▶ Conclusion





Pro7 Galileo



Can You Cheat People on Video Calls?



Can You Cheat People on Video Calls?



Harro Füllgrabe



Matthias Fiedler

Pro7 Galileo



Can You Cheat People on Video Calls?

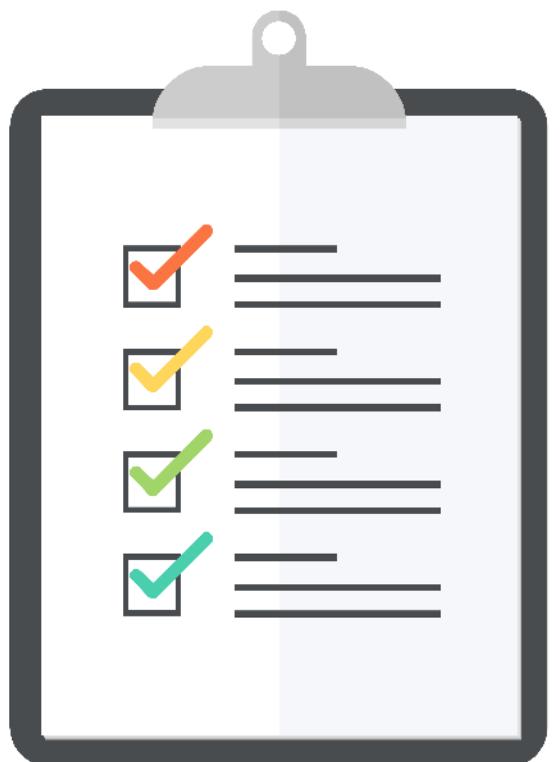


Realtime Deepfakes as Attack Vector

They Are Real and You Should Know about That!

Checklist: Attack Vectors

#1



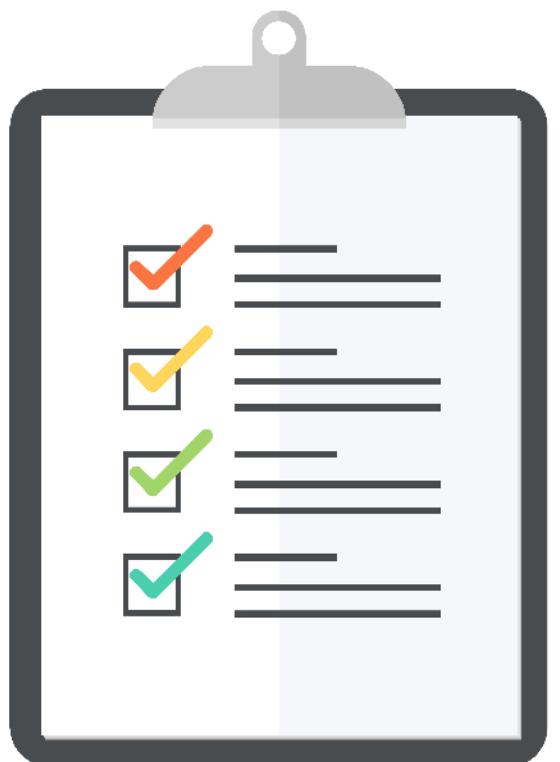
- 1 Phishing Scams
- 2 Data Breaches
- 3 Hoaxes
- 4 Celebrity Pron
- 5 Reputation Smearing

Realtime Deepfakes as Attack Vector

They Are Real and You Should Know about That!

Checklist: Attack Vectors

#2



6 Election Manipulation

7 Social Engineering

8 Identity Theft

9 Financial Fraud

10 Blackmail

Scam Alert! ⚠

Woman Thought Vin Diesel Loved Her - Sent £5,000 in Online Scam



Pro7 Galileo



Part 2 - Fooling Parents

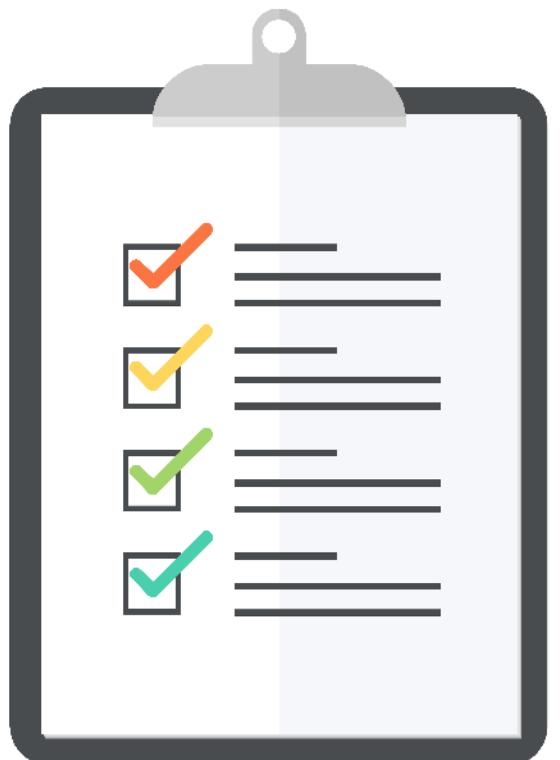


Realtime Deepfakes As Attack Vector

They Are Real and You Should Know about That!

Checklist: Signs to spot deepfakes

#1



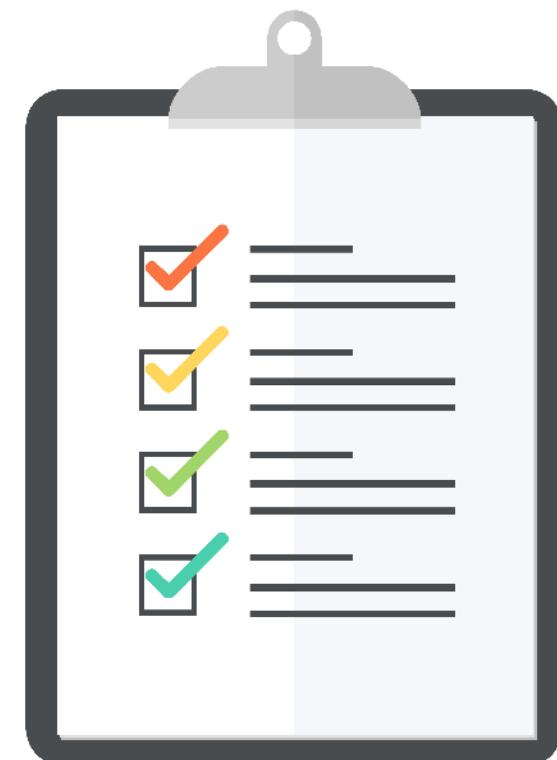
- 1 **Suspicious Behaviour**
- 2 **Low Level Of Skin Details**
- 3 **Unusual Distortions In Face**
- 4 **Lack of Emotion**
- 5 **Artifacts Around the Headedges**

Realtime Deepfakes As Attack Vector

They Are Real and You Should Know about That!

Checklist: Signs to spot deepfakes

#2



- 6 Inconsistent Noise or Audio
- 7 Unnatural Coloring
- 8 Unnatural Facial Expression
- 9 Unnatural Eye Movement
- 10 Hair & Teeth don't look real

Agenda

- ▶ Deepfakes in a Nutshell
- ▶ Realtime Deepfakes
- ▶ Pushing Deepfakes to the Limit
- ▶ Videocalls with Deepfakes
- ▶ Conclusion



Evolution of Deepfakes ...

... is much faster than we predicted in 2019

Year	Name	Replacing	Realtime	Open Source	Technology
2017	DeepFaceLab				FaceNet
2019	TNG Deepfakes 2.0				
2020	DeepFaceLab				FaceNet
2021	TNG Deepfakes 2.1				
2021	DeepFaceLive				FaceNet

In 2019 we predicted ...

... that Deepfakes will be used in the Movie Industry

CGI

Deepfake

Movie Industry

Our Predictions came true!

THE MANDALORIAN DEEPFAKE

BREAKING NEWS

Lucasfilm hires the YouTube deepfaker who put its Luke, Leia and Tarkin cameos to shame

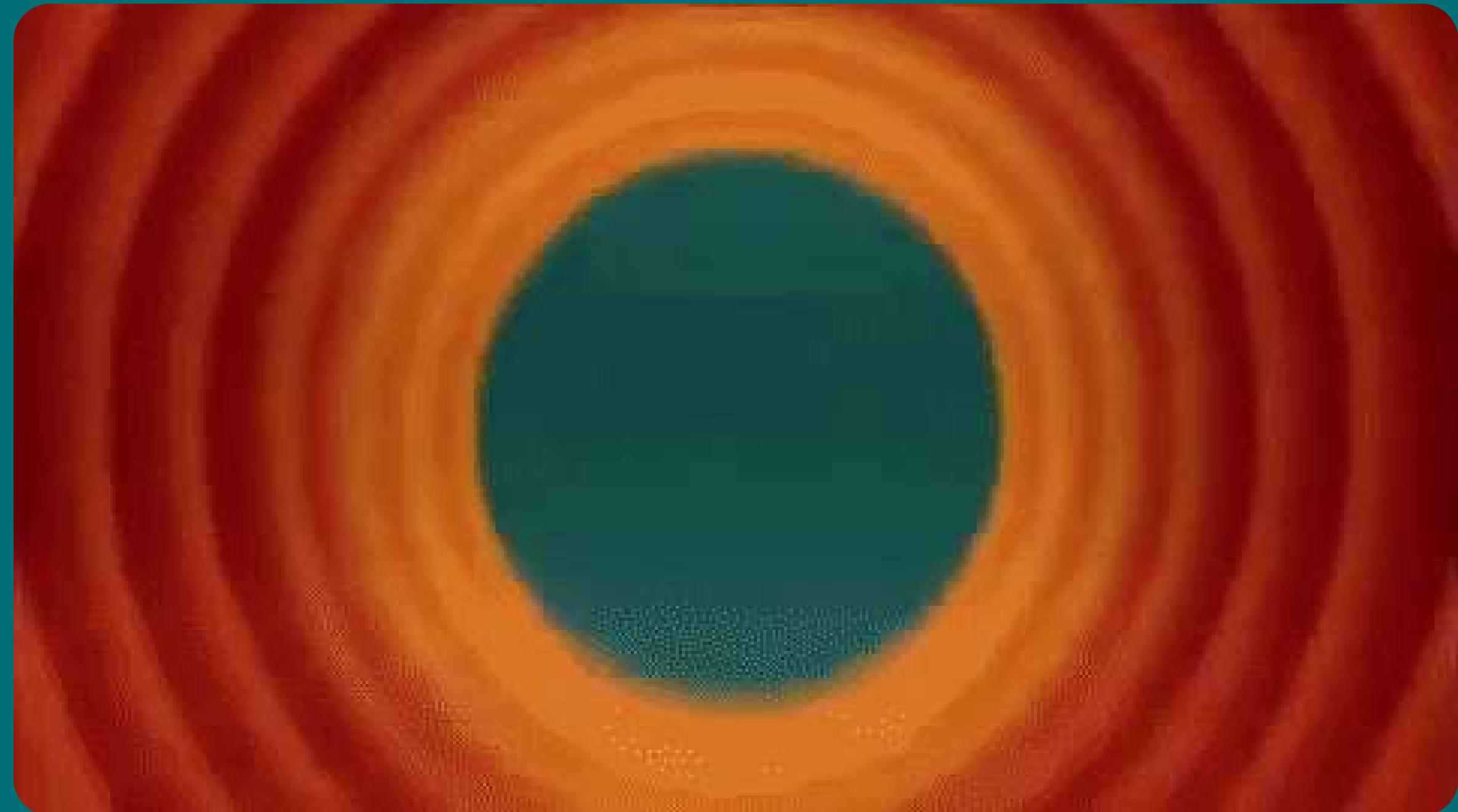
(theverge.com)

Lucasfilm Hires YouTuber After His Deepfake of Luke Skywalker in *The Mandalorian* Goes Viral

(gizmodo.com)

Finish. Final. Fin. Ende.

Fine. конец. Einde. Pää. Lõpp. Pabaiga.



Other AI related talks



Style Transfer AI

This talk introduces you into deep neural networks, how they work internally and how they process images.

Artificial Neurons, Gradient Descent, Deep Neural Networks, Cost Function



Realtime Deepfakes

This talk introduces you into how deep fakes can be created and what it took to realize deep fakes in realtime.

Deep Neural Networks, Autoencoder, Transfer Learning, Generative Adversarial Networks

Speakers



Thomas Endres

Partner

Oracle® JavaOne Rockstar

Intel® Black Belt Software Developer

Intel® Software Innovator

Intel® Top Innovator 2014 - 2018



Martin Förtsch

Principal Consultant

Oracle® JavaOne Rockstar

Intel® Black Belt Software Developer

Intel® Software Innovator

Intel® Top Innovator 2014 - 2018



Jonas Mayer

Senior Consultant

Bedroom DJ

Teakwondo Black Belt

GameStar Certified Hacker

Intel® Software Innovator

Audio Deepfakes

Tacotron 2 (2017)



Audio Deepfakes

Tacotron 2 (2017)



**THE MORE
YOU TAMPER
A SWORD THE
STRONGER
IT BECOMES.**



SCAN ME

Audio Deepfakes

Tacotron 2 (2017)

REAL

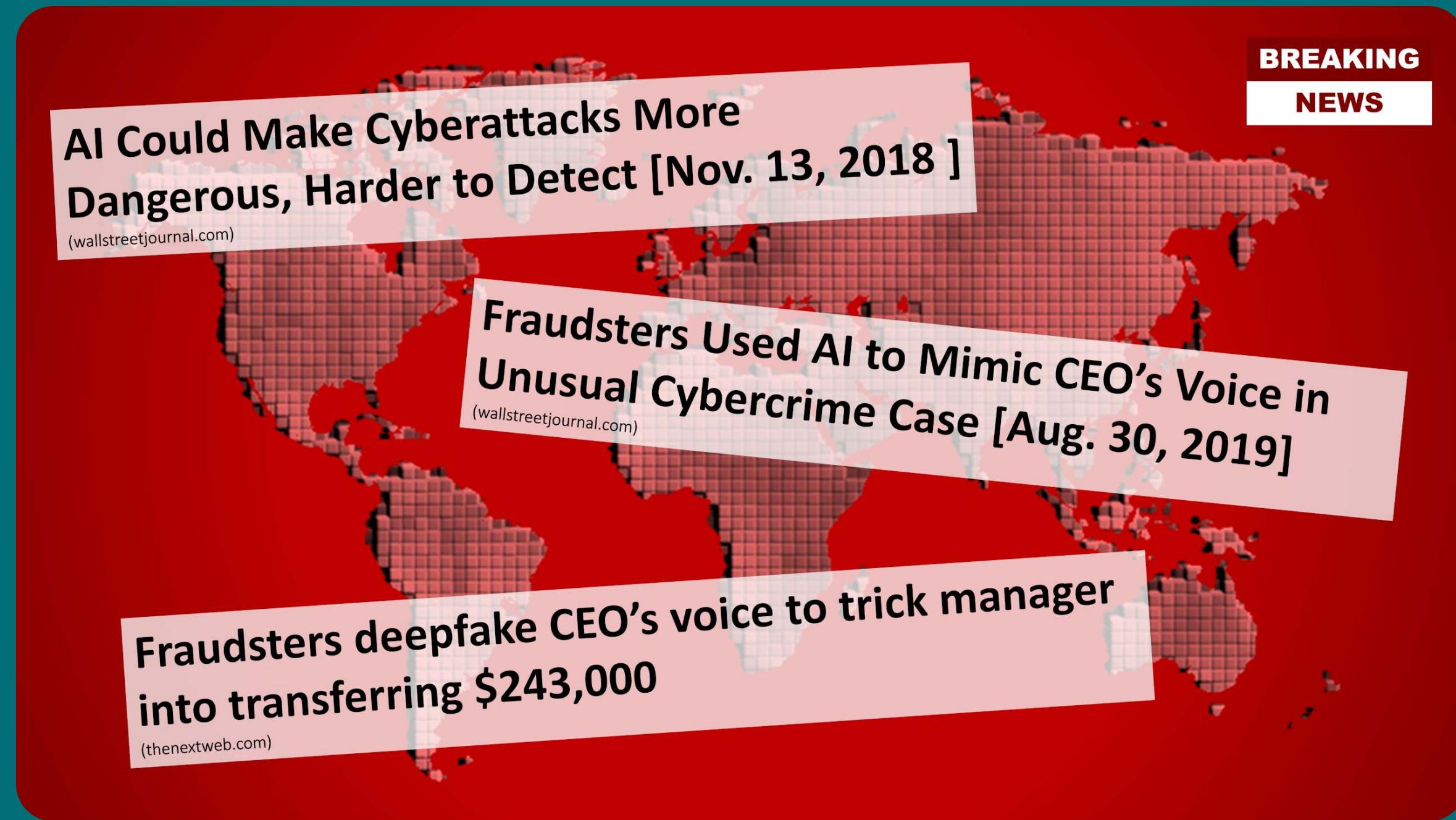
FAKE



SCAN ME

Audio Deepfakes

First Documented Audio Deepfake Fraud



AI Could Make Cyberattacks More Dangerous, Harder to Detect [Nov. 13, 2018]
(wallstreetjournal.com)

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case [Aug. 30, 2019]
(wallstreetjournal.com)

Fraudsters deepfake CEO's voice to trick manager into transferring \$243,000
(thenextweb.com)

BREAKING NEWS