Alyssa
MILLER

Stealing Reality

Exploiting the Human Element with Deep Fakes

Hacker/Researcher

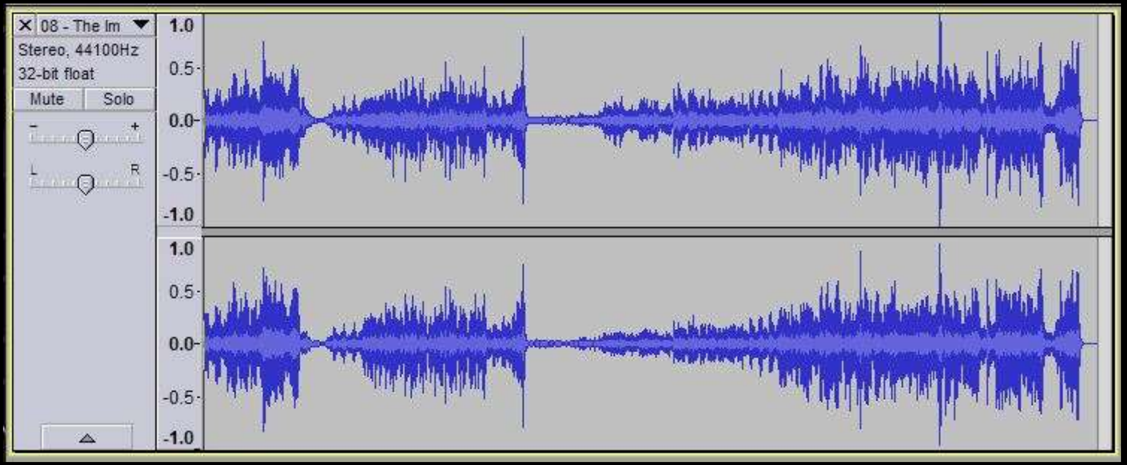
Security Advocate

Author & Blogger

Co-Host: Uncommon Journey

snyk

Deep Fakes…

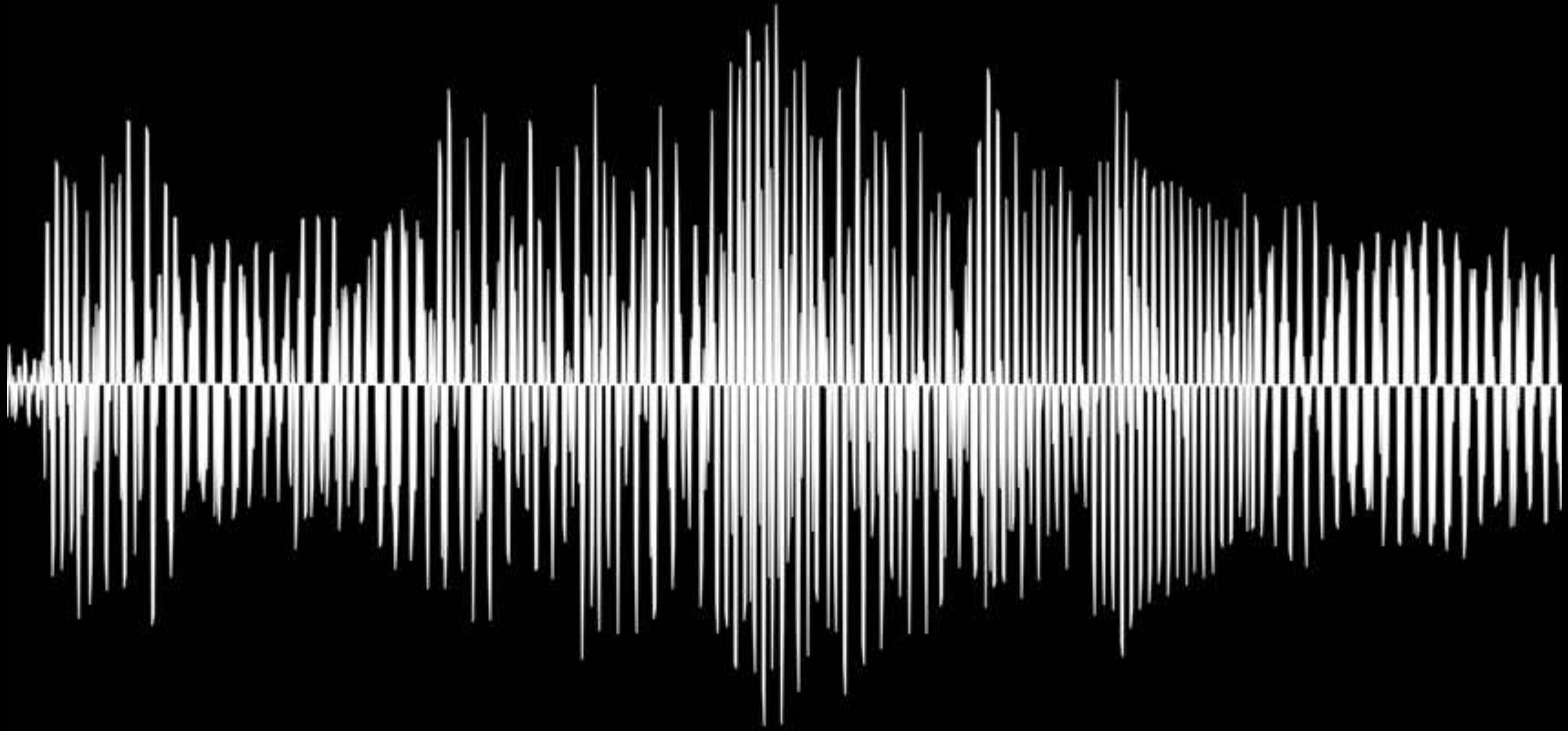

08 - The Im
Stereo, 44100Hz
32-bit float
Mute
Solo
L
R
1.0
0.5
0.0
-0.5
-1.0
1.0
0.5
0.0
-0.5
-1.0

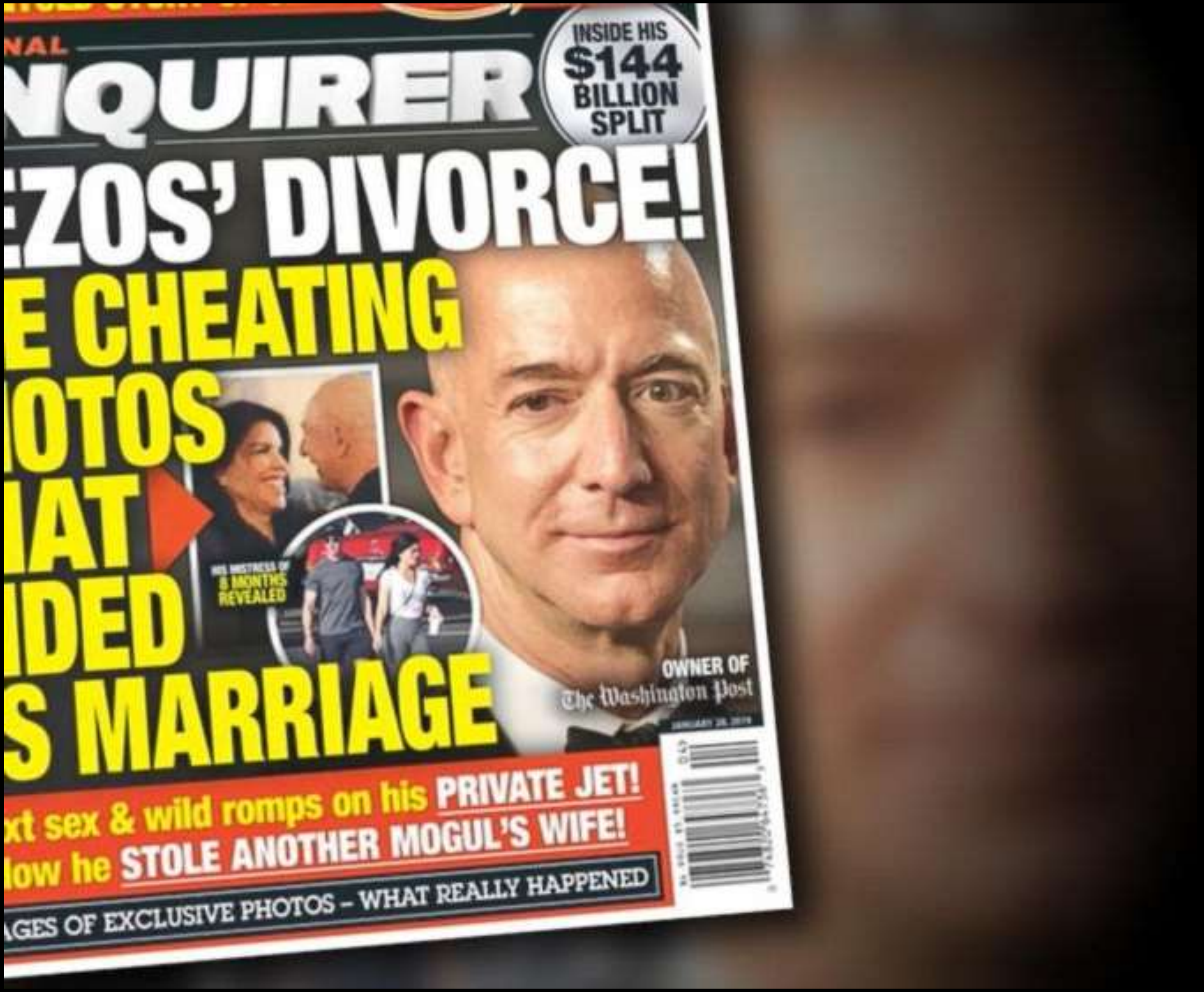
LLYWOOD
REIGN
ESS
OCIATION
GOLDEN
GLOBE
AWAR
GOLDEN
GLOB
AWA

Deepfake Beginnings…

Politics…

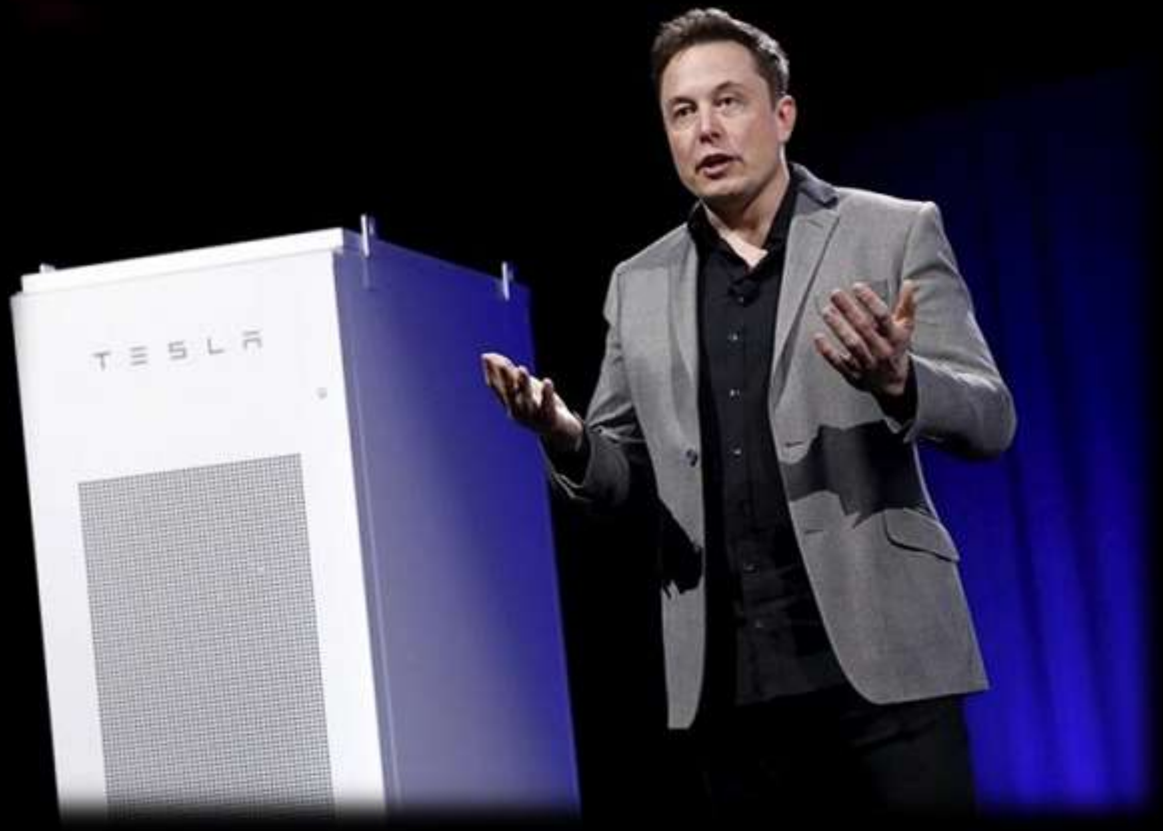
Social Engineering…

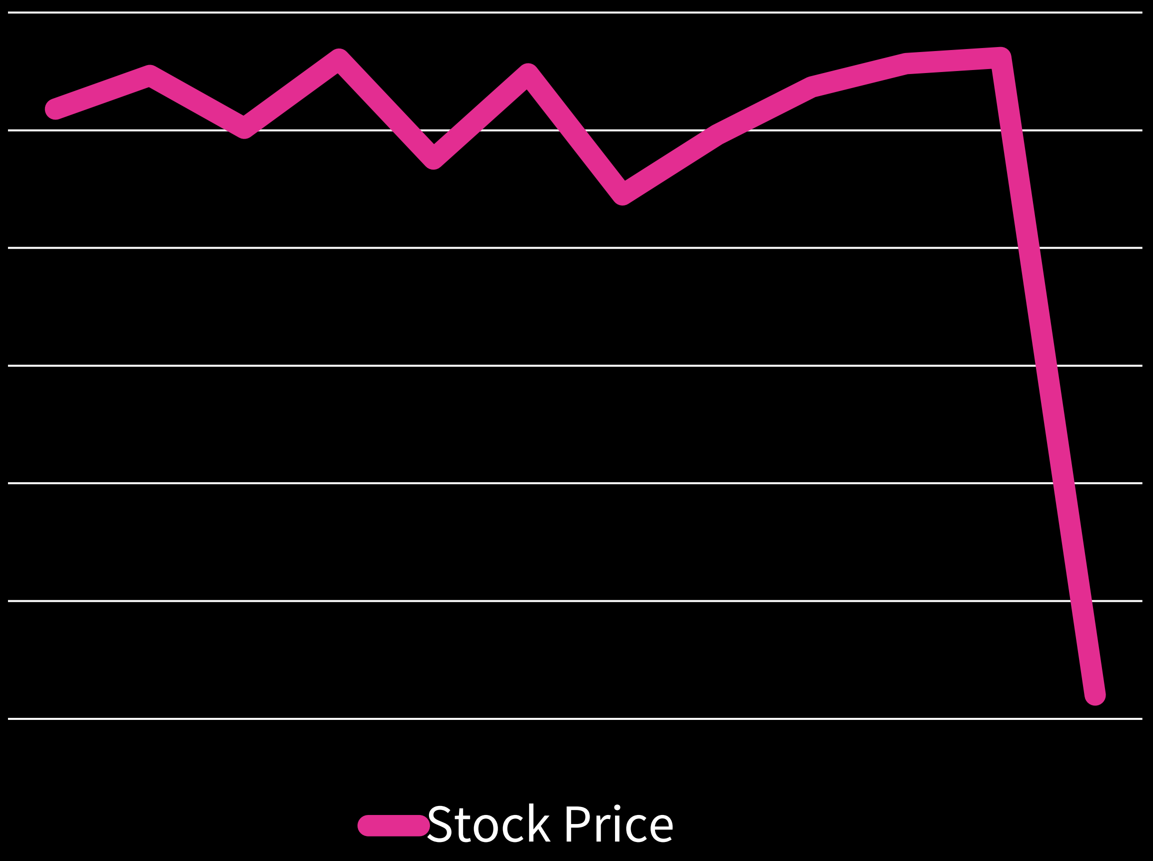



NAL
NQUIRER
INSIDE HIS $144 BILLION SPLIT
EZOS' DIVORCE!
E CHEATING
IOTOS
IAT
IDED
S MARRIAGE
HIS MISTRESS OF 8 MONTHS REVEALED
OWNER OF The Washington Post
JANUARY 28, 2019
xt sex & wild romps on his PRIVATE JET!
low he STOLE ANOTHER MOGUL'S WIFE!
AGES OF EXCLUSIVE PHOTOS – WHAT REALLY HAPPENED

Extortion...

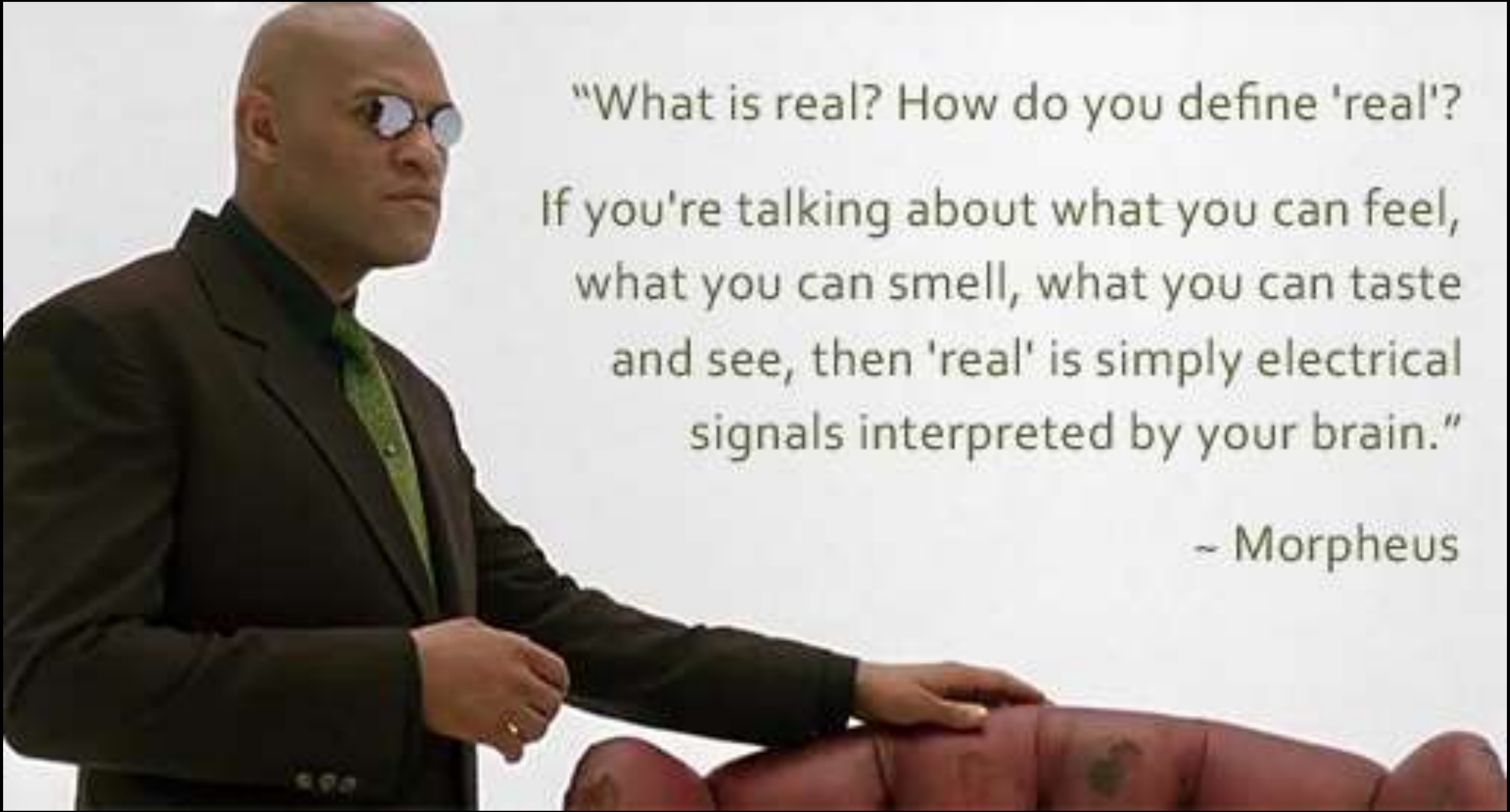
“Outsider” Trading…





Market Manipulation…

Fake News…

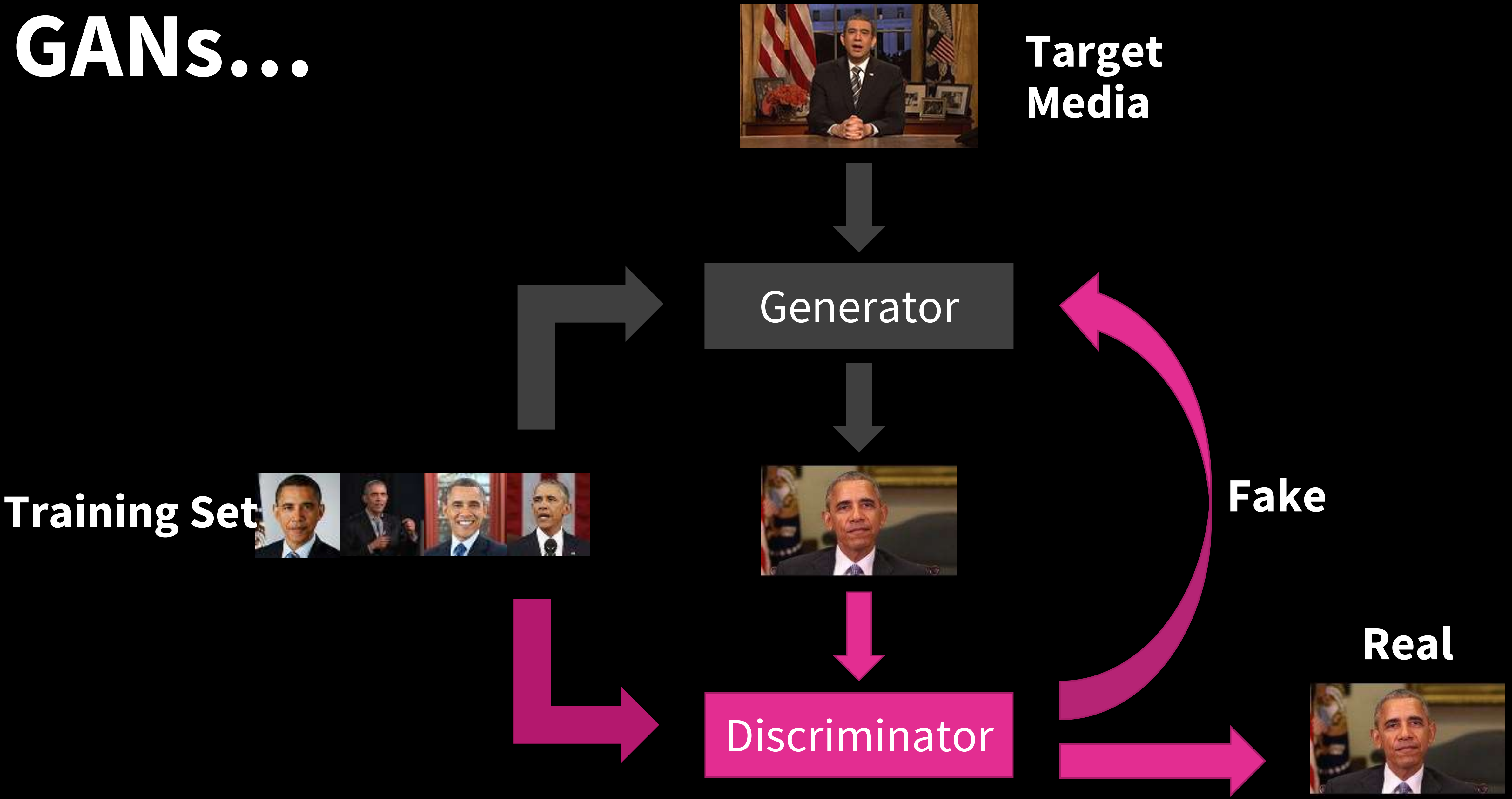


"What is real? How do you define 'real'?

If you're talking about what you can feel, what you can smell, what you can taste and see, then 'real' is simply electrical signals interpreted by your brain."

~ Morpheus

GANs...



Target Media

Generator

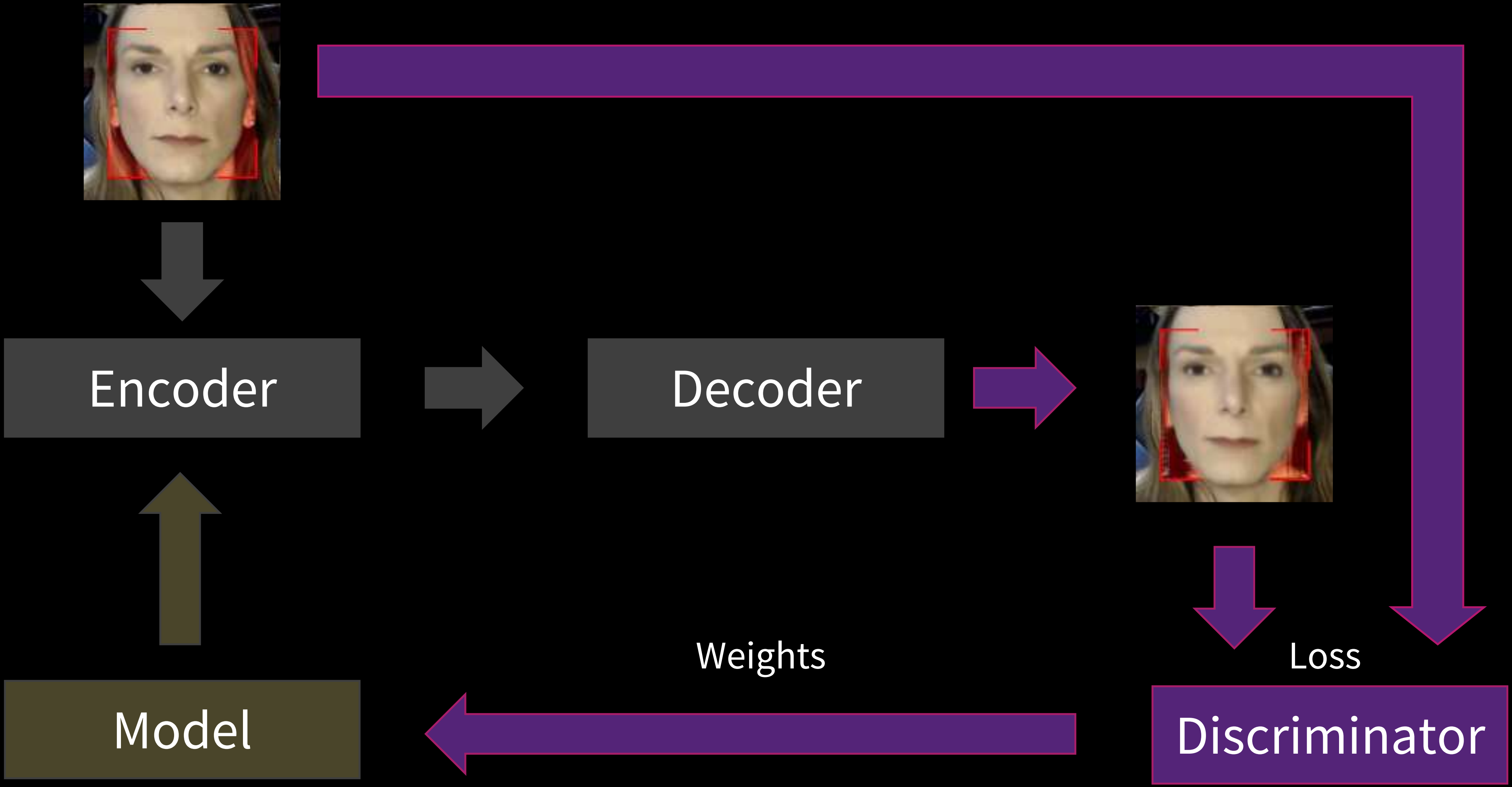
Training Set

Fake

Discriminator

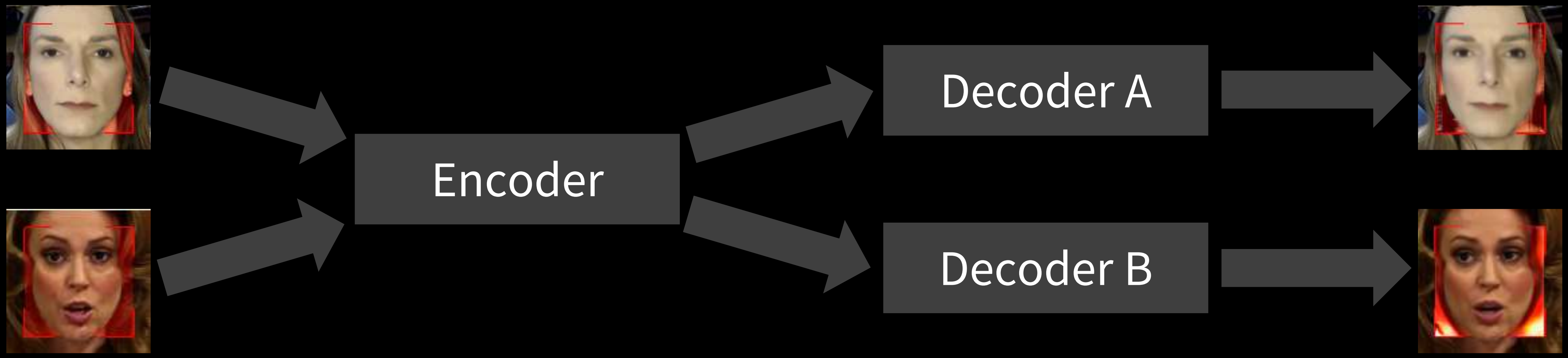
Real

A Deeper Look...



Conversion Models...

Training

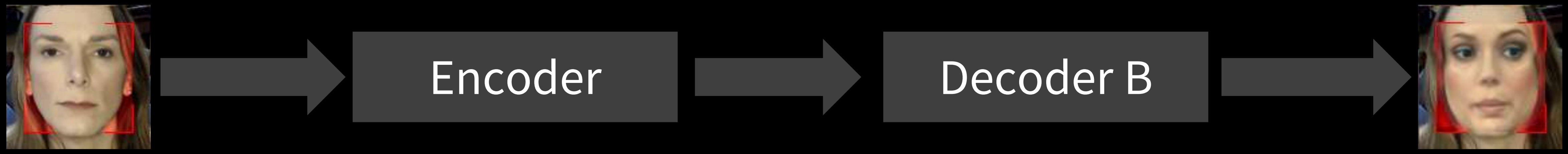


Encoder

Decoder A

Decoder B

Convert



Encoder

Decoder B

That Doesn’t Fit…

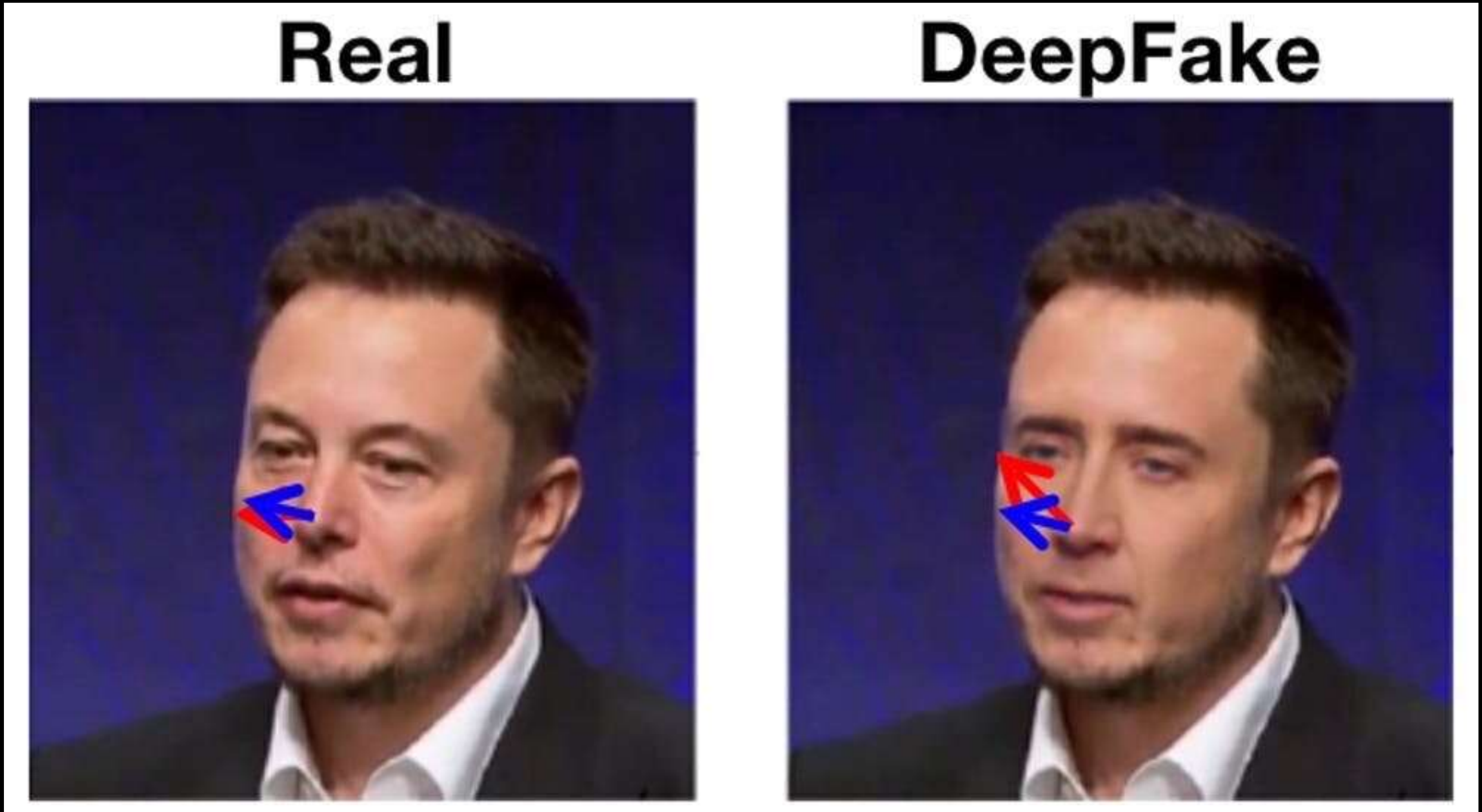


Image: Phys.org

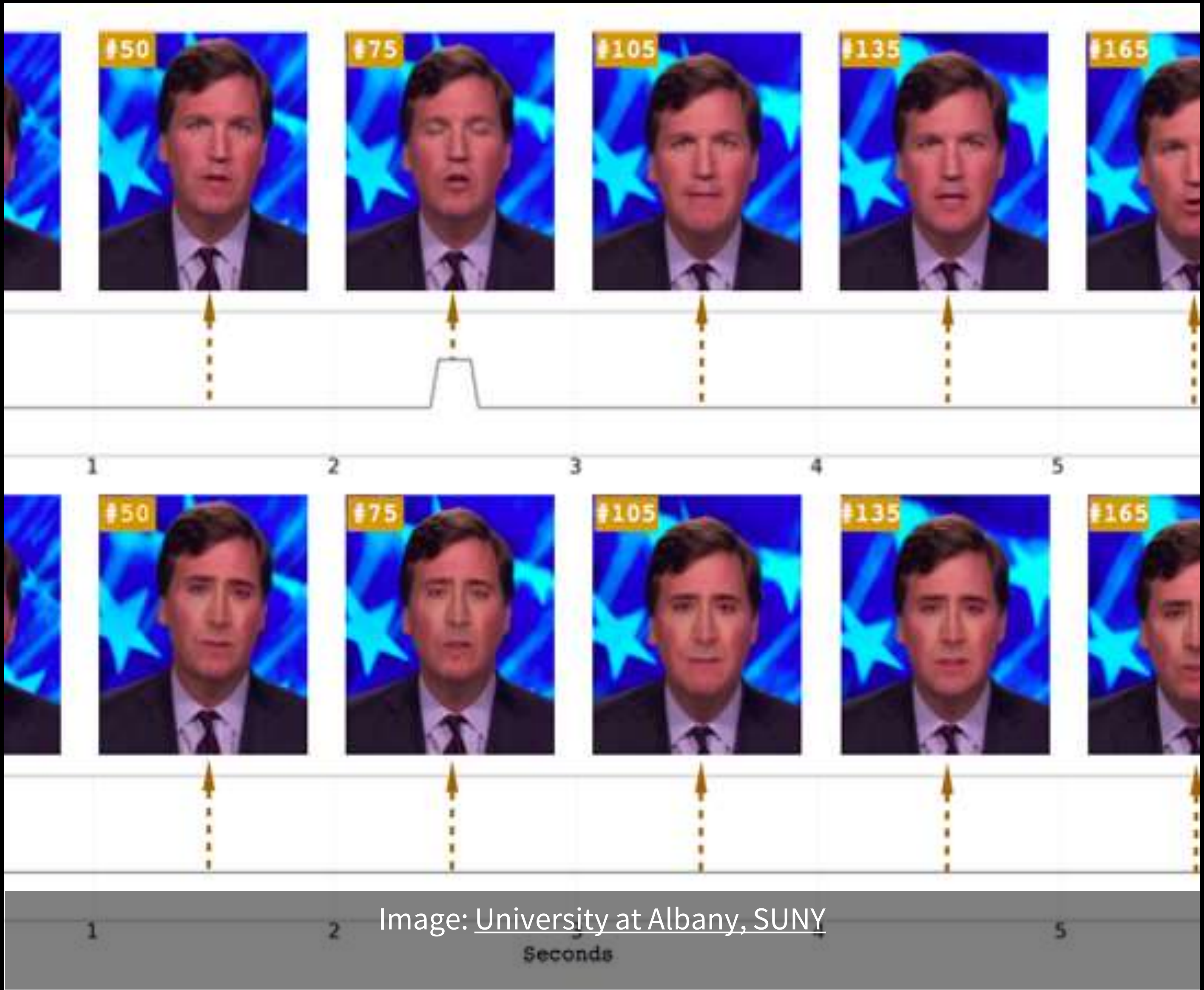


Image: University at Albany, SUNY

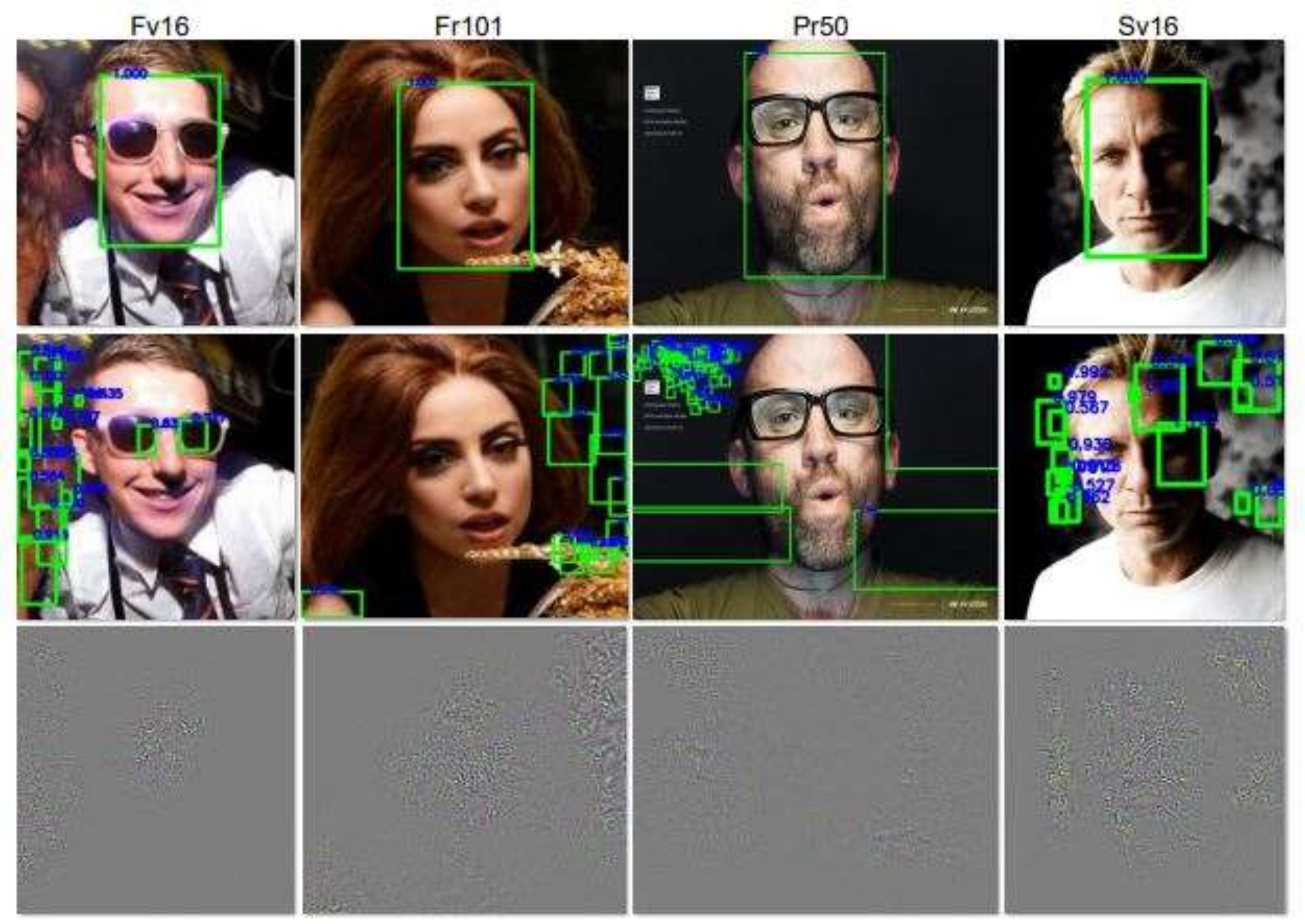
In The Blink of an Eye...

Warping Reality…

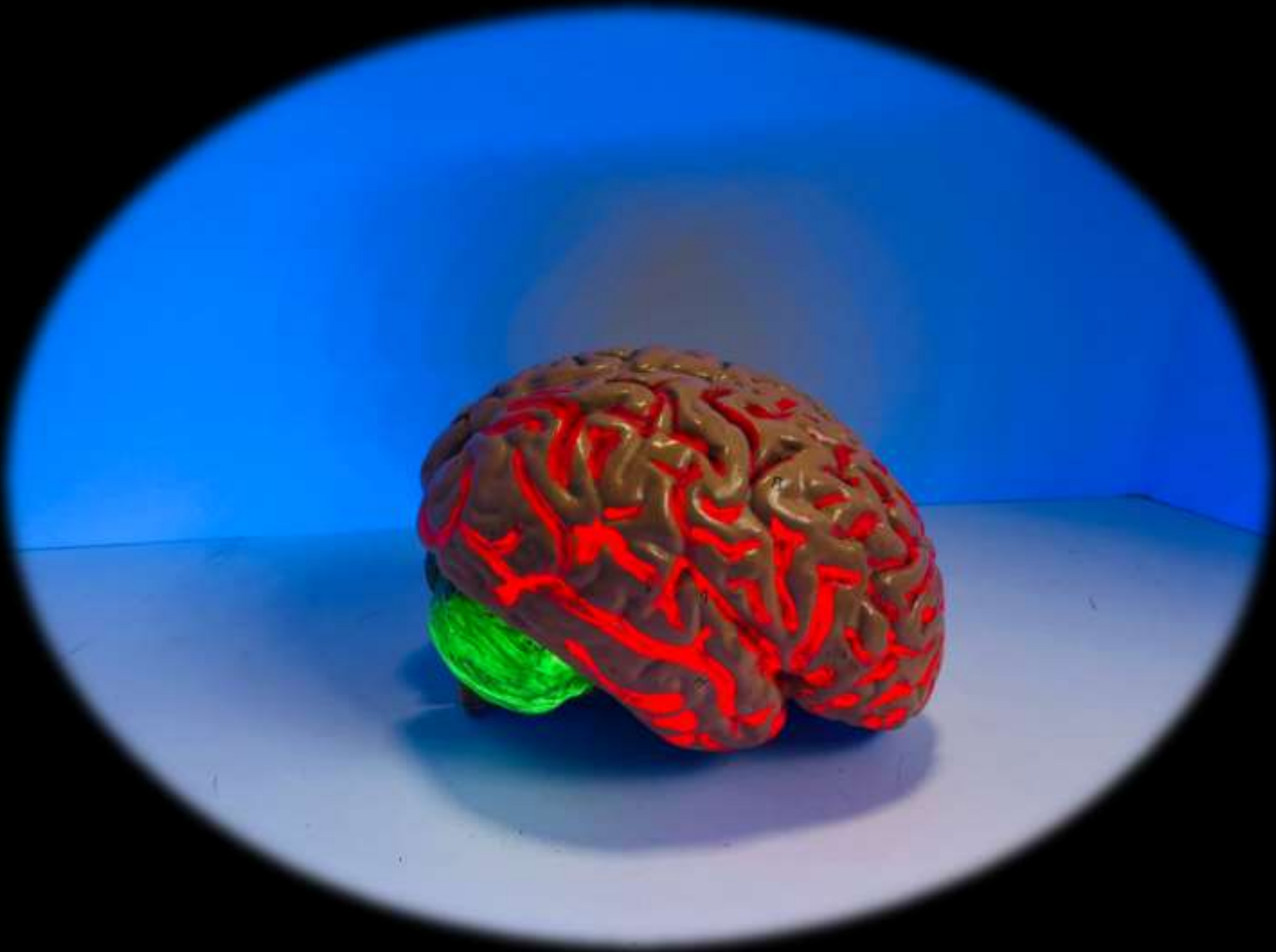
Modeling Behaviors…

Certifying Originals…

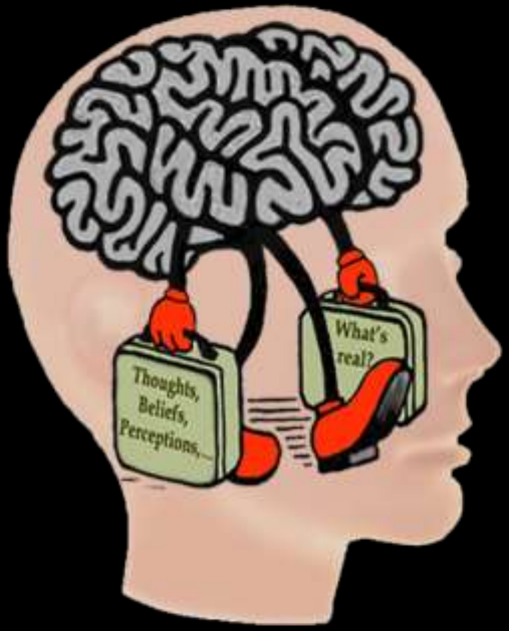
An Ounce of Prevention…

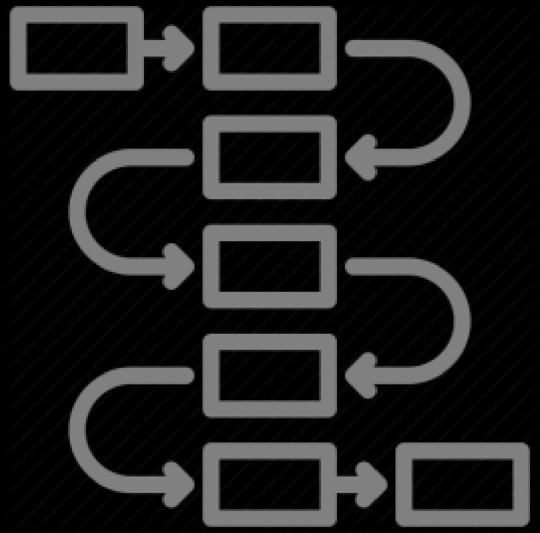


Misinformation is a Human Problem

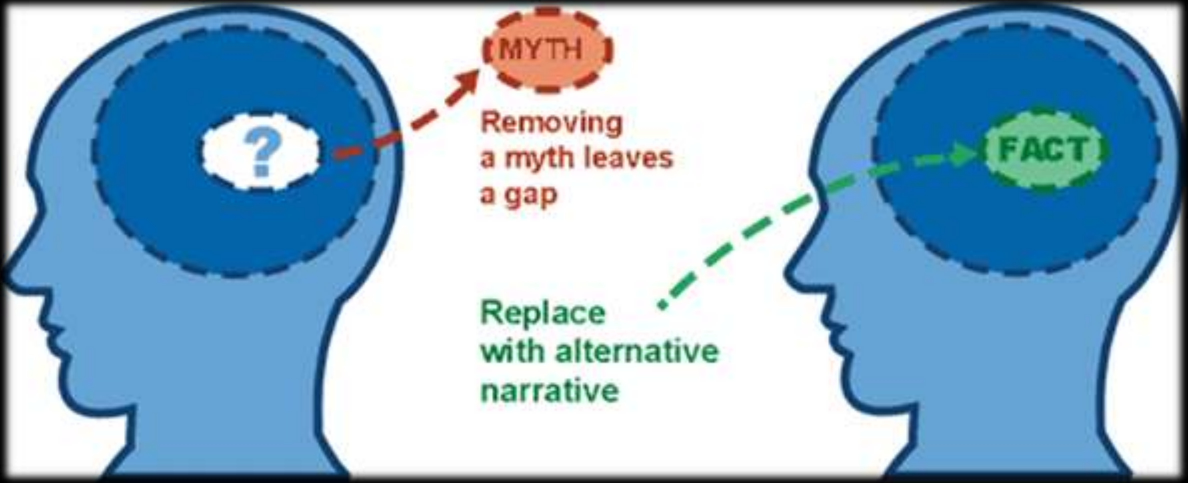


It’s So Sticky…





Debunking Misinformation…



Removing a myth leaves a gap

Replace with alternative narrative

Positive Intentions…

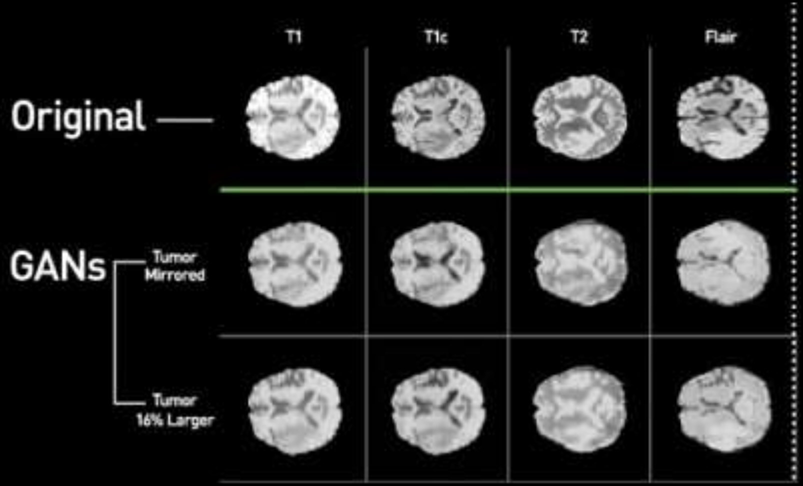


Image: Courtesy Shin et al.

"What it basically means is: to change the perception of reality of every [person] to such an extent that despite of the abundance of information no one is able to come to sensible conclusions in the interest of defending themselves, their families, their community, and their country.“

-Yuri Bezmenov (former KGB)

#ProjectDeepfake…

Example on YouTube
https://www.youtube.com/watch?v=iUOoApdY0lM

Follow on LinkedIn
https://www.linkedin.com/feed/hashtag/projectdeepfake/

Follow on Twitter
https://twitter.com/search?q=%23ProjectDeepfake

References…

Misinformation and its Correction
https://www.researchgate.net/publication/277816966_Misinformation_and_its_Correction

Detecting Deepfakes by Looking Closely…
https://phys.org/news/2019-06-deepfakes-reveals.html

In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking
https://arxiv.org/pdf/1806.02877.pdf

Exposing DeepFake Videos By Detecting Face Warping Artifacts
https://arxiv.org/pdf/1811.00656.pdf

Protecting World Leaders Against Deep Fakes
http://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Agarwal_Protecting_World_Leaders_Against_Deep_Fakes_CVPRW_2019_paper.pdf

Hiding Faces in Plain Sight: Disrupting AI Face Synthesis with Adversarial Perturbations
https://arxiv.org/pdf/1906.09288.pdf

@AlyssaM_Infosec

/in/alyssam-infosec

https://alyssasec.com

Thank You

Alyssa
MILLER

snyk