# Impact of AI Decal:
## *Artificially Generated Data*

Gokul Swamy, Brenton Chu,
and Angelina Wang
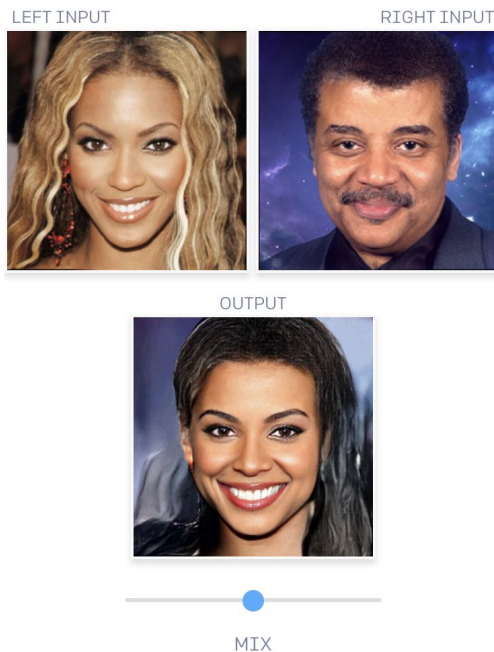
Quiz: https://tinyurl.com/impactsp19q7
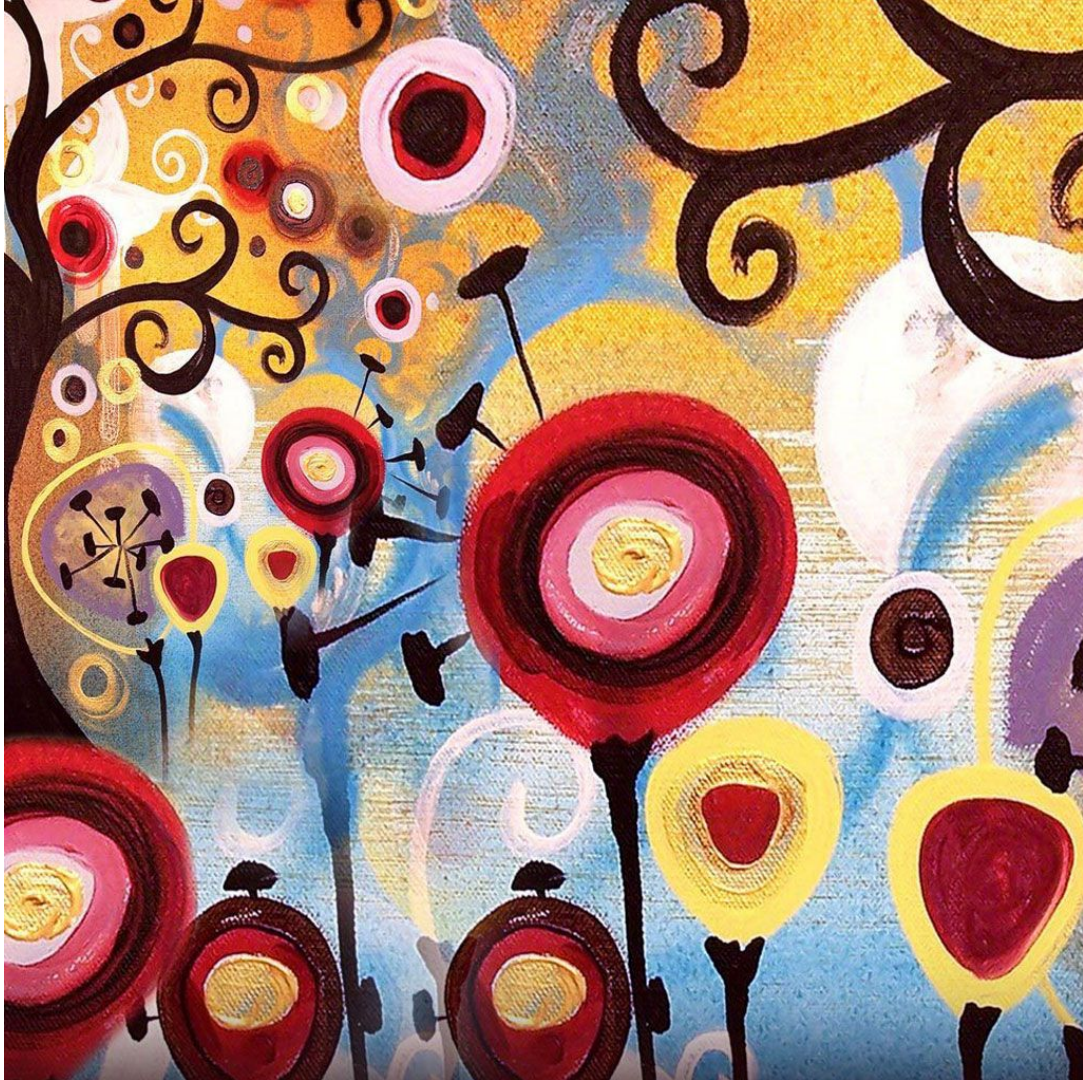
# Glow: another kind of generative model

➔ Faces: https://openai.com/blog/glow/

# Scaling this up

➔ https://thispersondoesnotexist.com/
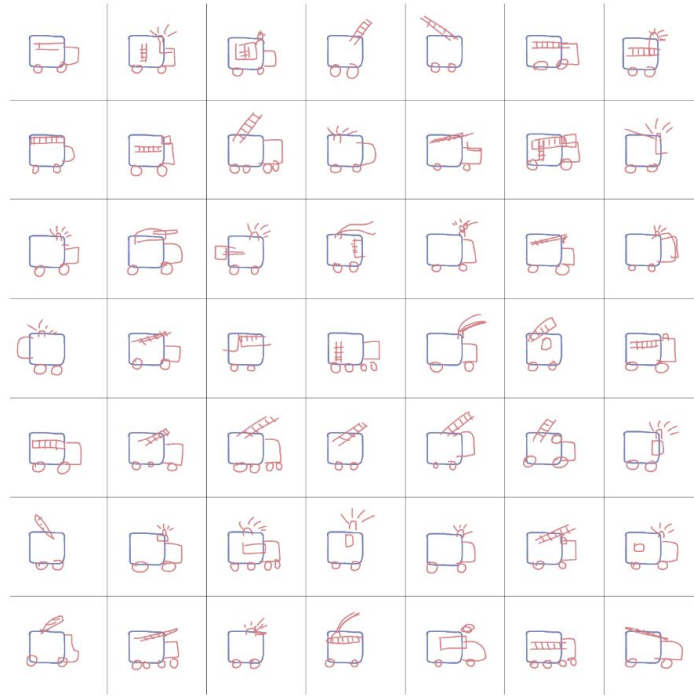
# Sketch RNN



*This is my firetruck. There are many like it, but this one is mine.*

https://magenta.tensorflow.org/assets/sketch_rnn_demo/index.html

# More Examples (Text/Audio)

➔ Music: https://magenta.tensorflow.org/music-transformer
➔ Google Duplex:
https://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html
➔ GPT2: https://gpt2.apps.allenai.org/?text=Joel%20is

# GAN Analogy
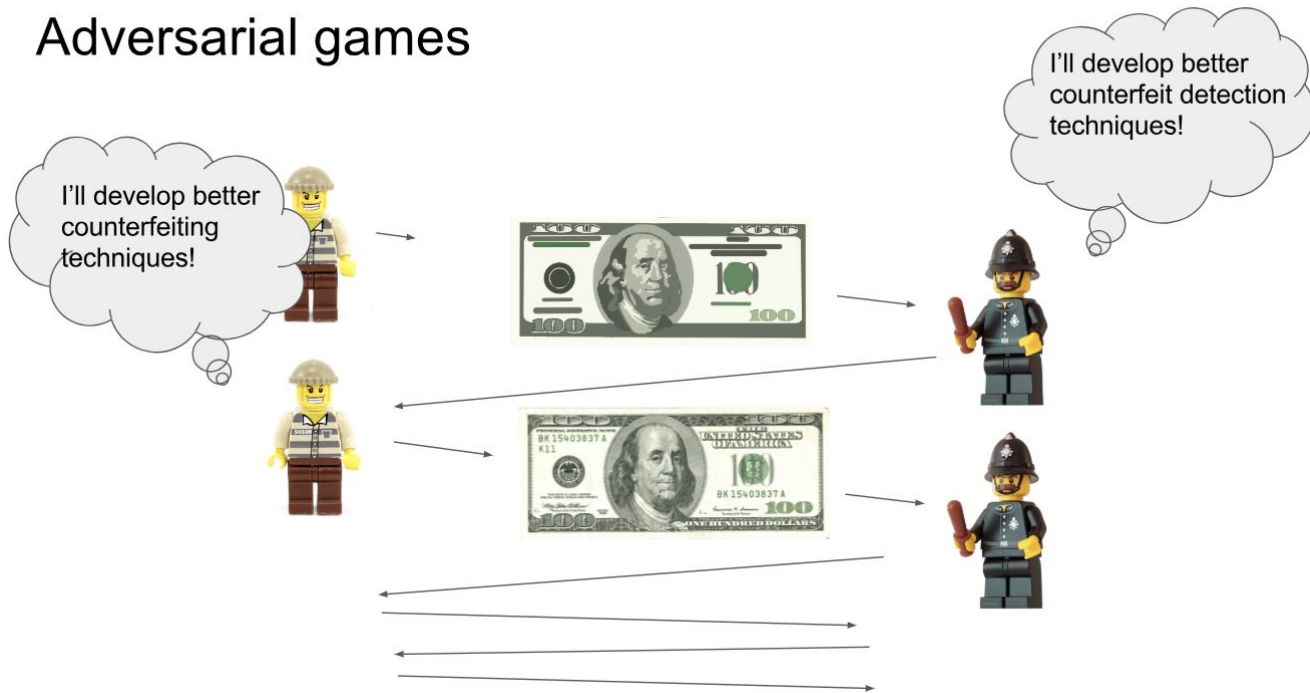
# Generative Adversarial Networks

Source Video

Detected Pose

Source to Target 1 Result

Source to Target 2 Result
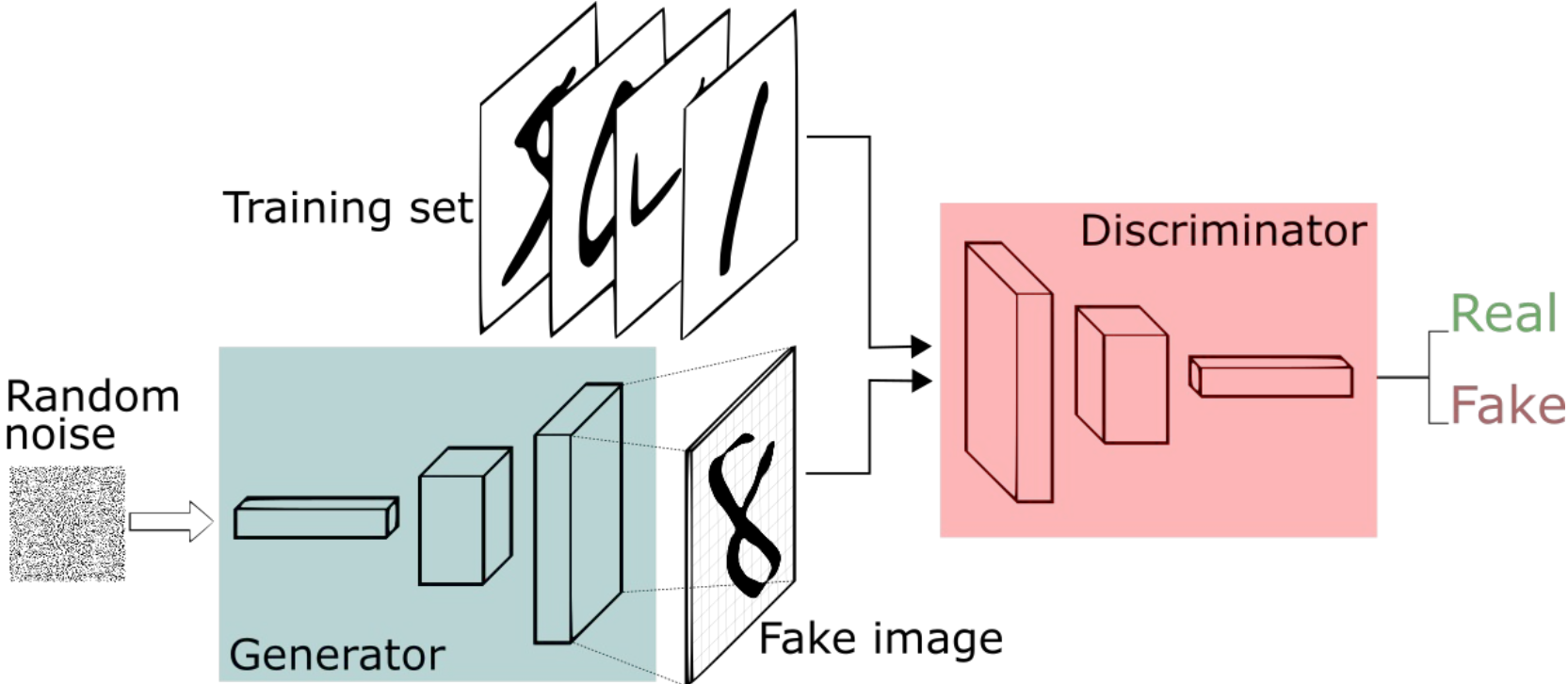
# CycleGAN

➔ Learn both forward and inverse mapping to leverage reconstruction signal.
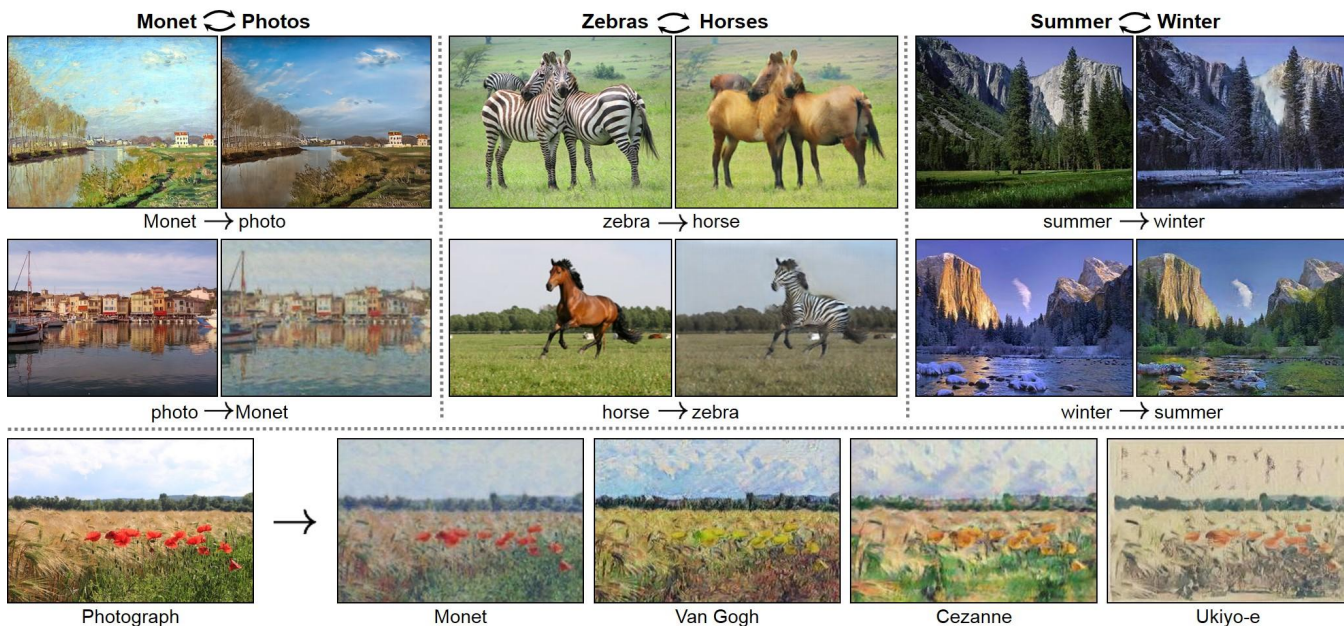
**Q:**

*In what applications can artificially generated data help us, both now and in the future?*

# Potential Applications of Generated Data

➜ Creative pursuits
- ◆ Art, sketching
- ◆ Films and animation
- ◆ Generating captions for videos

➜ Task planning

➜ Generating data for training algorithms
- ◆ Generating footage for self-driving cars
- ◆ Generating fake user profiles to not compromise actual data

# Planning Tasks With Generations
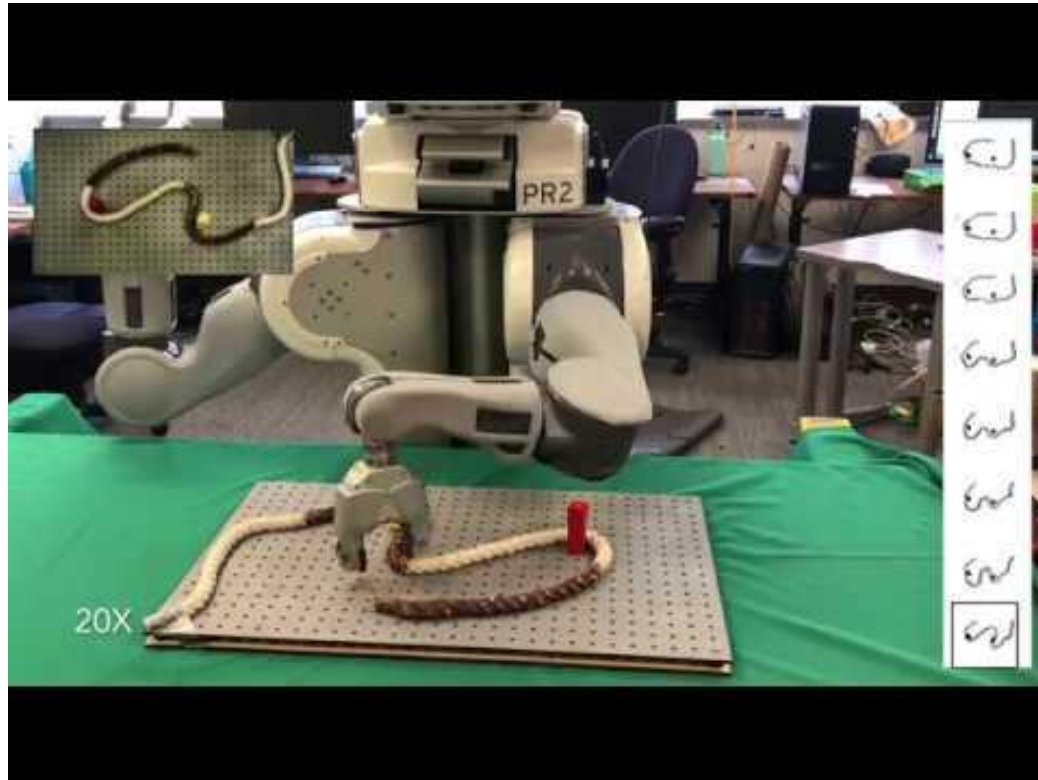
**Q:**

*What are some consequences of being able to generate realistic artificial data?*

# Legal Implications of Deep Fakes

➔ An adversary could make fake videos of a person doing something illegal and then blackmail the party
   ◆ Even if false, like "shouting fire in a crowded theatre"
➔ Fake news could be far more convincing with conflicting stories implanted
   ◆ Leads to less public trust in the fourth estate
➔ Confirmation bias: humans are more likely to believe things that agree with views they already hold
   ◆ If we can't trust data, we might be more willing to ignore evidence that conflicts what we want to believe

# Societal Implications of Deep Fakes (1)

➔ Fake election news like the Pope endorsing candidate Trump received more impressions than real election news

**Total Facebook Engagements for Top 20 Election Stories**

MAINSTREAM NEWS

FAKE NEWS

8.7 million

7.3 million

15 million
12 million
9 millon
6 million
3 millon

Feb.–April     May–July     Aug—Election Day

ENGAGEMENT REFERS TO THE TOTAL NUMBER OF SHARES, REACTIONS, AND COMMENTS FOR A PIECE OF CONTENT ON FACEBOOK SOURCE: FACEBOOK DATA VIA BUZZSUMO
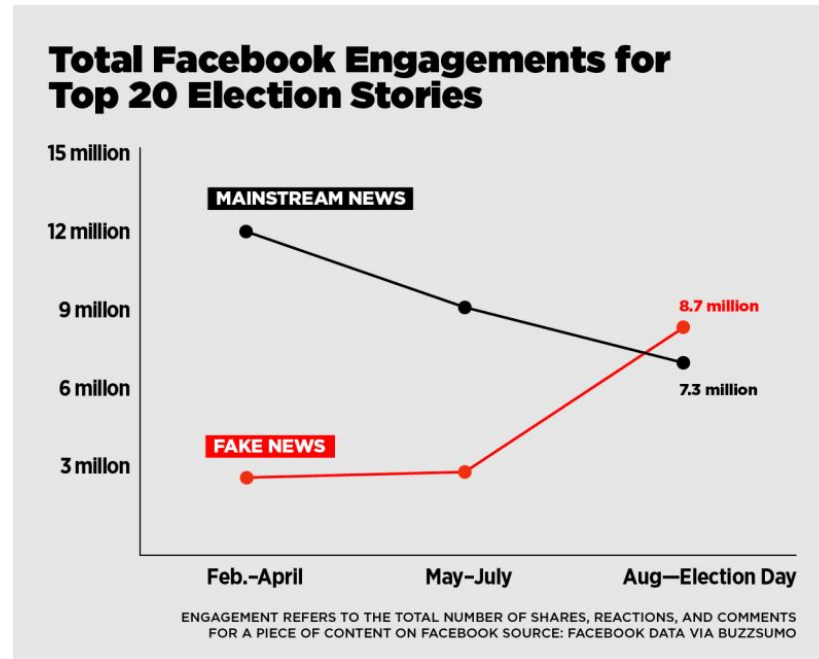
# Potential Legislation (1)

➔ https://www.theregister.co.uk/2018/06/12/new_york_state_is_trying_to_ban_deepfakes_and_hollywood_isnt_happy/

**Emergent Tech**

# New York State is trying to ban 'deepfakes' and Hollywood isn't happy

Disney and NBCUniversal say the new bill is potentially unconstitutional

# Potential Legislation (2)

➔ https://www.congress.gov/bill/115th-congress/senate-bill/3805/text?

**S.3805 - Malicious Deep Fake Prohibition Act of 2018**
115th Congress (2017-2018)

**BILL**    Hide Overview ✖

**Sponsor:**   Sen. Sasse, Ben [R-NE] (Introduced 12/21/2018)

**Committees:**   Senate - Judiciary

**Latest Action:**   Senate - 12/21/2018 Read twice and referred to the Committee on the Judiciary. (All Actions)
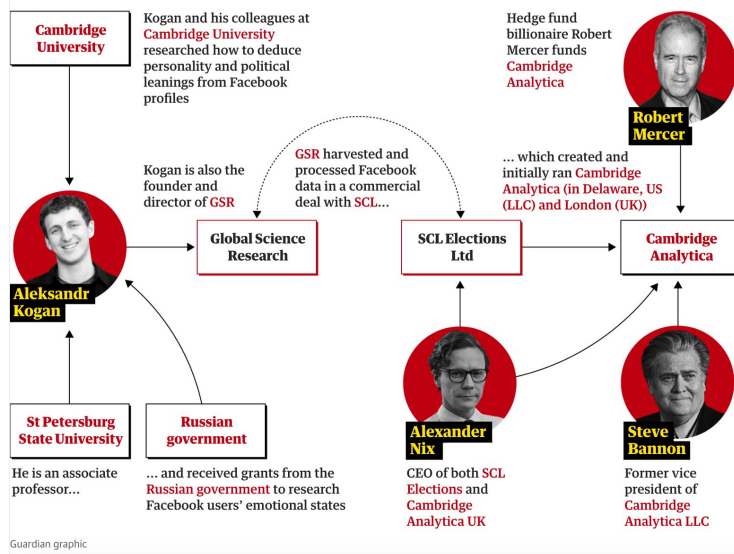
**Tracker:**

Introduced

# Ad Targeting + Deep Fakes

➔  Concerns that GPT2 can be used to generate realistic text
➔  This can be combined with ad targeting to manipulate public opinion.

**Cambridge Analytica: how the key players are linked**



Kogan and his colleagues at Cambridge University researched how to deduce personality and political leanings from Facebook profiles

Hedge fund billionaire Robert Mercer funds Cambridge Analytica

GSR harvested and processed Facebook data in a commercial deal with SCL…

… which created and initially ran Cambridge Analytica (in Delaware, US (LLC) and London (UK))

Kogan is also the founder and director of GSR

He is an associate professor…

… and received grants from the Russian government to research Facebook users' emotional states

CEO of both SCL Elections and Cambridge Analytica UK

Former vice president of Cambridge Analytica LLC

Cambridge University · Robert Mercer · Global Science Research · SCL Elections Ltd · Cambridge Analytica · Aleksandr Kogan · St Petersburg State University · Russian government · Alexander Nix · Steve Bannon

Guardian graphic

# Forgery Detection Models

➔ Cat-and-mouse game just like other parts of cybersecurity
➔ We can use the discriminator part of the GAN to counter the deep fakes created by the generator

# Impact of AI Decal:
*Activity*

# Activity

➔ We're going to try and determine which of the following is real and which is artificially generated
- ◆ Try and define a strategy for differentiating
➔ Split into teams and vote

# Comparison 1

# Comparison 2

# Comparison 3

President Barack Obama launched a new round of airstrikes against Islamic State in Iraq and Syria (ISIS) on Tuesday, killing at least 30 ISIS fighters and wounding more than 100 others.

The Obama administration has been bombing ISIS targets in Iraq and Syria since late last year, but the U.S. has been unable to strike the group's stronghold of Raqqa, Syria, since the group's advance into the city in June.

President Obama on Thursday announced he had authorized limited airstrikes against Islamic militants in Iraq, scrambling to avert the fall of the Kurdish capital, Erbil, and returning the United States to a significant battlefield role in Iraq for the first time since the last American soldier left the country at the end of 2011.

Speaking at the White House on Thursday night, Mr. Obama also said that American military aircraft had dropped food and water to tens of thousands of Iraqis trapped on a barren mountain range in northwestern Iraq, having fled the militants, from the Islamic State of Iraq and Syria, who threaten them with what Mr. Obama called "genocide."

# Comparison 4

→ [Option 1](#)                    → [Option 2](#)

REAL

# Comparison 5

→ [Option 1](#)

→ [Option 2](#)

REAL

# Impact of AI Decal:

*Next: Bias in AI*