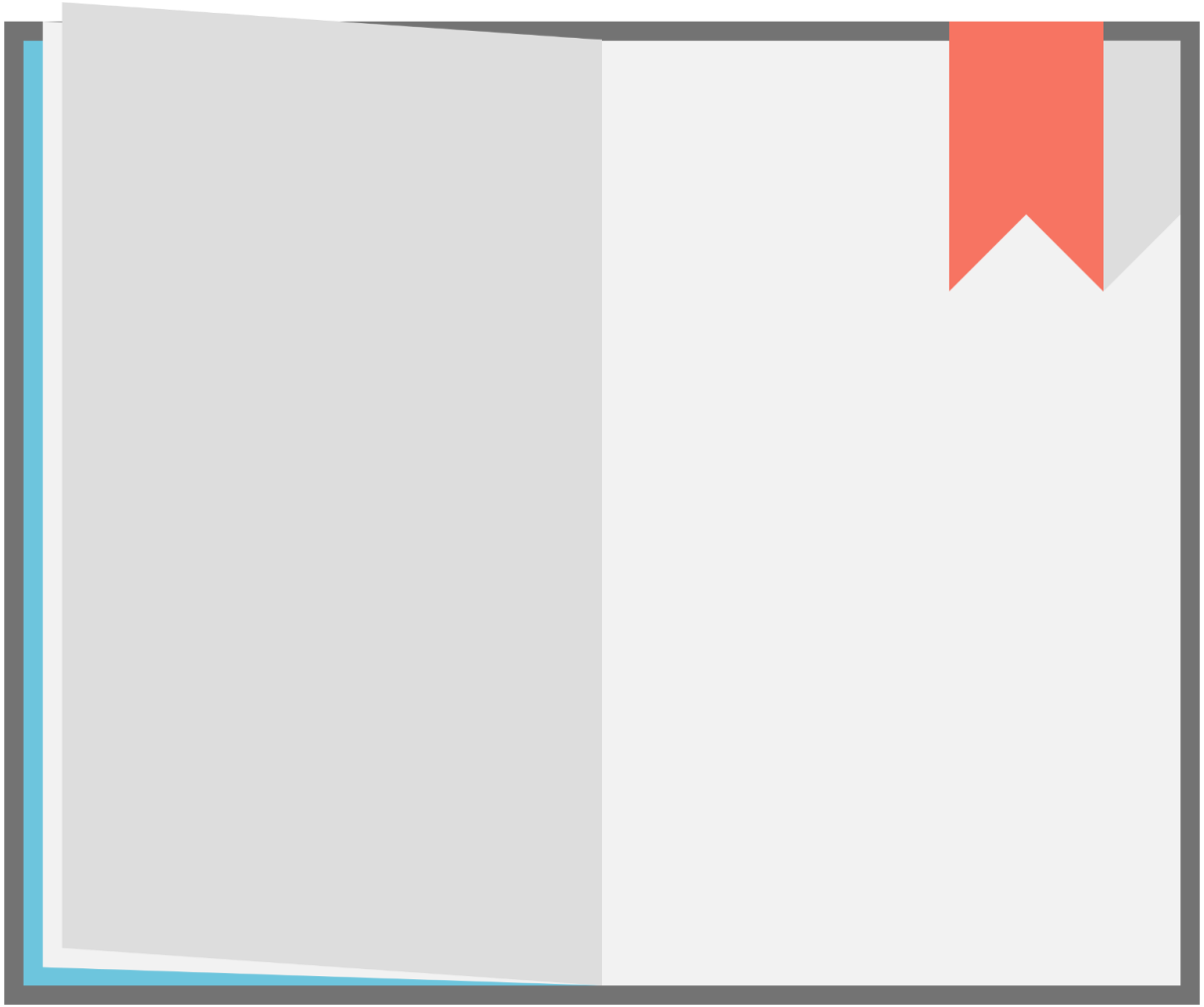
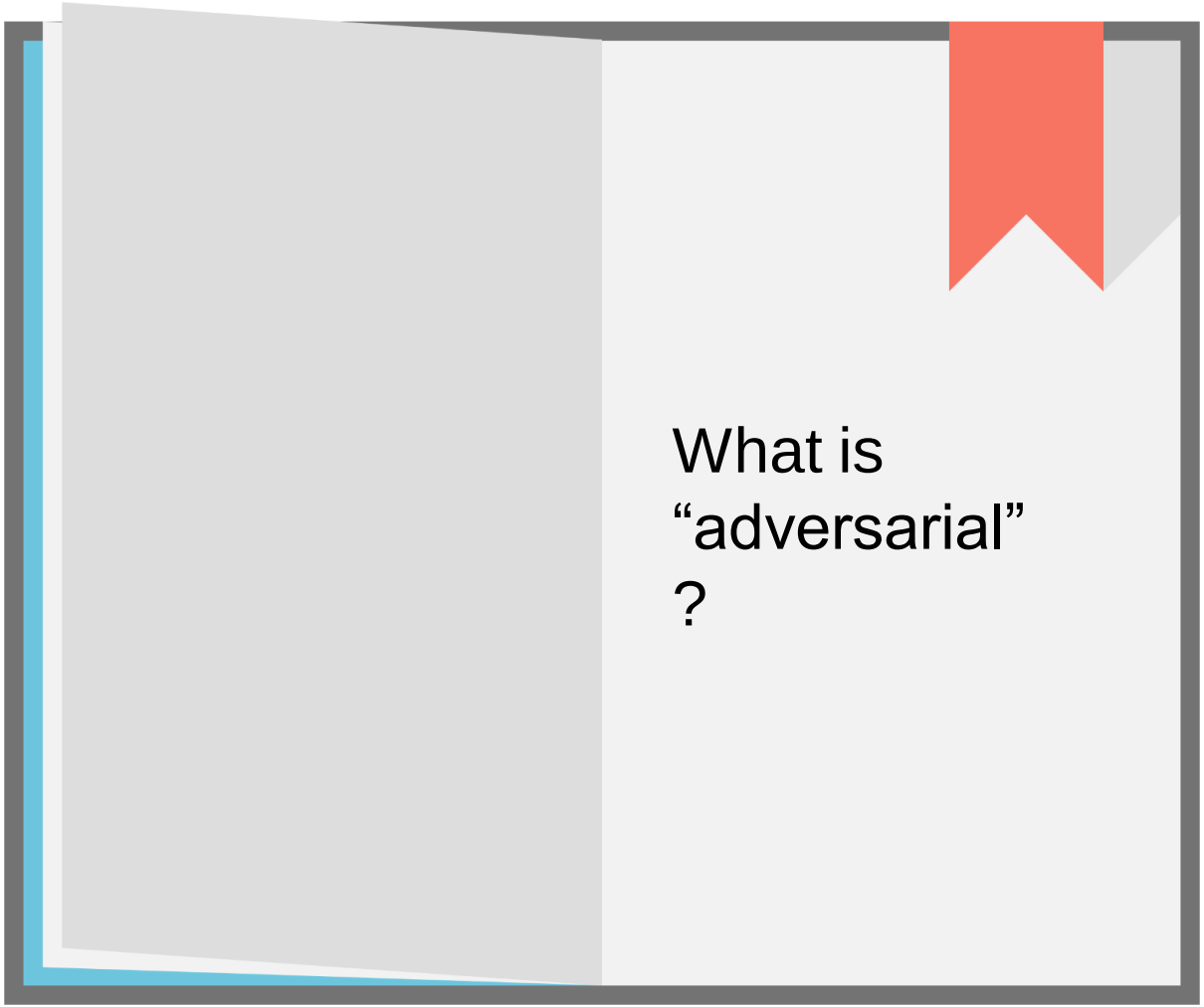
New views on multimedia data

Privacy and other reasons for research on data minimization

Martha Larson
MMM 2019 25th International Conference on MultiMedia Modeling
Thessaloniki, Greece, Friday, January 11th, 2019



https://openclipart.org/detail/182527/open-book



https://openclipart.org/detail/182527/open-book

“Adversarial”: two contexts in machine learning

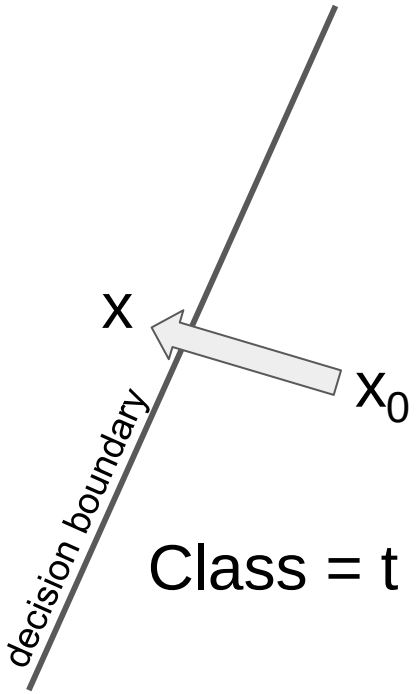
Generative Adversarial Network (GAN)	**Adversarial Example**
Network that learns by attempting to outsmart another network.	Example that surprises us because it gets misclassified.

How to generate adversarial examples

Constraint optimization

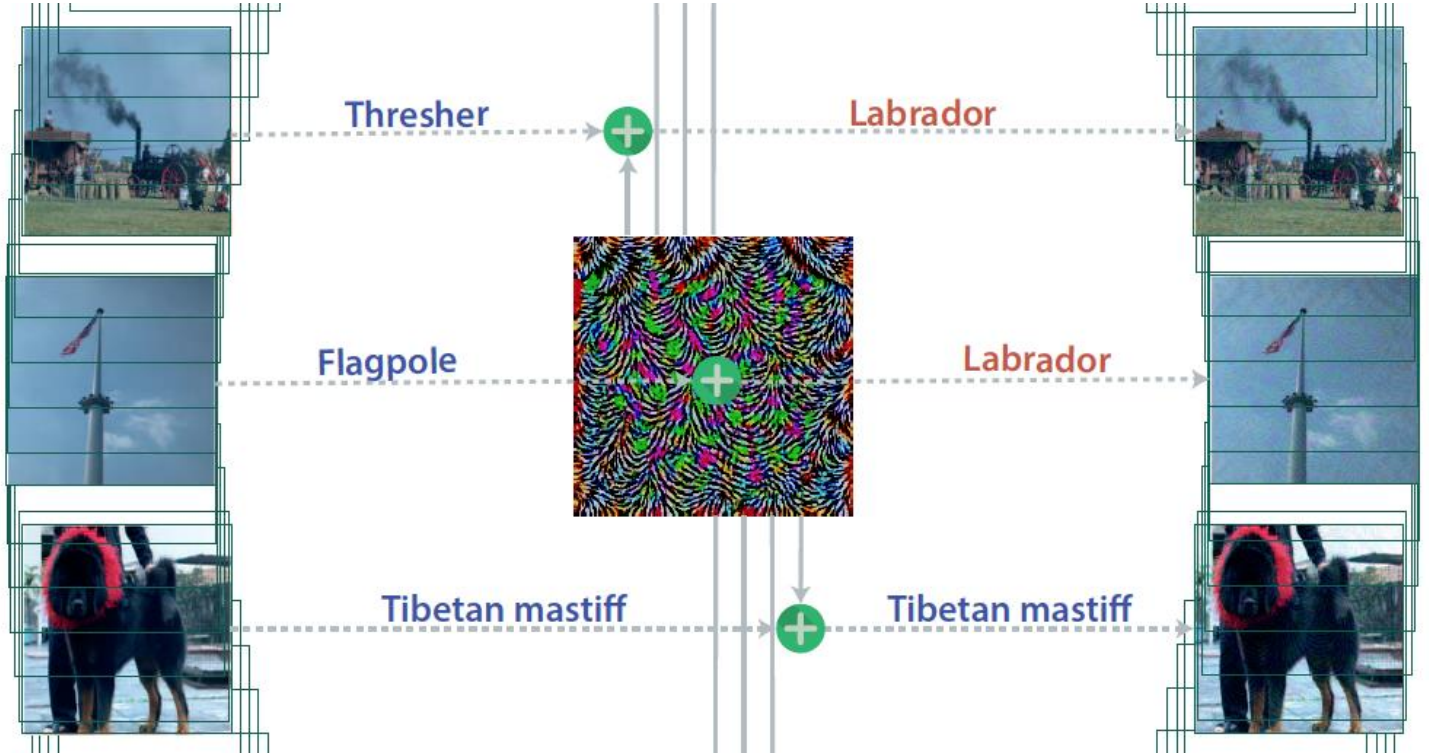
$$\begin{aligned} \text{minimize} \quad & \|x_0 - x\|_2^2 \\ \text{such that} \quad & C(x) \neq \mathrm{t} \end{aligned}$$

where t is the label of x_0.



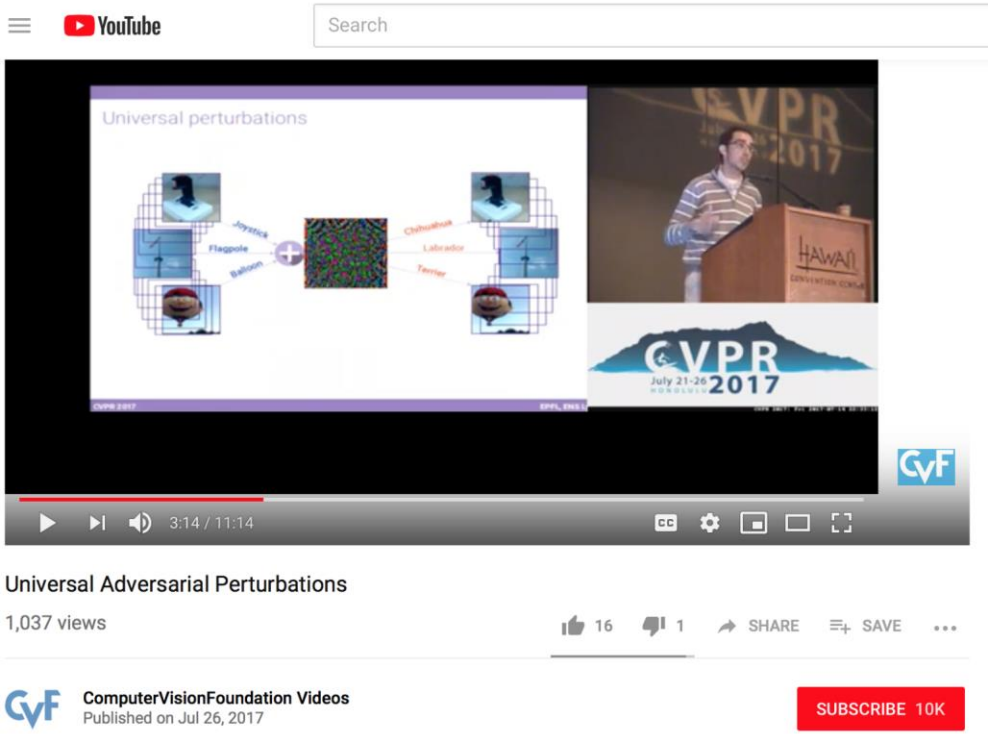
Christian Szegedy et al. “Intriguing properties of neural networks”. Conference on Learning Representations. 2014.

Universal Adversarial Perturbations



Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, Omar Fawzi, and Pascal Frossard. 2017. Universal adversarial perturbations. CVPR 2017.

Universal Adversarial Perturbations



Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, Omar Fawzi, and Pascal Frossard. 2017. Universal adversarial perturbations. CVPR 2017.

“Adversarial examples” are not inherently bad, they may help us by minimizing information.

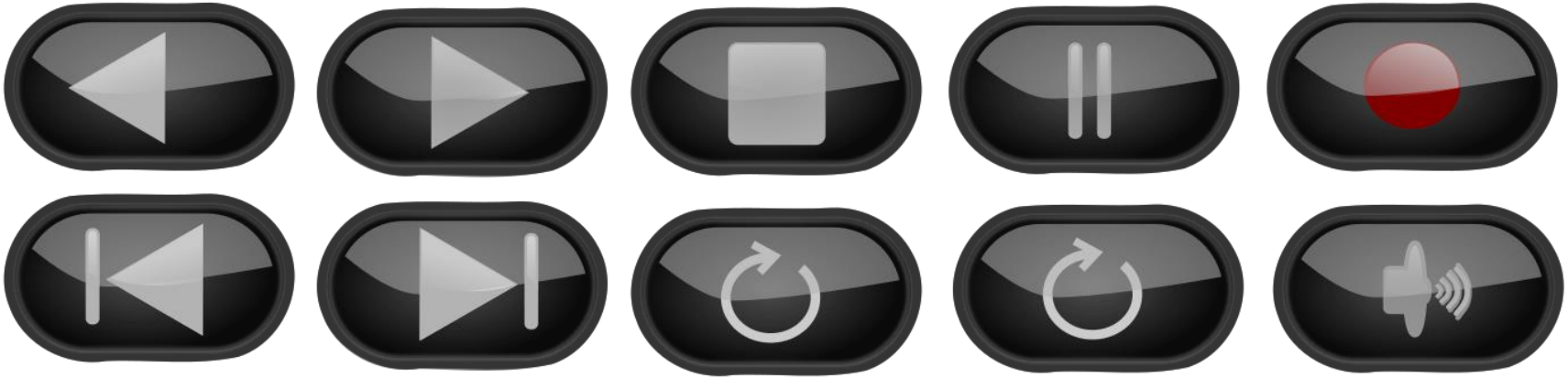
Take home message

Take home message

As multimedia researchers:

- Let’s use only what’s essential.
- Let’s help people produce only what’s essential.

What is multimedia?



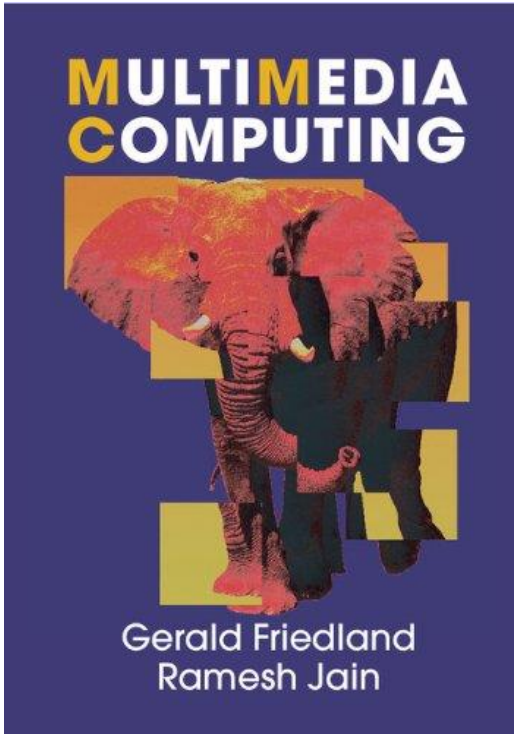
https://openclipart.org/detail/75337/multimedia-buttons

Multimedia

Multimedia is content that:

- Comprises more than one modality. (Modalities include: audio, video, images, text, and metadata, such as geo-location.)
- The modalities are complementary. Together, they contain complete information.

The elephant



The modalities are complementary. Together, they contain complete information.

Friedland, G. and Jain, R. Multimedia Computing. Cambridge University Press. 2014.

multimedia signals

Communication Words Visual content Audio	

Today’s multimedia signals

Communication	**Behavior**
Words Visual content Audio	Views Purchases Location

Today’s multimedia signals

Content	**Context**
Words Visual content Audio	Views Purchases Location

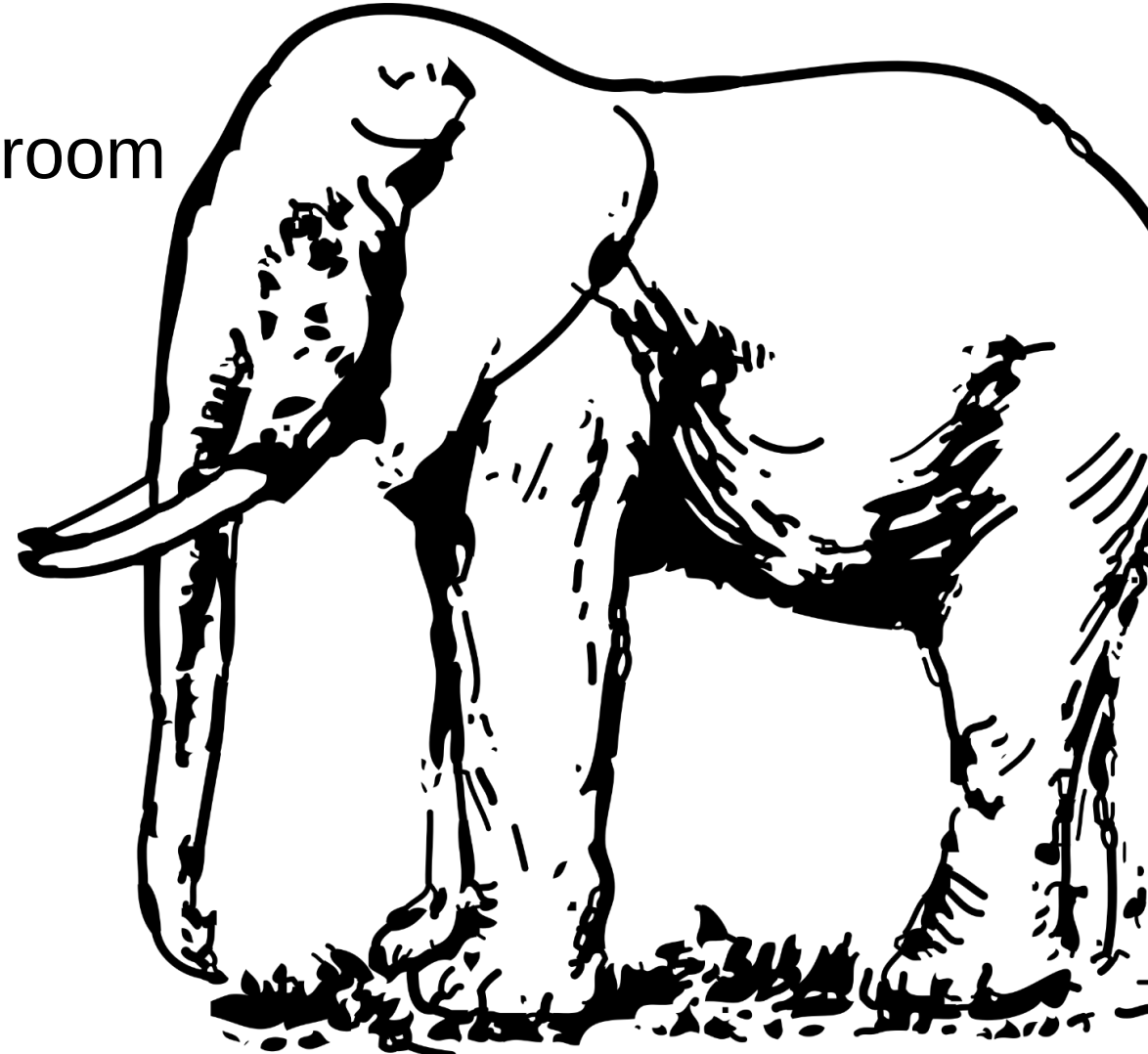
Today’s multimedia signals

Intentional	**Unintentional**
Words Visual content Audio	Views Purchases Location

Today’s multimedia signals

Intentional	**Unintentional**
Words Visual content Audio	Views Purchases Location
User initiates and controls.	*User lacks complete, (conscious) control.*

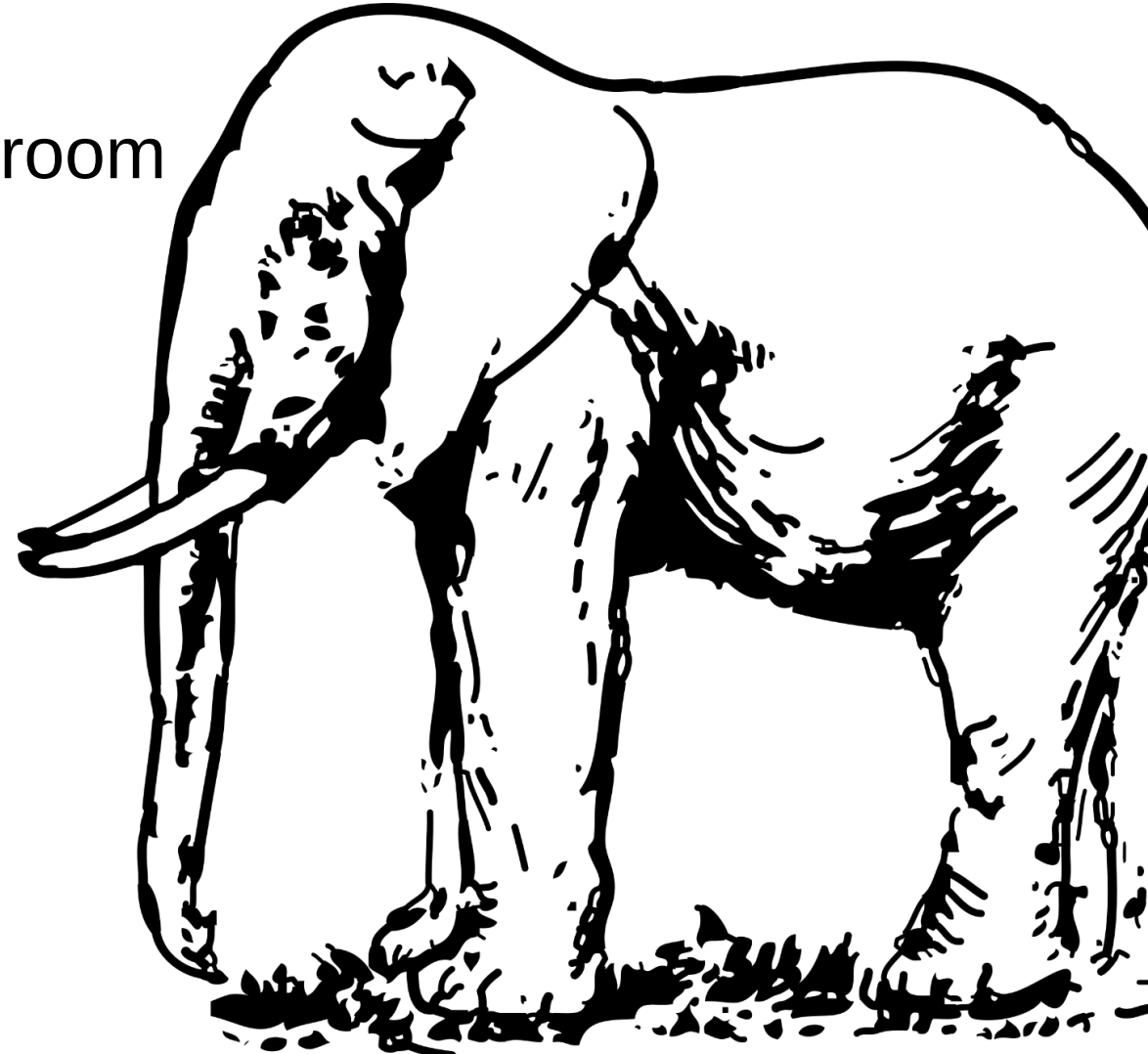
The elephant in the room



https://openclipart.org/detail/7505/elephant

The elephant in the room

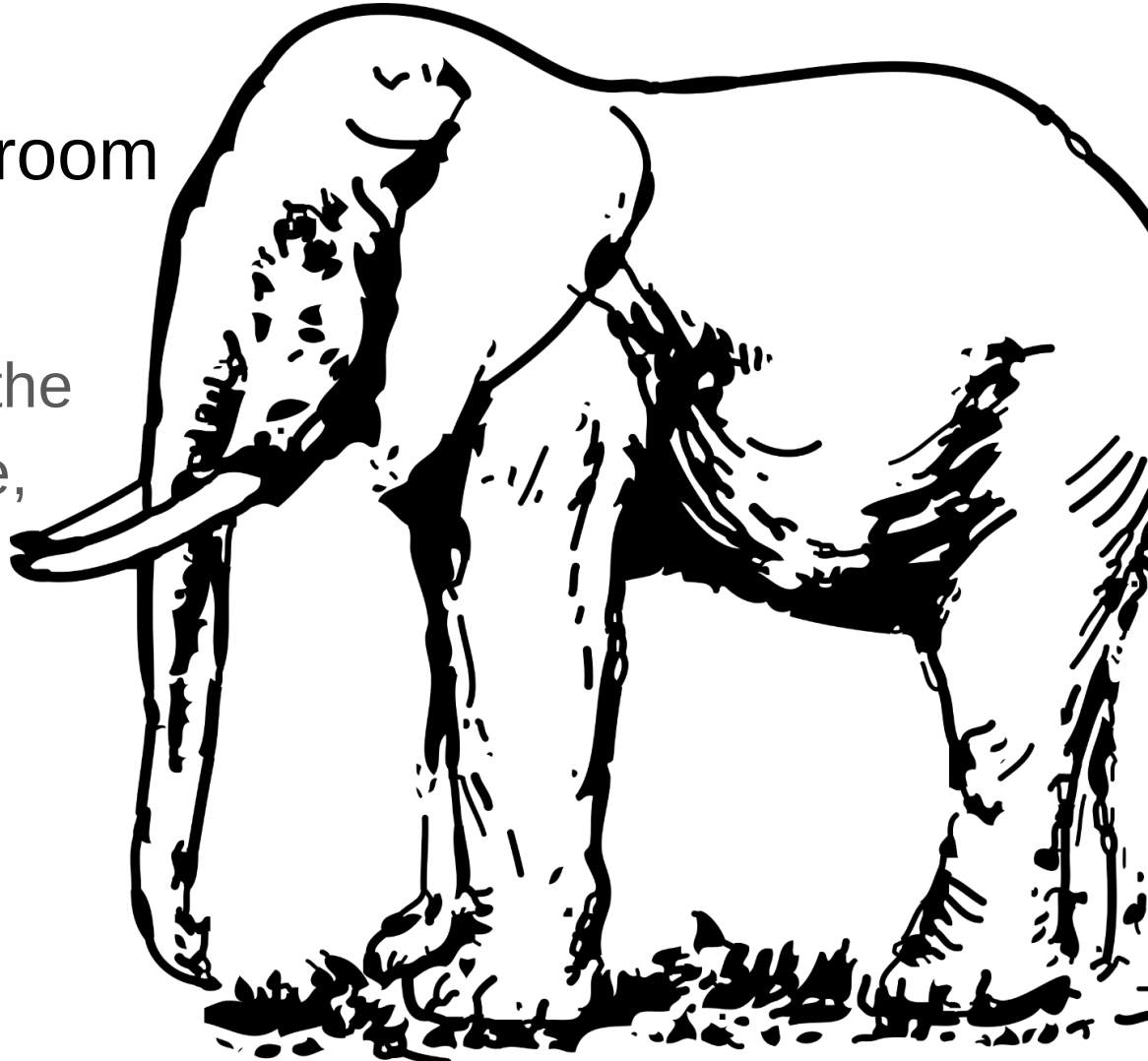
There is no elephant.



https://openclipart.org/detail/7505/elephant

The elephant in the room

If users lack complete conscious control over the signal that they produce, who then decides what constitutes complete information?



https://openclipart.org/detail/7505/elephant

The elephant in the room

There is no elephant.

https://openclipart.org/detail/7505/elephant

Take home message

As multimedia researchers:

- Let’s use only what’s essential.

Reason: We have no principled manner of deciding the relevance of signals that users produced unintentionally.

Take home message

As multimedia researchers:

- Let’s use only what’s essential.

Reason: We have no principled manner of deciding the relevance of signals that users produced unintentionally.

And these signals are dangerous.

Cybercrime
Inside IT

Personal data is as hot as nuclear waste

Cory Doctorow

We should treat personal electronic data with the same care and respect as weapons-grade plutonium - it is dangerous, long-lasting and once it has leaked there's no getting it back

Tuesday 15 January 2008
08.27 EST

Photo: AFP

https://www.theguardian.com/technology/2008/jan/15/data.security

https://openclipart.org/detail/281522/turnstyle

Location is a liability

A log of when and where we board a train reveals:

- When we visit the doctor.
- Who we meet in public spaces.

https://openclipart.org/detail/281522/turnstyle

General Data Protection Regulation (GDPR)

As of May 2018...there is one set of data protection rules for all companies operating in the EU, wherever they are based.

Stronger rules on data protection mean

- people have more control over their personal data
- businesses benefit from a level playing field

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

“Personal Data” and the GDPR

What is personal data?

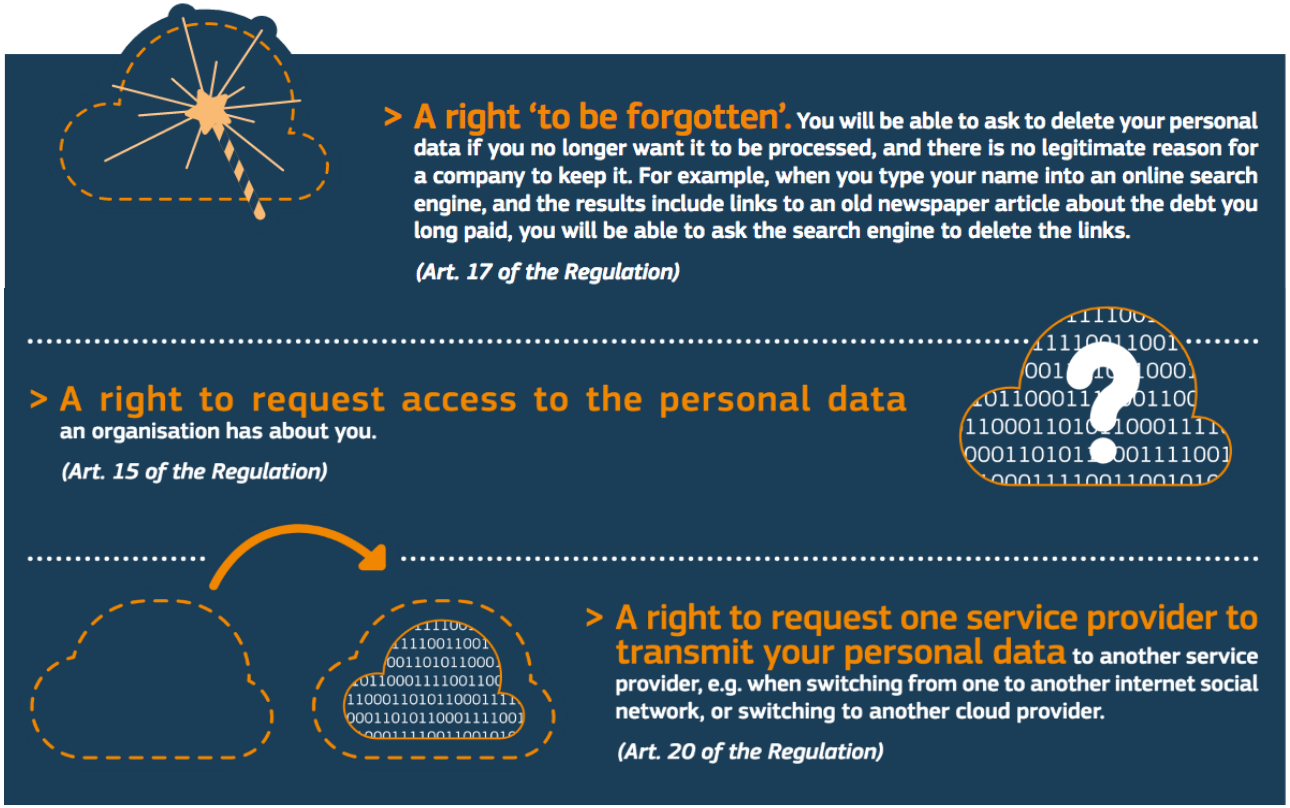
“Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.”

Examples of personal data:

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

Our rights under GDPR (examples)



https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-citizens_en_0.pdf

Privacy

- **Physical privacy**: the state of being free from intrusion into your personal space, including your possessions and your own body.
- **Information privacy**: the state of control over information about you that is collected, stored, processed, or shared.
- **Organization privacy**: the state of secrecy used by companies and governments to hide their activities from competitors and enemies.

Craig, Terence, and Mary Ludloff. Privacy and big data. O'Reilly Media, 2011.

Information privacy is about control

- **Information privacy**: the state of control over information about you that is collected, stored, processed, or shared.

Craig, Terence, and Mary Ludloff. Privacy and big data. O'Reilly Media, 2011.

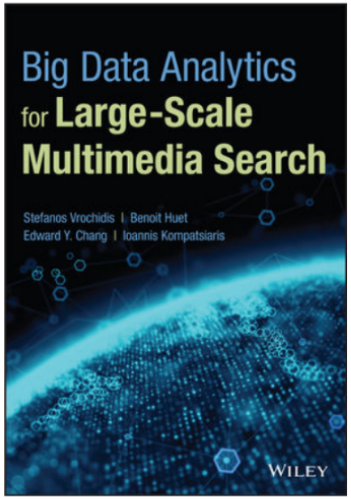
Take home message

As multimedia researchers:

- Let’s use only what’s essential.

Reason: Less work to be compatible with European Law.

More on multimedia privacy



Big Data Analytics for Large-Scale Multimedia Search

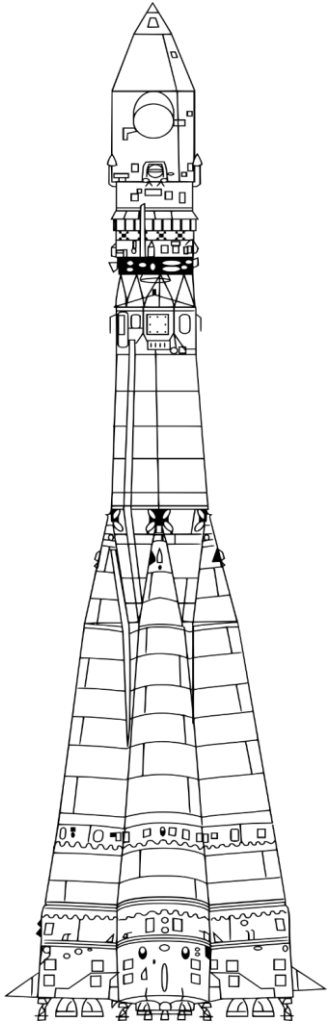
Stefanos Vrochidis, Benoit B. Huet, Edward Y. Chang, Ioannis Kompatsiaris

ISBN: 978-1-119-37697-2 | April 2019 | 408 Pages

Pre-order
HARDCOVER
$130.00

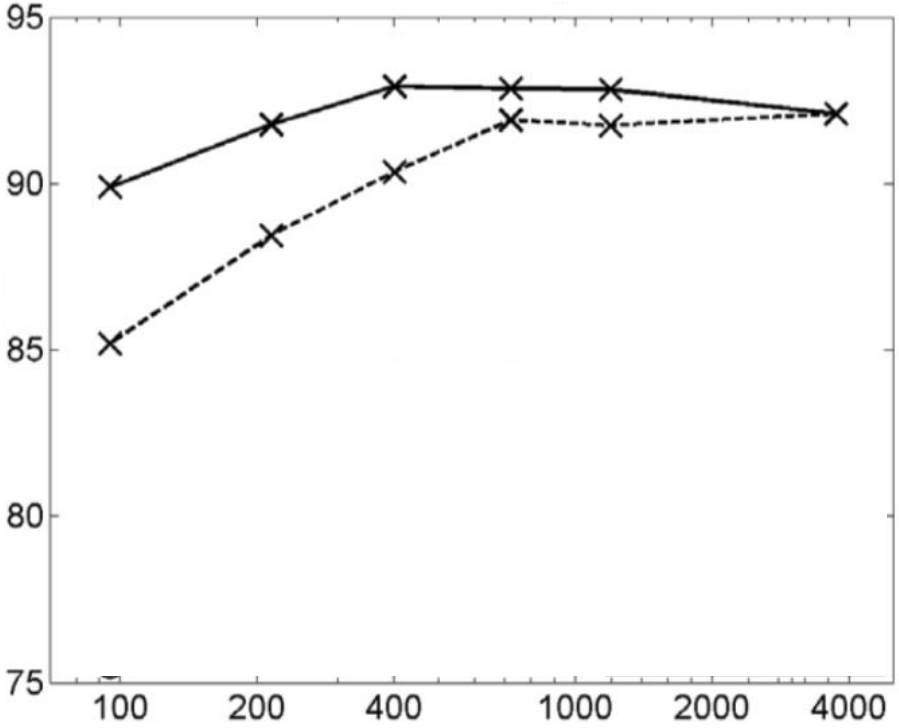
Chapter 7: Privacy and audiovisual content: Protecting users as big multimedia data grows bigger.

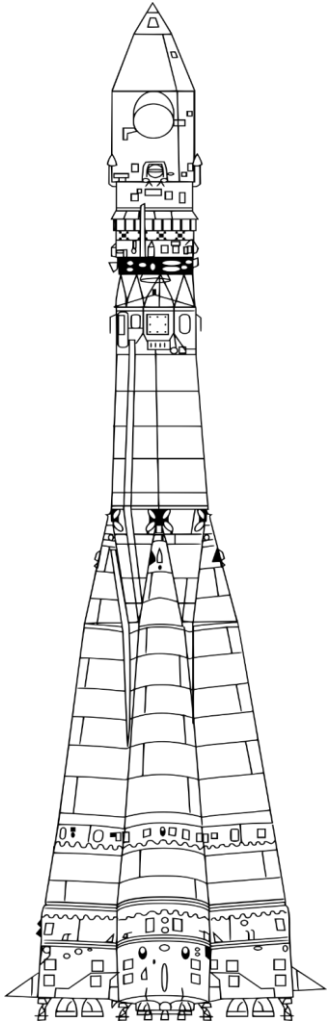
Blast from the past



https://openclipart.org/detail/270554/vostock-rocket

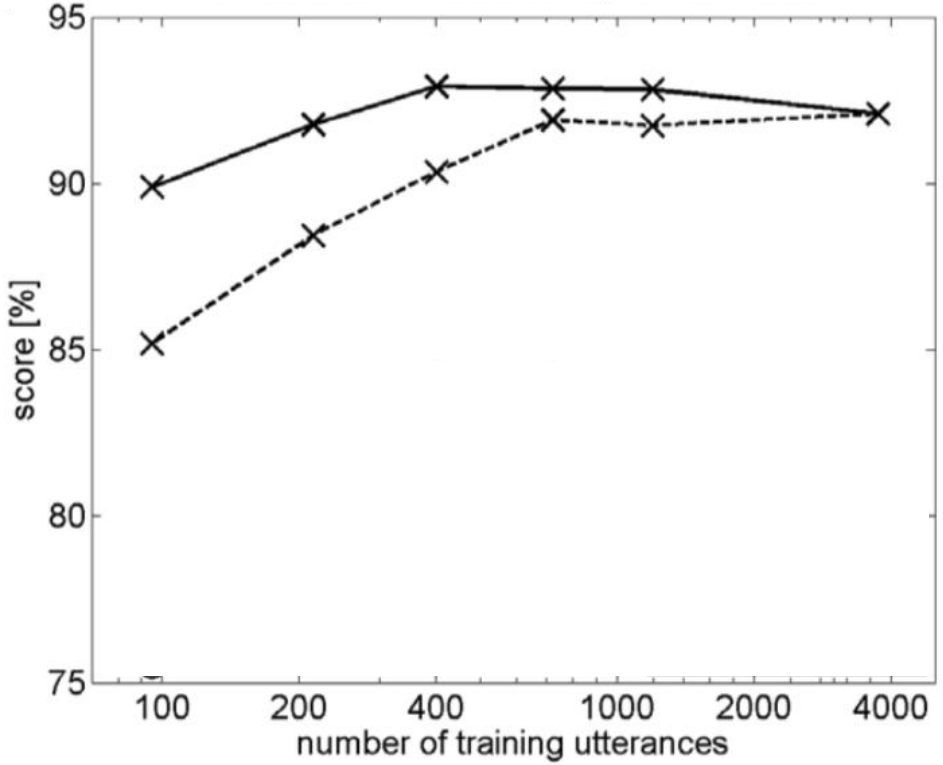
Blast from the past





https://openclipart.org/detail/270554/vostock-rocket

Learning curve

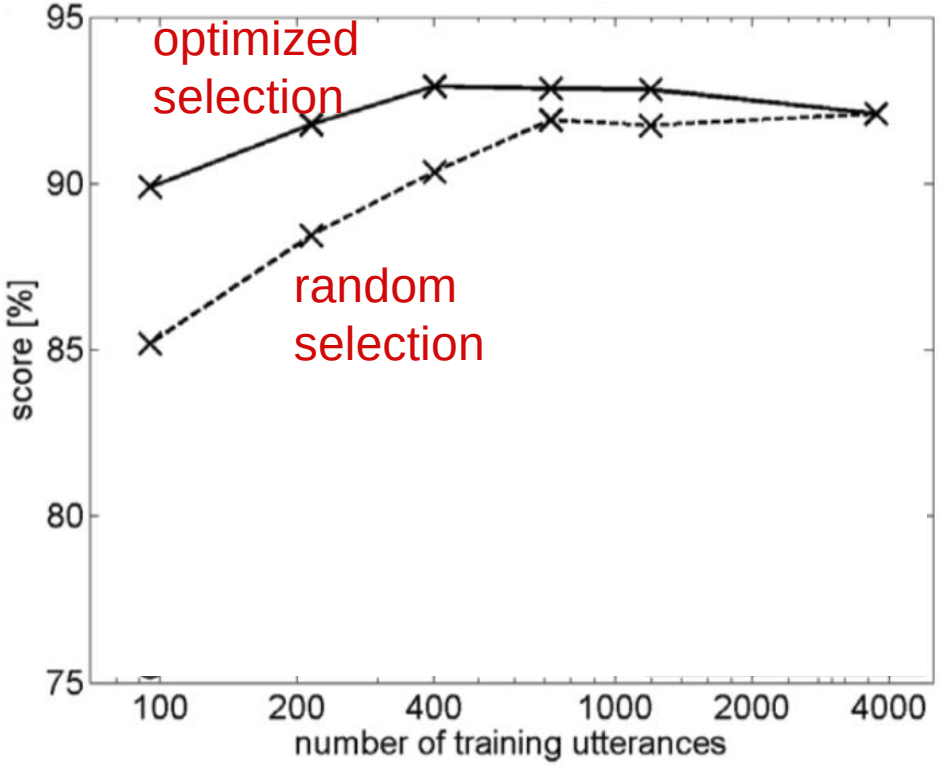


Performance vs. amount of training data.

Here, a speech recognizer is being trained to recognize spoken numbers.

Nagorski, A., Boves, L., Steeneken, H. Optimal Selection of Speech Data for Automatic Speech Recognition Systems. ICSLP 2002.

Optimal selection of data



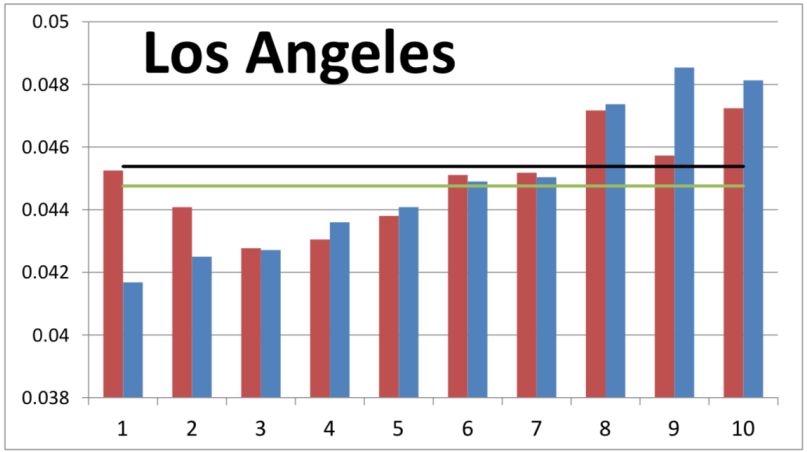
Performance saturates: after a point, more is not better.

The right data: Not all data contributes equally to performance.

Nagorski, A., Boves, L., Steeneken, H. Optimal Selection of Speech Data for Automatic Speech Recognition Systems. ICSLP 2002.

Differential data Analysis

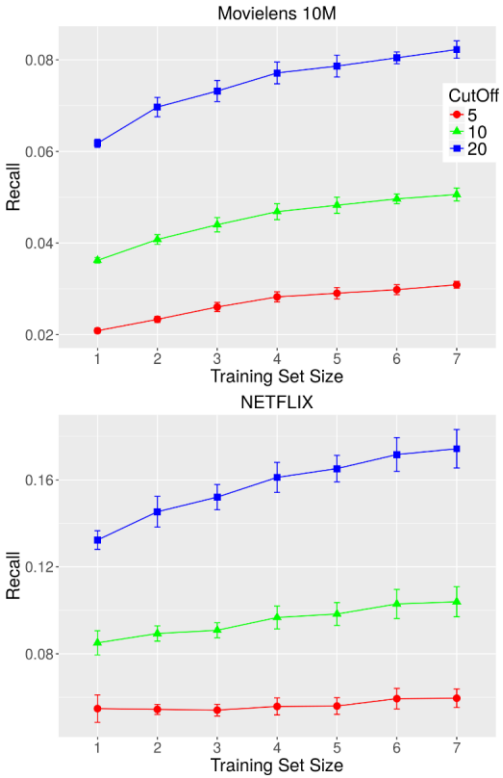
"Is all this data really necessary for making good recommendations?"



- Each bar represents the removal of a different 10% of the data.
- Analysis shows that some removal strategies improve recommendations over using all data (dark horizontal line).

Richard Chow, Hongxia Jin, Bart Knijnenburg, and Gokay Saldamli. 2013. Differential data analysis for recommender systems. ACM RecSys 2013. ("Longplay" arXiv version: https://arxiv.org/pdf/1310.0894.pdf)

Data dropping



- Larger training set size increases storage and computational costs.
- The improvement in the evaluation metric yielded by more data may not impact user experience or the bottom line.
- Adding “stale data” might not actually improve the metric at all.

Larson, M., Zito, A., Loni, B., Cremonesi, P. Towards Minimal Necessary Data: The Case for Analyzing Training Data Requirements of Recommender Algorithms, FATREC’17: Fairness, Accountability and Transparency in Recommender Systems.

Take home message

As multimedia researchers:

- Let’s use only what’s essential.

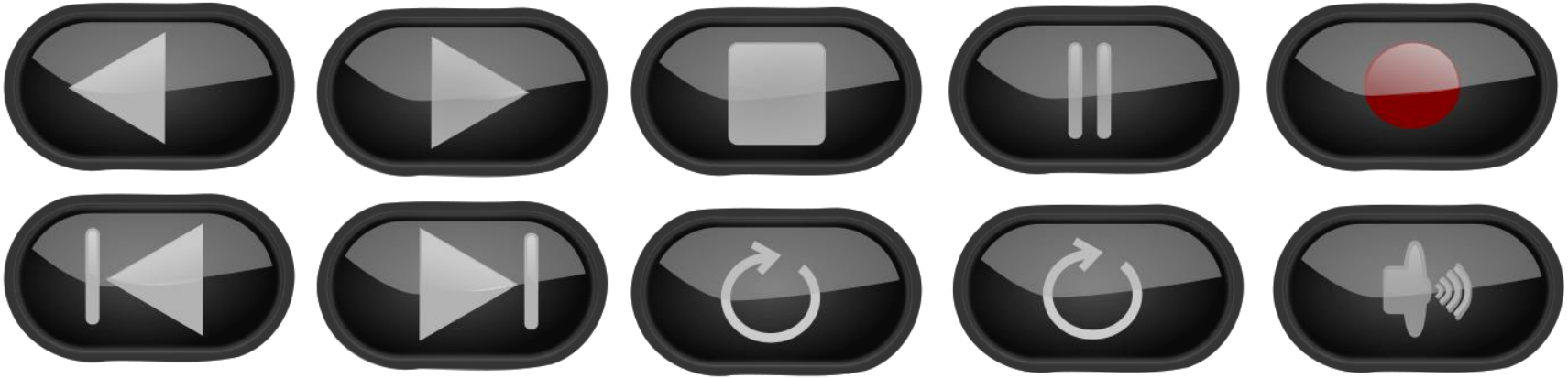
Reason: It is good engineering.

Take home message

As multimedia researchers:

- Let’s use only what’s essential.
- Let’s help people produce only what’s essential.

What is multimedia data?



https://openclipart.org/detail/75337/multimedia-buttons

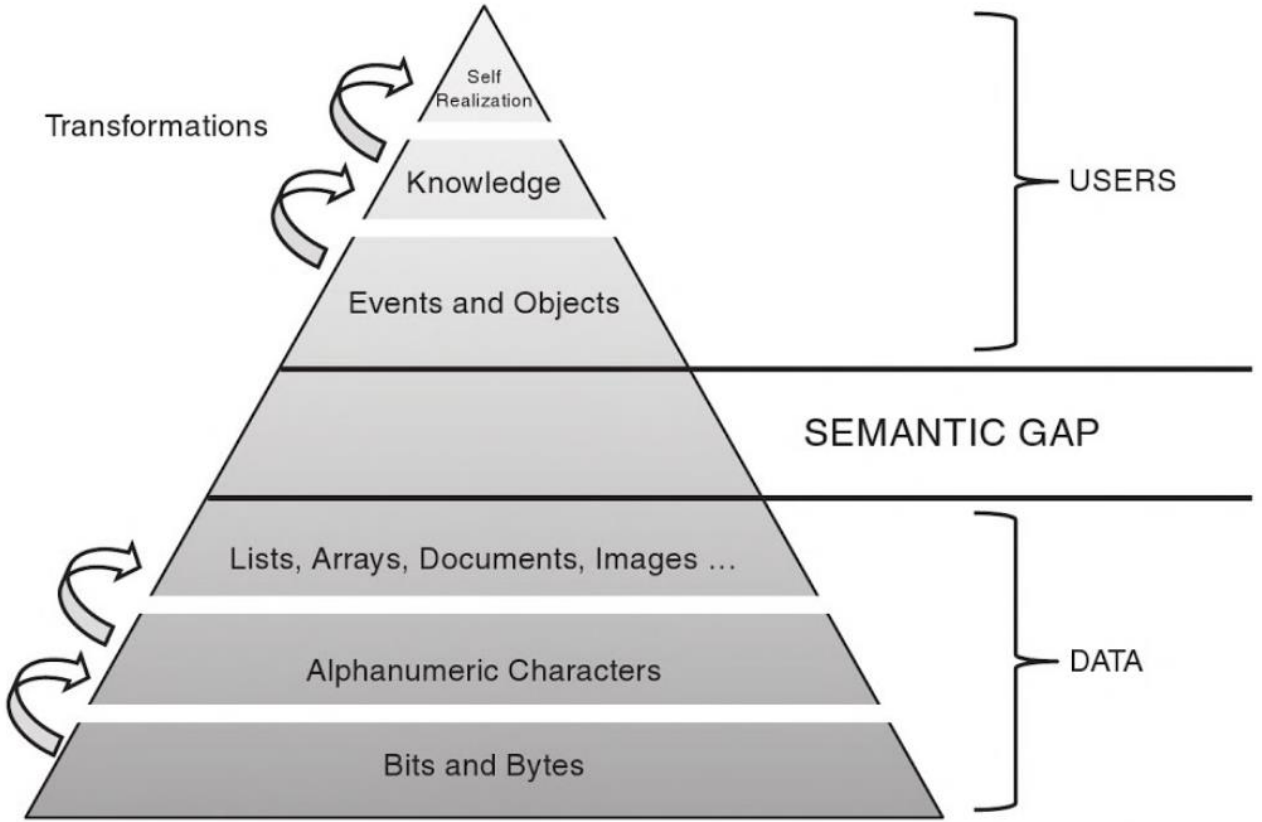


Figure 3.4. Semantic Gap. There is a big gap in how computers represent data like images in bits and bytes and how people think about images as collections of objects or events.

Friedland, G. and Jain, R. Multimedia Computing. Cambridge University Press. 2014.

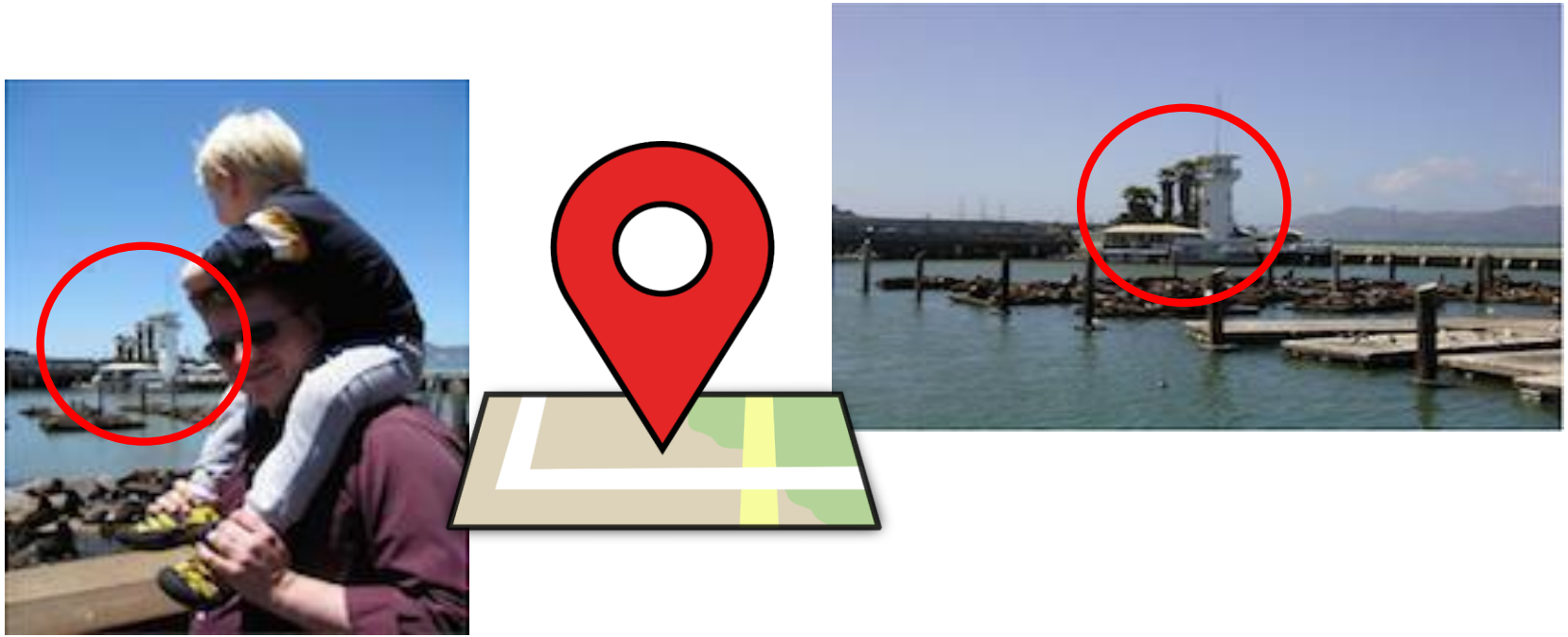
Personal data

https://openclipart.org/detail/177208/map-location

Personal data + more data

https://openclipart.org/detail/177208/map-location

Personal data + more data = personal information



X. Li, M. Larson and A. Hanjalic, "Global-Scale Location Prediction for Social Images Using Geo-Visual Ranking," in *IEEE Transactions on Multimedia*, vol. 17, no. 5, pp. 674-686, May 2015.

https://openclipart.org/detail/177208/map-location

Personal data reveals health information

Figure 1 Comparison of HSV values. Right photograph has higher Hue (bluer), lower Saturation (grayer), and lower Brightness (darker) than left photograph. Instagram photos posted by depressed individuals had HSV values shifted towards those in the right photograph, compared with photos posted by healthy individuals.

Reece AG, Danforth CM (2017) Instagram photos reveal predictive markers of depression. EPJ Data Sci 6(1):15.

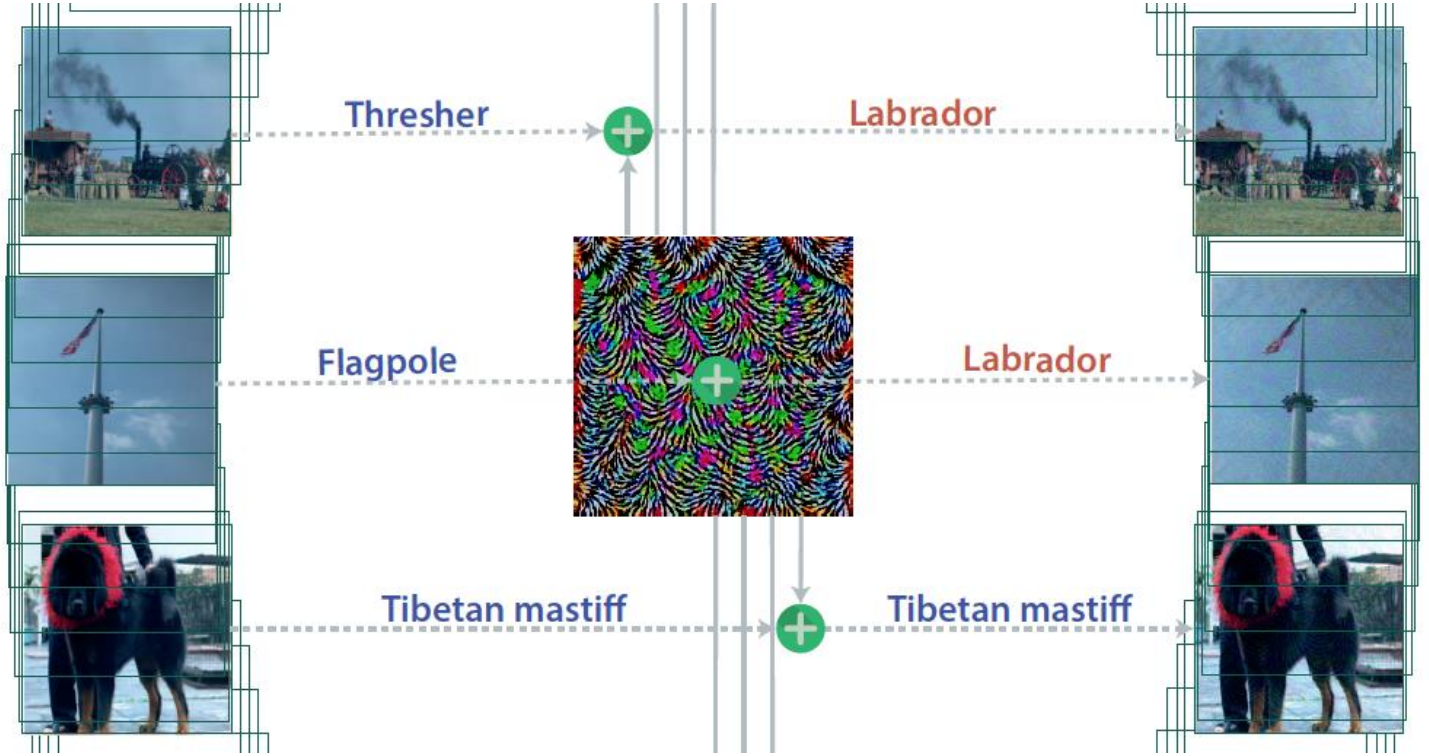
Our reality

BRIAN BARRETT SECURITY 12.14.18 12:22 PM

FACEBOOK EXPOSED 6.8 MILLION USERS' PHOTOS TO CAP OFF A TERRIBLE 2018

https://www.wired.com/story/facebook-photo-api-bug-millions-users-exposed

Adversarial examples reduce image information



Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, Omar Fawzi, and Pascal Frossard. 2017. Universal adversarial perturbations. CVPR 2017.

From data minimization to information minimization

Information minimization technologies:

Technologies that support users in sharing a multimedia message without sharing unintentional information.

From data minimization to information minimization

Information minimization technologies:

Technologies that support users in sharing a multimedia message without sharing unintentional information.

Why are so few people working on information minimization?

Instagram filters can mask geo-location information

Jaeyoung Choi, Martha Larson, Xinchao Li, Kevin Li, Gerald Friedland, and Alan Hanjalic. 2017. The Geo-Privacy Bonus of Popular Photo Enhancements. ACM ICMR 2017.

Information privacy is about control

- **Information privacy**: the state of control over information about you that is collected, stored, processed, or shared.

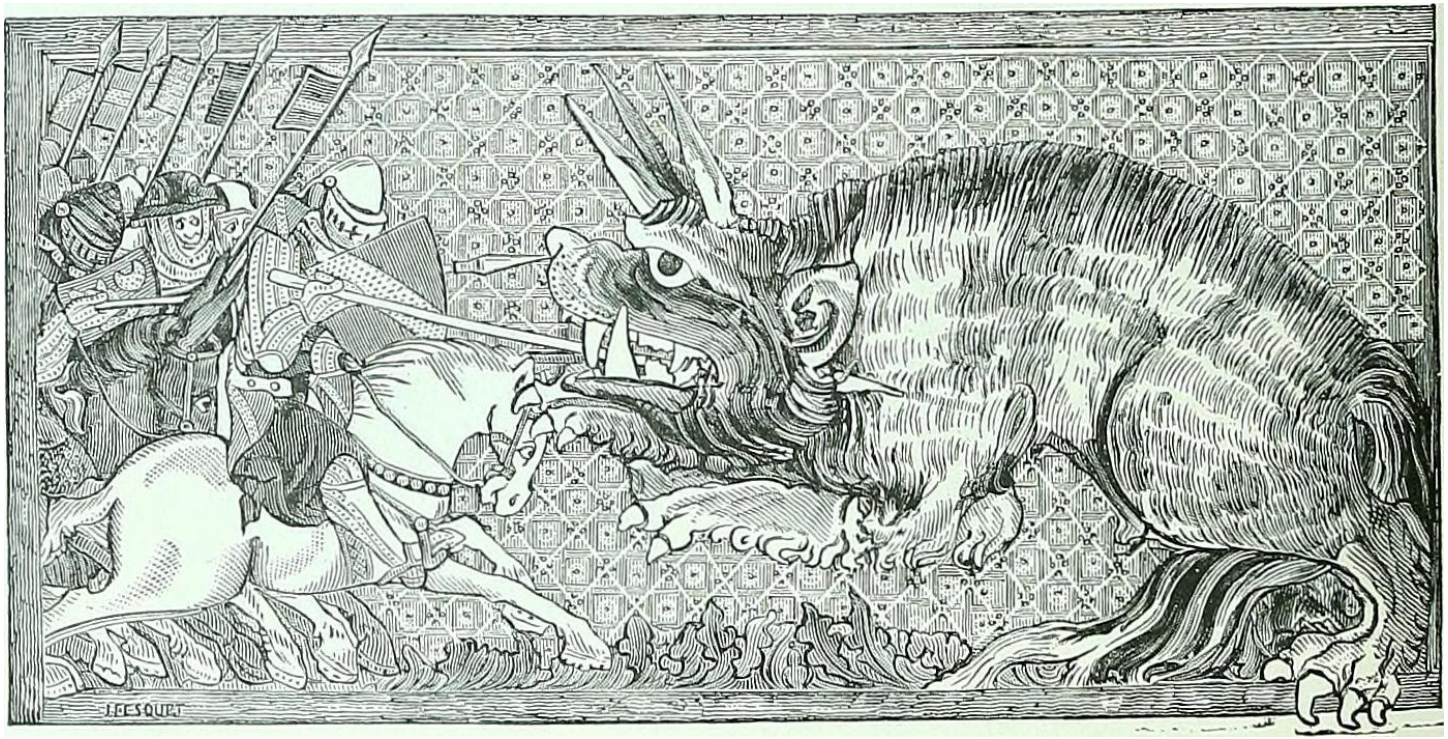
Craig, Terence, and Mary Ludloff. Privacy and big data. O'Reilly Media, 2011.

Take home message

As multimedia researchers:

- Let’s use only what’s essential.
- Let’s let people produce only what’s essential.

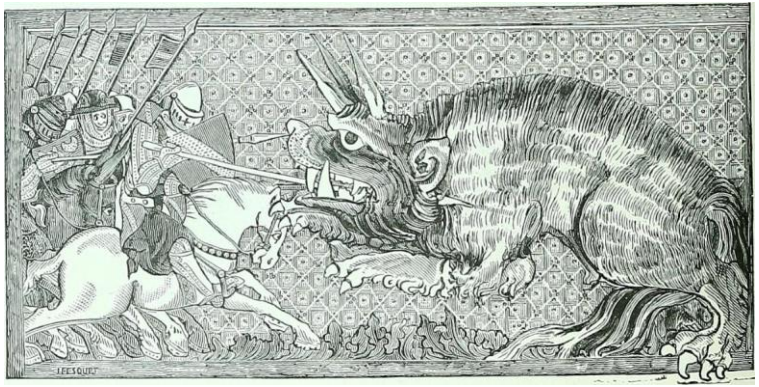
The dragon in the room



Multimedia Evaluation (MediaEval) Benchmark

- offers shared tasks on multimedia access and retrieval,
- focuses on the human and social aspects of multimedia,
- exploits features from multiple modalities.

multimediaeval.org



Pixel Privacy at MediaEval

Task Goal: Increasing image appeal, while blocking automatic inference of sensitive scene information.

Evaluation Criteria:

- **Protection**: % of images whose location categories can no longer be inferred by the “attack algorithm”.
- **Appeal**: Degree to which the images are enhanced from the point of view of users.

Novelty: We combine work on adversarial examples and image enhancement, which have been previously studied separately.

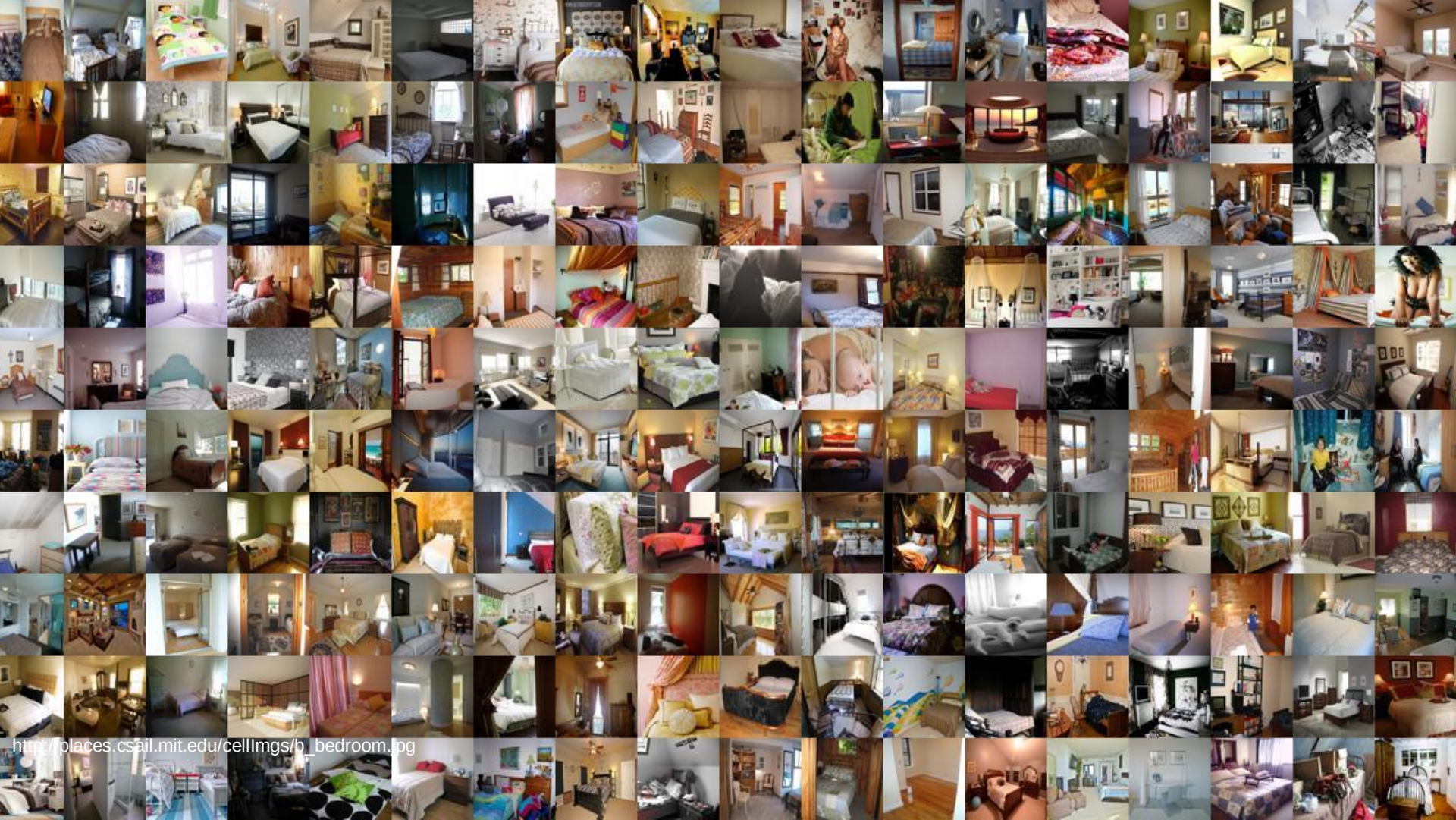
Pixel Privacy at MediaEval 2018

Task Data: Places365-Standard dataset

Sensitive scene information: Taken to be the class labels of classes in Places365-Standard dataset associated privacy criteria (that we defined):

- Places in the home,
- Places far away from the home (typical vacation places),
- Places typical for children,
- Places related to religion,
- Places related to people's health,
- Places related to alcohol consumption,
- Places in which people do not typically wear street clothes,
- Places related to people's living conditions/income,
- Places related to security, Places related to military.

B. Zhou, A. Lapedriza, A. Khosla, A. Oliva and A. Torralba, "Places: A 10 Million Image Database for Scene Recognition," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 40, no. 6, pp. 1452-1464, 1 June 2018.


http://places.csail.mit.edu/cellImgs/b_bedroom.jpg


NO FILTER

Scene information protected by style transfer

army_base (1.000)
hospital_room (0.000)
runway (0.000)
physics_laboratory (0.000)
landing_deck (0.000)

bedroom (0.229)
hotel_room (0.185)
bedchamber (0.185)
television_room (0.158)
living_room (0.045)

temple asia (0.589)
pagoda (0.287)
tower (0.023)
mausoleum (0.015)
palace (0.012)

shoe_shop (0.381)
clothing_store (0.080)
toyshop (0.055)
dressing_room (0.045)
closet (0.039)

beauty_salon (0.357)
hospital_room (0.183)
operating_room (0.076)
hotel_room (0.054)
youth_hostel (0.047)

nursery (0.235)
childs_room (0.204)
art_studio (0.074)
fabric_store (0.064)
playroom (0.041)

Examples for which style transfer is successful in protecting scene information.

Yang Chen, Yu-Kun Lai, and Yong-Jin Liu. CartoonGAN: Generative Adversarial Networks for Photo Cartoonization. CVPR 2018.

army_base (1.000)
hospital_room (0.000)
runway (0.000)
physics_laboratory (0.000)
landing_deck (0.000)

bedroom (0.229)
hotel_room (0.185)
bedchamber (0.185)
television_room (0.158)
living_room (0.045)

temple asia (0.589)
pagoda (0.287)
tower (0.023)
mausoleum (0.015)
palace (0.012)

shoe_shop (0.381)
clothing_store (0.080)
toyshop (0.055)
dressing_room (0.045)
closet (0.039)

beauty_salon (0.357)
hospital_room (0.183)
operating_room (0.076)
hotel_room (0.054)
youth_hostel (0.047)

nursery (0.235)
childs_room (0.204)
art_studio (0.074)
fabric_store (0.064)
playroom (0.041)

Baseline: Protection with CartoonGAN

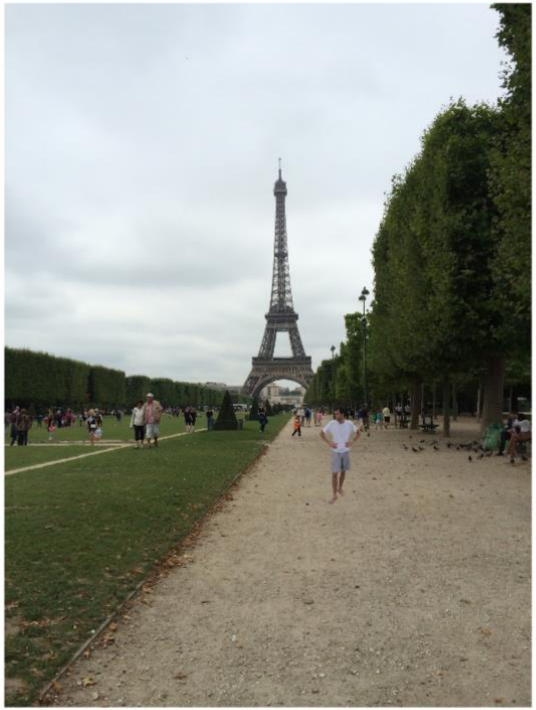
Protection: From 60% accuracy to 35% accuracy.

Table 1: Evaluation results in terms of Top-1 and top-5 prediction accuracy on the scene images from the MEPP18test dataset.

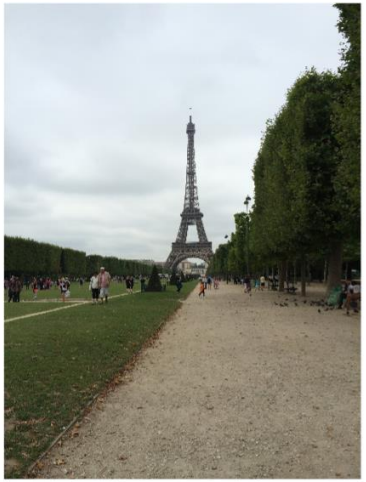
	Top-1 acc.	Top-5 acc.
Original	60.23%	88.63%
Hayao	41.57%	69.97%
Ukiyo-e	34.23%	62.00%
C-crop	39.33%	70.57%
R-crop	34.27%	63.17%
UAP	45.33%	76.97%

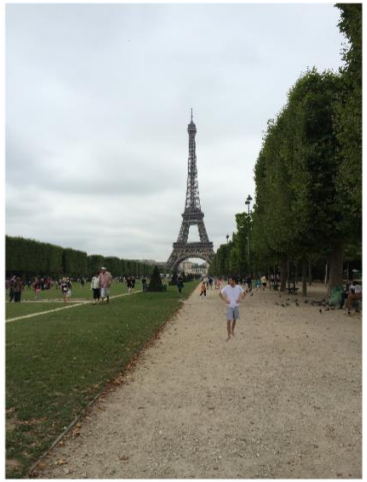
Zhuoran Liu, Zhengyu Zhao. First Steps in Pixel Privacy: Exploring Deep Learning-based Image Enhancement against Large-Scale Image Inference. MediaEval 2018 Working Notes Proceedings.

Who was in Paris?



Scene Change Task


+

=


- Size and orientation
- Lighting conditions
- Segmentation

Scene change, planned pilot MediaEval 2018

Task Goal: Put people in Paris, by combining two images into a third, fun-to-share image.

Evaluation Criterion:

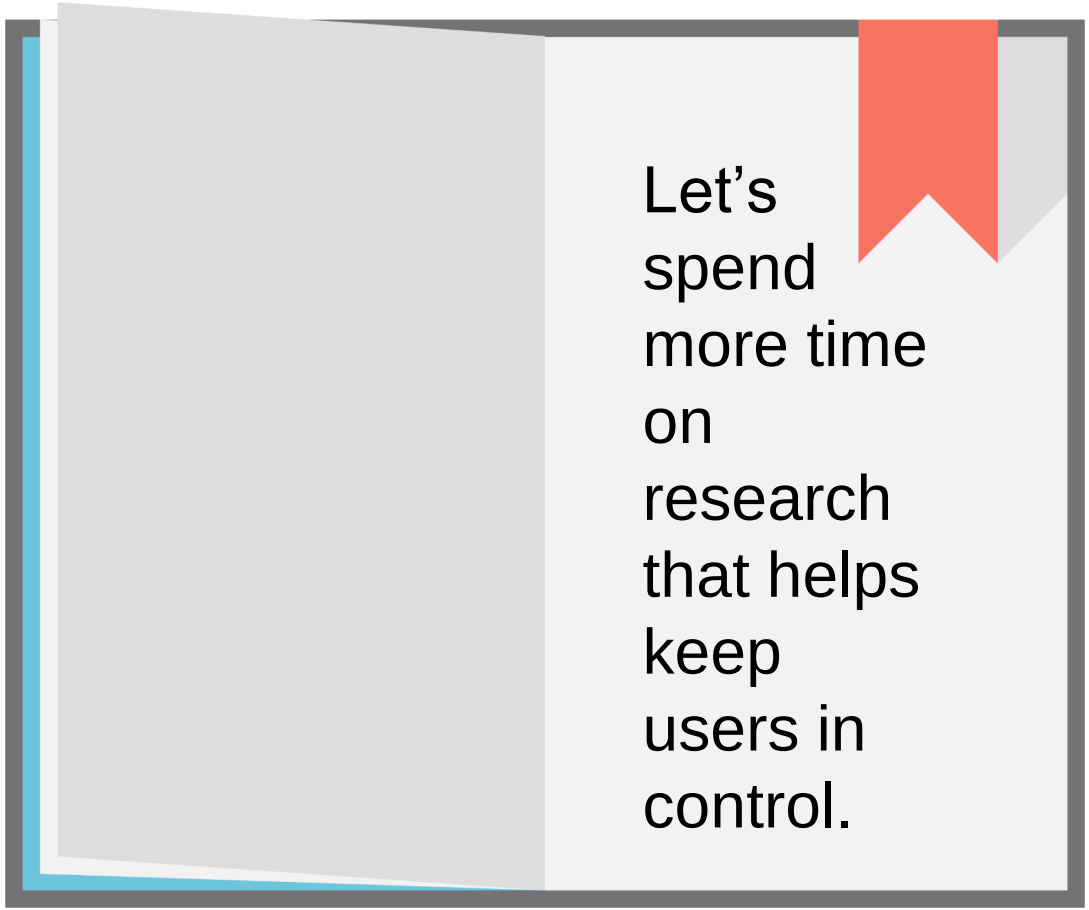
- **Appeal**: Degree to which the images are realistic or acceptable.

Novelty: We want to discover why more consumer products don’t offer combination options.

Take home message

As multimedia researchers:

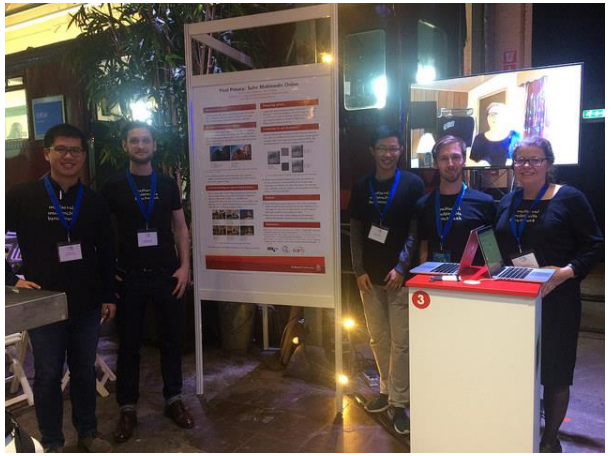
- Let’s use only what’s essential.
  - It’s good engineering.
  - It supports compatibility with the law.
  - “Complete information” is not well defined, anyhow.
- Let’s help people produce only what’s essential.
  - Creativity is control.
  - Supporting control improves privacy.



https://openclipart.org/detail/182527/open-book

Thank you

- The MMM 2019 Organizers
- The Pixel Privacy team: Zhuoran Liu, Simon Brugman, Zhenyu Zhao, Maciej Wysokinski
- The hundreds of researchers who invest time in effort in organizing and participating in MediaEval.



Pixel Privacy

Open Mind make a difference

NWO Netherlands Organisation for Scientific Research

Caution needed

As more people can edit multimedia, certain dangers multiply.

https://openclipart.org

Importance of control

- Legal solutions
- Social solutions
- Technical solutions

https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target

The Washington Post
Democracy Dies in Darkness

The Switch

Fake-porn videos are being weaponized to harass and humiliate women: 'Everybody is a potential target'

'Deepfake' creators are making disturbingly realistic, computer-generated videos with photos taken from the Web, and ordinary women are suffering the damage

A new technology is being used to put women's faces on porn stars' bodies. (Sarah Hashemi/The Washington Post)

By Drew Harwell
December 30, 2018

Importance of control

“The internet is a vast wormhole of darkness that eats itself.”

- Scarlett Johansson

https://www.washingtonpost.com/opinions/a-reason-to-despair-about-the-digital-future-deepfakes/2019/01/06

The Washington Post
Democracy Dies in Darkness

The Post's View • Opinion

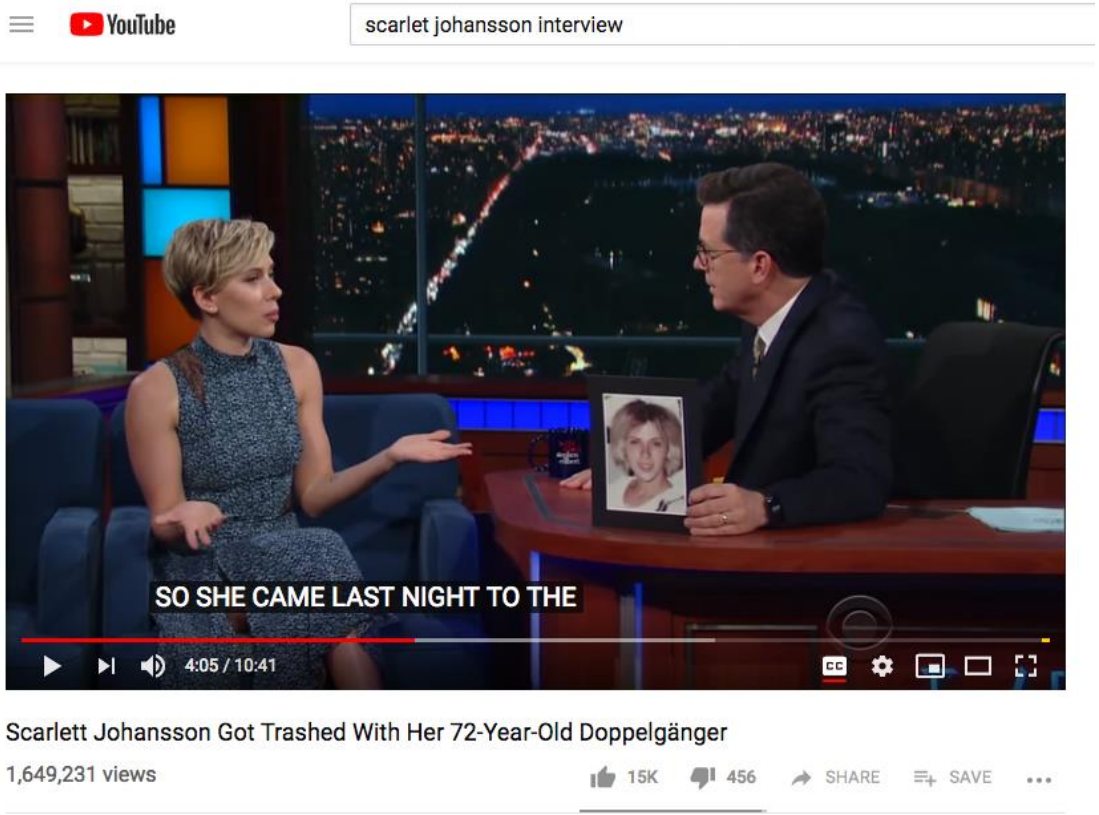
A reason to despair about the digital future: Deepfakes

Actress Scarlett Johansson speaks during the 2012 Democratic National Convention in Charlotte. (Jonathan Newton/The Washington Post)

By **Editorial Board**
January 6

A DESPAIRING prediction for the digital future came from an unlikely source recently. Speaking of “deepfakes,” or media manipulated through artificial intelligence, the actress Scarlett Johansson told The Post that “the Internet is a vast wormhole of darkness that eats itself.”

Importance of trust and control



Actress Scarlett Johansson speaks during the 2012 Democratic National Convention in Charlotte. (Jonathan Newton/The Washington Post)

By **Editorial Board**
January 6

A DESPAIRING prediction for the digital future came from an unlikely source recently. Speaking of "deepfakes," or media manipulated through artificial intelligence, the actress Scarlett Johansson told The Post

Importance of imitation

- Imitation is part of the way we express ourselves.
- Even if it is confusing at times.

https://edition.cnn.com/2017/02/12/politics/dominican-newspaper-confuses-baldwin-trump/index.html

Importance of imitation

- Imitation is part of the way we express ourselves.
- Even if it is confusing at times.

https://edition.cnn.com/2017/02/12/politics/dominican-newspaper-confuses-baldwin-trump/index.html

CNN politics 45 CONGRESS SUPREME COURT 2018 ELECTION RESULTS

Newspaper apologizes after mistaking Alec Baldwin for President Trump

By Jay Croft, CNN

Updated 1100 GMT (1900 HKT) February 13, 2017

Source: NBC/Broadway Video

'SNL': Trump's day in court 01:11

STORY HIGHLIGHTS

Error occurred in El Nacional, a newspaper in the Dominican Republic

The actor often impersonates Trump on "Saturday Night Live"

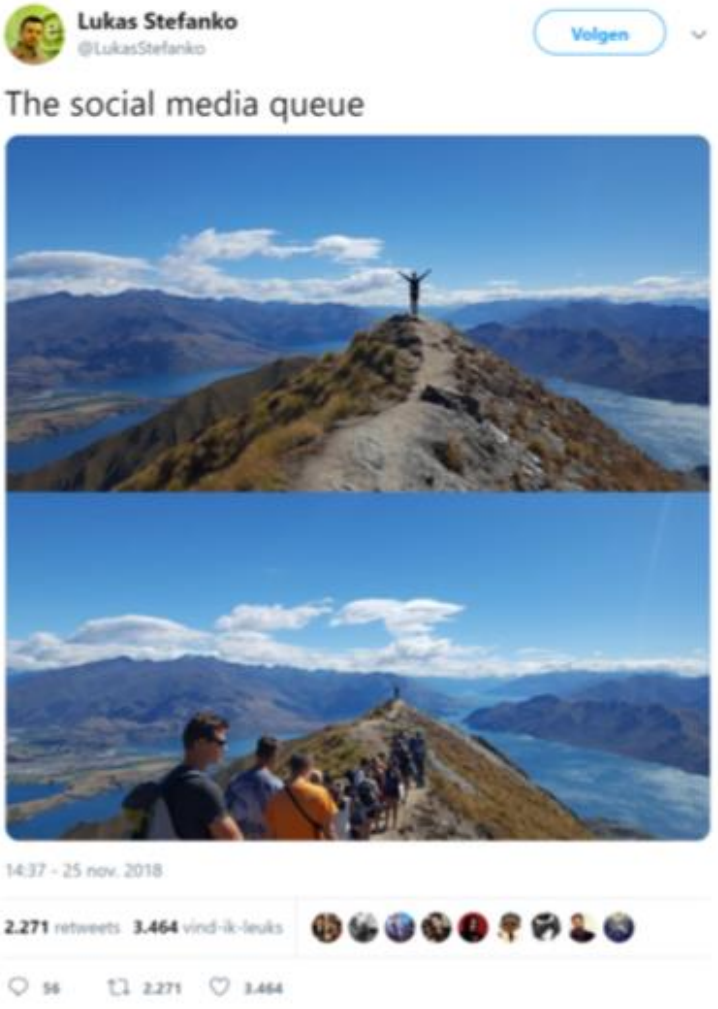
(CNN) — Alec Baldwin has two Emmys and an Oscar nomination. But a newspaper in the Dominican Republic may have given the actor his highest praise yet.

Trump dice colonias de Israel no favorecen paz

Es la primera vez que el presidente de Estados Unidos asume una posición sobre el desarrollo de los conflictivos asentamientos israelíes

Familiares policías protestan en Brasil

The social media queue



SHARING

https://openclipart.org/detail/19519/stop-sign

SHARING

https://pixabay.com/en/steering-wheel-steering-wheel-150137/