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
What is “adversarial”?
“Adversarial”: two contexts in machine learning

<table>
<thead>
<tr>
<th>Generative Adversarial Network (GAN)</th>
<th>Adversarial Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network that learns by attempting to outsmart another network.</td>
<td>Example that surprises us because it gets misclassified.</td>
</tr>
</tbody>
</table>
How to generate adversarial examples

Constraint optimization

\[
\begin{align*}
\text{minimize} & \quad \|x_0 - x\|_2^2 \\
\text{such that} & \quad C(x) \neq t
\end{align*}
\]

where \( t \) is the label of \( x_0 \).

Class \( \neq t \) \quad Class = t

Universal Adversarial Perturbations

Universal Adversarial Perturbations

“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?
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 modalities are complementary. Together, they contain complete information.
multimedia signals

<table>
<thead>
<tr>
<th>Communication</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Words</td>
<td></td>
</tr>
<tr>
<td>Visual content</td>
<td></td>
</tr>
<tr>
<td>Audio</td>
<td></td>
</tr>
</tbody>
</table>
## Today’s multimedia signals

<table>
<thead>
<tr>
<th>Communication</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words</td>
<td>Views</td>
</tr>
<tr>
<td>Visual content</td>
<td>Purchases</td>
</tr>
<tr>
<td>Audio</td>
<td>Location</td>
</tr>
</tbody>
</table>
Today’s multimedia signals

<table>
<thead>
<tr>
<th>Content</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words</td>
<td>Views</td>
</tr>
<tr>
<td>Visual content</td>
<td>Purchases</td>
</tr>
<tr>
<td>Audio</td>
<td>Location</td>
</tr>
</tbody>
</table>
Today’s multimedia signals

<table>
<thead>
<tr>
<th>Intentional</th>
<th>Unintentional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words</td>
<td>Views</td>
</tr>
<tr>
<td>Visual content</td>
<td>Purchases</td>
</tr>
<tr>
<td>Audio</td>
<td>Location</td>
</tr>
</tbody>
</table>
Today’s multimedia signals

<table>
<thead>
<tr>
<th>Intentional</th>
<th>Unintentional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words</td>
<td>Views</td>
</tr>
<tr>
<td>Visual content</td>
<td>Purchases</td>
</tr>
<tr>
<td>Audio</td>
<td>Location</td>
</tr>
<tr>
<td><em>User initiates and controls.</em></td>
<td><em>User lacks complete, (conscious) control.</em></td>
</tr>
</tbody>
</table>
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.
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.
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.
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.
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

“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

Our rights under GDPR (examples)

> A right ‘to be forgotten’. You will be able to ask to delete your personal data if you no longer want it to be processed, and there is no legitimate reason for a company to keep it. For example, when you type your name into an online search engine, and the results include links to an old newspaper article about the debt you long paid, you will be able to ask the search engine to delete the links.

(Art. 17 of the Regulation)

> A right to request access to the personal data an organisation has about you.

(Art. 15 of the Regulation)

> A right to request one service provider to transmit your personal data to another service provider, e.g. when switching from one to another internet social network, or switching to another cloud provider.

(Art. 20 of the Regulation)

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.

Information privacy is about control

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

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

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.

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

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

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).

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.

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.
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

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.

Our reality

https://www.wired.com/story/facebook-photo-api-bug-millions-users-exposed
Adversarial examples reduce image information

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

Information privacy is about control

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

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.

Scene information protected by style transfer

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

Baseline: Protection with CartoonGAN

Protection: From 60% accuracy to 35% accuracy.

<table>
<thead>
<tr>
<th>Method</th>
<th>Top-1 acc.</th>
<th>Top-5 acc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original</td>
<td>60.23%</td>
<td>88.63%</td>
</tr>
<tr>
<td>Hayao</td>
<td>41.57%</td>
<td>69.97%</td>
</tr>
<tr>
<td>Ukiyo-e</td>
<td>34.23%</td>
<td>62.00%</td>
</tr>
<tr>
<td>C-crop</td>
<td>39.33%</td>
<td>70.57%</td>
</tr>
<tr>
<td>R-crop</td>
<td>34.27%</td>
<td>63.17%</td>
</tr>
<tr>
<td>UAP</td>
<td>45.33%</td>
<td>76.97%</td>
</tr>
</tbody>
</table>

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.
Let’s spend more time on research that helps keep users in control.
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.
Caution needed

As more people can edit multimedia, certain dangers multiply.
Importance of control

- Legal solutions
- Social solutions
- Technical solutions

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
Importance of control

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

- Scarlett Johansson

A reason to despair about the digital future: Deepfakes

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
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.

Importance of imitation

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

The social media queue
SHARING