



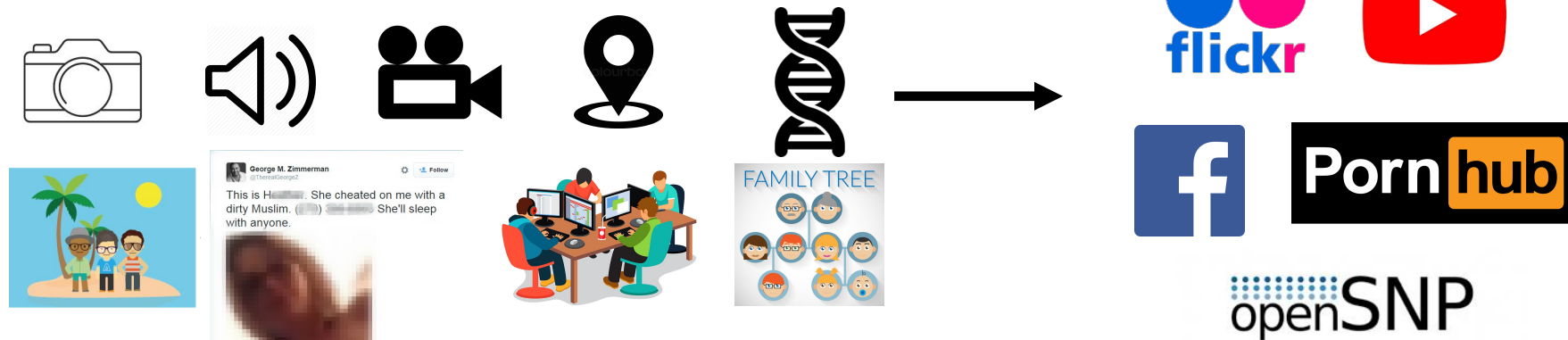
# Consensual and Privacy-Preserving Sharing of Multi-Subject and Interdependent Data

*Alexandra-Mihaela Olteanu*<sup>1,2</sup>, Kévin Huguenin<sup>2</sup>, Italo Dacosta<sup>1</sup>, and Jean-Pierre Hubaux<sup>1</sup>

<sup>1</sup>EPFL, <sup>2</sup>UNIL

# Multi-Subject and interdependent data is abundant

- Individuals share increasing amounts of data online



- **Other individuals** are **irrevocably affected** by the shared data
  - The uploader is not the owner of the data
  - The data has consequences for other individuals due to interdependencies



# (Privacy) problems



- For the users
  - Sensitive information leaked **without** users' **consent** or even **awareness**
  - **Prejudice** and **discrimination**
  - **Revenge pornography**
- For the service providers
  - Lawsuits

## Facebook pays costs in naked photo settlement

9 January 2018

f t m e Share



The photo was allegedly posted on a so-called 'shame' page on Facebook several times in two years

A 14-year-old girl who sued Facebook after a man allegedly posted a naked photo of her on the website has settled the landmark legal action out of court.

Facebook will pay the Northern Ireland teenager's legal costs, under the terms of the settlement which a court heard was the first of its kind in the world.

The photo was allegedly posted on a so-called "shame" page on Facebook several times between 2014 and 2016.

## Facebook warned it faces legal action from 'revenge porn' victims

Settlement with teenager over naked images of her posted online on networking site has 'moved goalposts', say lawyers



Facebook is facing a number of lawsuits from victims of "revenge porn", a leading libel lawyer has warned, after a teenager reached a settlement with the social networking site over naked images of her that were posted online.

## Facebook Asks Australia For Nude Pics To Test 'Revenge Porn' Defense



Janet Burns, [WOMEN@FORBES](#)

I cover AI, cybersecurity, culture, drugs, and more. [FULL BIO](#) ▾

Opinions expressed by Forbes Contributors are their own.



Shutterstock

Facebook is working on a new way to rid the platform of 'revenge porn,' and giving it a first whirl in Australia (where, incidentally, Domino's Pizza and McDonald's have also experimented with [unusual deliveries](#)); specifically, they'll be asking for nudes.

The [Australia Broadcasting Corporation](#) (ABC) reported this week that Facebook will be testing out a new preemptive method for blocking the unauthorized distribution of nude photos on the site, and (they hope) with the help of Australian Facebook users. According to ABC, Facebook has partnered with the country's e-Safety Commissioner to develop the program, aimed at protecting not just extant victims of vindictive image-sharing, but also potential ones.

# (Privacy) problems



- For the users
  - Sensitive information leaked **without** users' **consent** or even **awareness**
  - **Prejudice** and **discrimination**
  - **Revenge pornography**
- For the service providers
  - Lawsuits
- Amazon MTurk survey (N=321)
  - **10.3%** of the participants claimed they were **victims** of **discrimination** or **prejudice** based on online content
    - **66.7%** of these reported as **cause content shared by others**
  - **4.1%** of the participants reported being **victims of revenge pornography**



# Some good elements do exist

- Tagging can be automated
- Companies start to work around the notion of consent

When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?

Friends

Edit

Who sees **tag suggestions** when photos that look like you are uploaded?

Close


When a photo that looks like you is uploaded, we'll suggest adding a tag of you. This helps save time when adding tags to photos, especially when labeling many photos from one event. Suggestions can always be ignored and no one will be tagged automatically. [Learn more.](#)

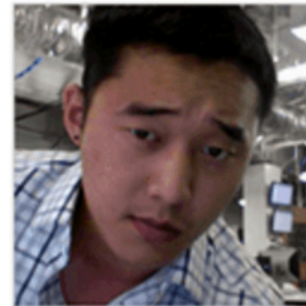
Friends ▾


## Who Is in These Photos?

The photos you uploaded were grouped automatically so you can quickly label and notify friends in these pictures. (Friends can always untag themselves.)



 Albert Hong



 Albert Hong



Anne Marie added a new photo.

Just now · 🌐

You looked so much younger before your PhD, Alexandra 🤔 — with Alexandra Olteanu.



👍 Like

💬 Comment

## Report a Privacy Rights Violation

Please note that this channel is reserved for people reporting potential violations of their privacy rights concerning their image on Facebook. If you're writing in about something else, please return to the Help Center:

[www.facebook.com/help](http://www.facebook.com/help)

If you need help because someone is threatening to share something you want to keep private, follow this steps outlined in this form:

[www.facebook.com/help/561743407175049](http://www.facebook.com/help/561743407175049)

Also note that while we do review all reports, you won't receive a confirmation email if we take action on your report.

### What are you trying to report?

- Photo
- Video
- Other

### What type of photo are you trying to report?

- Profile picture
- Other photo

### Where do you live?

- In the US
- Outside the US

Please provide a link to the content you're trying to report so we can investigate. To get a link to the exact content you want to report:

1. Find the content (ex: photo, video, comment) you want to report
2. If this content is on someone's Timeline, click on the date/time it was posted (ex: 27 minutes, May 30 at 7:30pm)
3. Copy the URL from your browser's address bar:



# Pornhub is using machine learning to tag its 5 million videos

The company is starting with facial recognition, but wants its AI to recognize

By James Vincent | @jvincent

Oct 11, 2017, 2:03pm EDT

f t SHARE



## Content Removal Request?

Pornhub takes all content removal requests seriously. Should you be a victim of revenge porn, blackmailing or intimidation because of a video or photo of yourself on our sites that you did not authorize, please complete the form below and we will remove the content expeditiously.

For all other content removal requests related to copyright infringement, please contact [copyright@pornhub.com](mailto:copyright@pornhub.com) or use the DMCA takedown request form on [/information#dmca](#).

Email:

Name:



But ...



# Goals



***Privately detect & inform*** all affected individuals when content regarding them is submitted

Enable individuals to grant their ***consent before*** such content is made available

# Challenges



- Identity claim
- ***Privately & securely determine*** the affected users by some piece of data
- ***Privately & securely contact users*** and provide them with enough context to make an ***informed decision***
- Privately & securely collect and enforce consent decisions






**! *Data dependent***

# System model & adversarial assumptions



- Key features
  - Effectiveness
  - User privacy through ***anonymity*** and ***unlinkability***
    - wrt to any other users and to any service providers
  - Robustness against malicious user behavior
  - Usability and transparency
- Service providers: ***honest-but-curious***
- Users of the system: ***malicious***

# System overview

- **Content Management Service** (CMS) – user-generated content sites (e.g., , , , , etc.)
- **Identity Management Service** (IMS) – e.g., , government agencies
  - Manages users' identities
  - Offers services to identify the users associated with a particular content
  - In charge of users' relationships (social and family)
- **User applications** (CMS and IMS) – components that users interact with to publish content and to review consent requests

# ConsenShare: an example for photos



Original photo



Background image

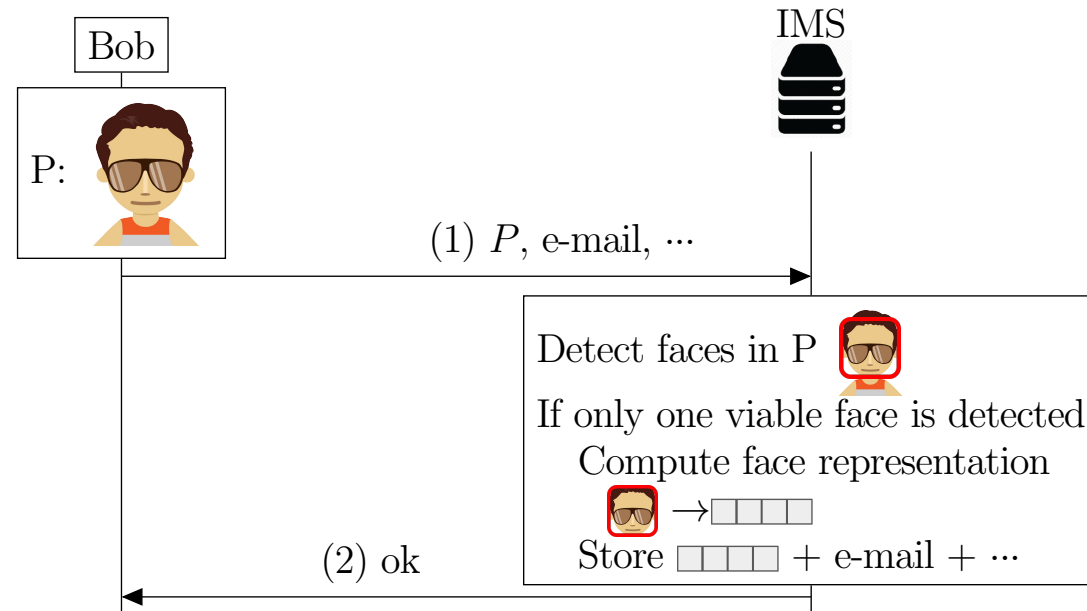


Final photo

Photo source (Creative Commons):  
<https://pixabay.com/en/runners-running-jogging-1517163/>

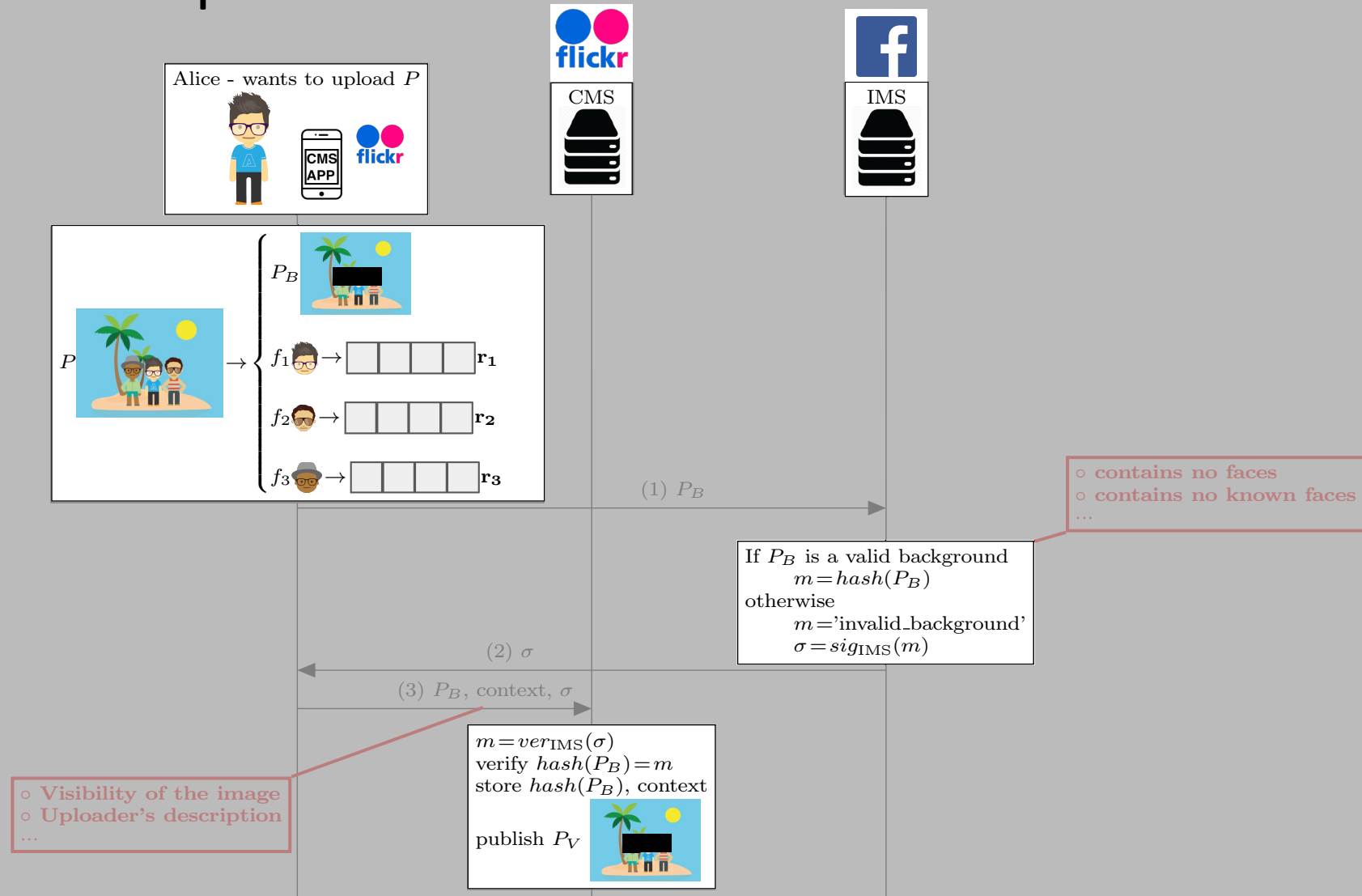
# User registration protocol

The user provides a webcam photo/video to the IMS





# Photo upload protocol



Alice - wants to upload  $P$

CMS

IMS

Bob - appears in  $P$

(4)  $hash(P_B), E_{Pk_{IMS}}(r_2)$

verify  $hash(P_B)$  is stored  
 generate random  $sid$   
 store  $sid, E_{Pk_{IMS}}(r_2)$  linked to  $hash(P_B)$   
 status( $sid$ ) = *Pending*

(5)  $sid, E_{Pk_{IMS}}(r_2)$

$r_2 = D_{Sk_{IMS}}(E_{Pk_{IMS}}(r_2))$   
 lookup best match( $r_2$ )

(6)  $sid, CMS$

Generate key pair ( $Pk_{sid}, Sk_{sid}$ )

(7)  $sid, Pk_{sid}$

(8)  $sid, Pk_{sid}$

Encrypt using  $Pk_{sid}$

(9)  $sid, E_{Pk_{sid}}(\text{person icon})$

store  $E_{Pk_{sid}}(\text{person icon})$  linked to  $sid$

(10)  $P_B, \text{'Alice'}, \text{context}, E_{Pk_{sid}}(\text{person icon})$

$\text{person icon} = D_{Sk_{sid}}(E_{Pk_{sid}}(\text{person icon}))$   
 review and decide

spam filtering

- o manual decision
- o policy (e.g., "accept if not nude", "accept if I am the uploader")
- o automatic decision (e.g., machine learning)
- ...

- o content obfuscation
- o specific audience
- ...

Repeat for

(11a)  $sid, Sk_{sid}$

$\bar{f} = D_{Sk_{sid}}(E_{Pk_{sid}}(\text{person icon}))$   
 $\bar{f} \rightarrow \bar{r}$   
 verify  $E_{Pk_{IMS}}(r_2) = E_{Pk_{IMS}}(\bar{r})$   
 status( $sid$ ) = *Accepted*  
 update  $P_V$

If accept




(11b)  $sid, \text{'deny'}$

status( $sid$ ) = *Denied*

If deny

# Privacy analysis



- Information observed by the CMS (  )
  - Background image
  - Encrypted faces and encrypted face vectors
- Information observed by the IMS (  )
  - Background image
  - Face vectors
- Information observed by a consenter (  )
  - Context
  - Background image
  - His own face






***Cannot link encrypted faces to users' identities***

***Cannot link users' identities to photos***

***Guaranteed user anonymity, unlinkability and robustness against malicious users***

# Potential for adoption

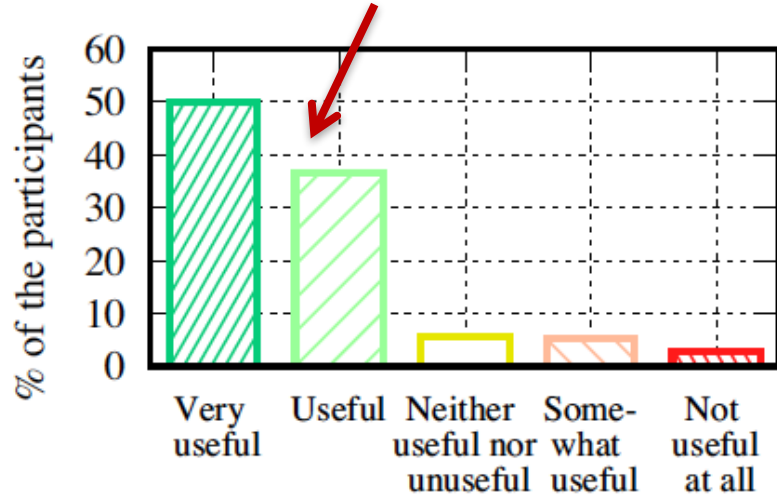


- CMS incentives ( ,  )
  - Follow new trends and/or regulations, lawsuit avoidance, maintain good reputation, increase user base
- IMS incentives (  )
  - B2B arrangements with different CMS, increase user base
- User incentives ( ,  )
  - **Awareness** and **control** over their data, usability and transparency

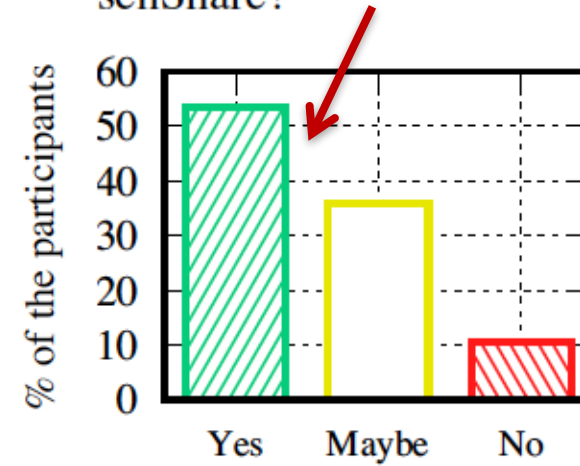
# Surveyed potential interest



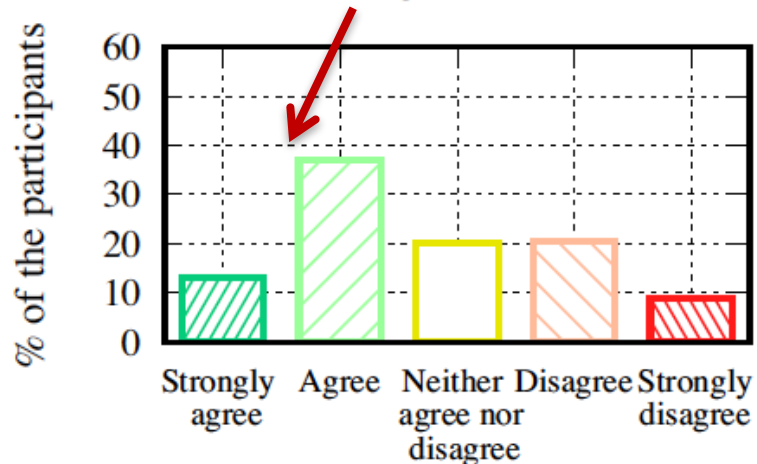
Q27: Do you find ConsenShare useful?



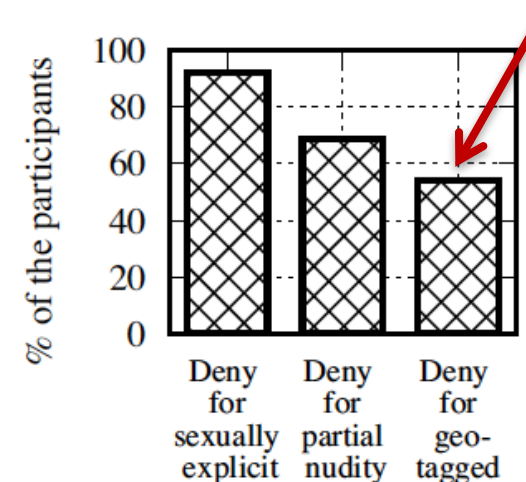
Q32: Would you use ConsenShare?



Q29: Would you use ConsenShare with Machine Learning automation?



Q28: Which policies would you use with ConsenShare?



# Implementation

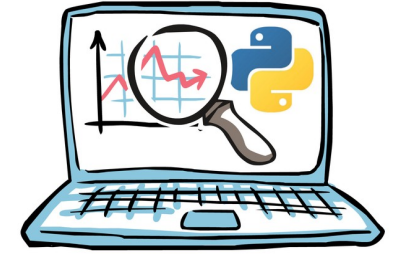


- 128-bits security for the basic cryptographic operations (hash, sign/verify, encrypt/decrypt and generate keys)
- Python with PyNaCl\* and OpenFace\*\*
- W/o any CPU optimizations

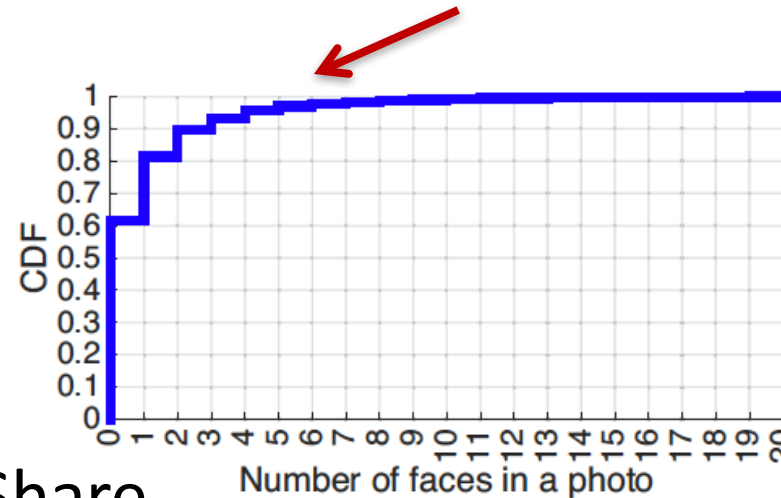
\* PyNaCl - Python binding to the Networking and Cryptography library. <https://github.com/pyca/pynacl>

\*\* OpenFace - Free and open source face recognition with deep neural networks.  
<https://cmusatyalab.github.io/openface/>

# Evaluation



- Dataset: random sample of 17k+ photos from Yahoo's YFCC100m
  - Original photos uploaded by real users on Flickr



- Efficiency of ConsenShare
  - Per-photo CPU and bandwidth consumption (CMS, IMS, uploader, consenter)
  - Measured on Intel i7 CPU, 2.8 GHz, 8GB RAM
  - Reasonable bandwidth and CPU requirements

# Conclusion

**CONCLUSION**

- ConsenShare: practical and privacy-preserving
  - *Preserves* the *main features* of existing CMS
  - Provides *privacy* guarantees (*wrt to service providers and to other users*)
  - Has negligible overhead
- Next steps
  - Include more human interaction aspects
  - Perform a usability study for a fully integrated prototype
- *Extensible* to other data types
  - *Audio, video, genomic, co-location* data





<https://infoscience.epfl.ch/record/232563>