Design and Development of a Facebook Application to Raise Privacy Awareness

Dr. Gianpiero Costantino

Co-author
Dr. Daniele Sgandurra

Consiglio Nazionale delle Ricerche

Imperial College London

Outline

- **Online Social Network**
  - Users and private contents
  - Facebook and Photos
  - The Photo issue
- **The Phook web-app**
  - What is
  - How it works
- **Conclusion**

Online Social Networks (OSNs)

- OSNs represent a huge container of users' personal information, i.e. photos, comments, interests…
- OSNs provide tools to set up content visibility
- Users choose who can see their contents:
  - Familiar People
  - Friends
  - Anyone

Users and their Privacy

Results from *“Pew Research Center”*

2008

60% of adult users restrict access profile to only their friends

36% of adult users have a public profile

2012

Women set highest restrictions *(67% Vs 48%)*

11% users have posted content they regret

2013

86% of Internet users remove of mask their digital footprints

My Thought

- By protecting my digital contents, I think that I am protected against undesired access

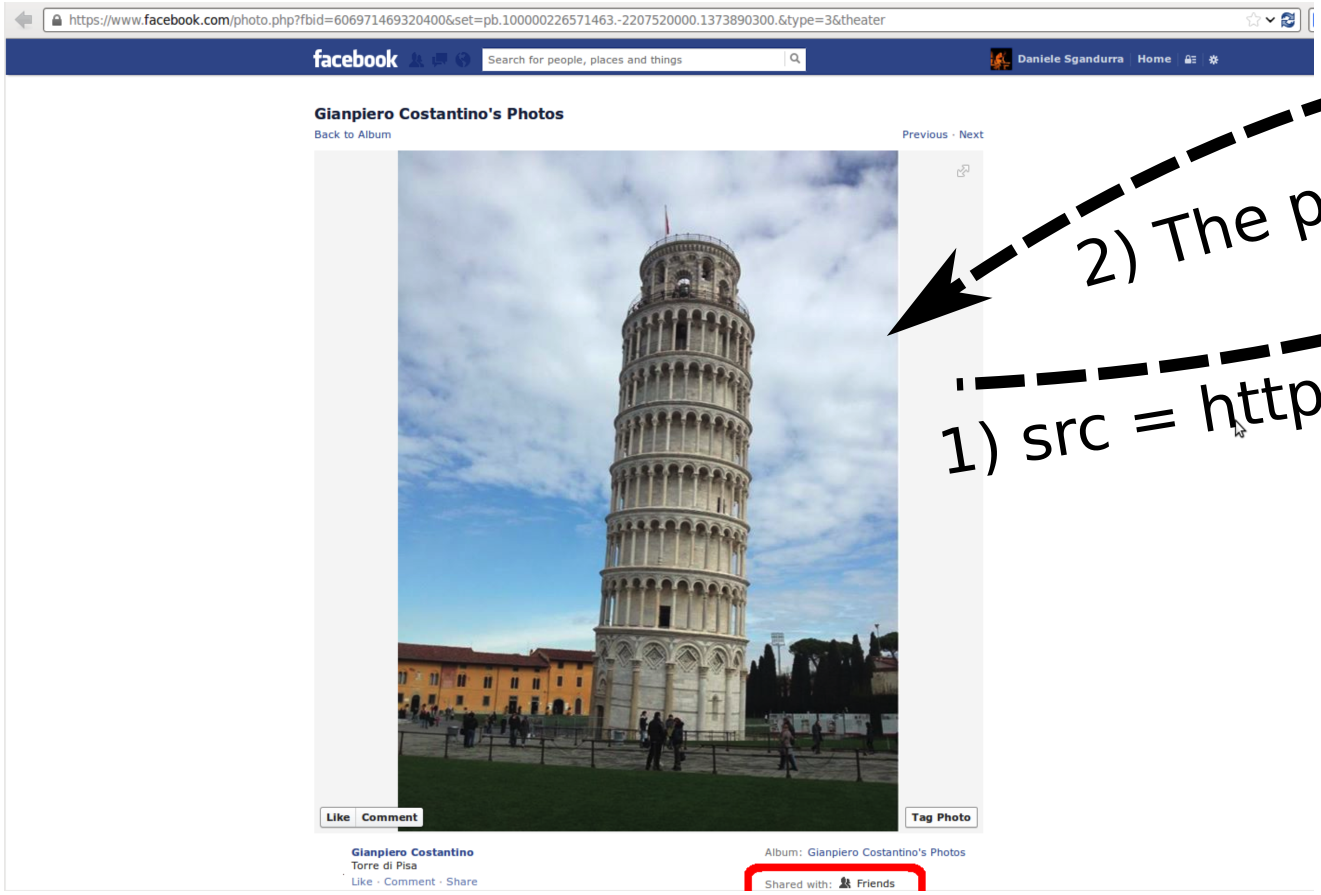
- This belief is based upon:

  i) OSNs correctly implement secure mechanisms

  ii) All authorised users will correctly behave

Case Study - A private photo

User's Browser


https://www.facebook.com/photo.php?fbid=606971469320400&set=pb.100000226571463.-2207520000.1373890300.&type=3&theater

Gianpiero Costantino's Photos

Back to Album

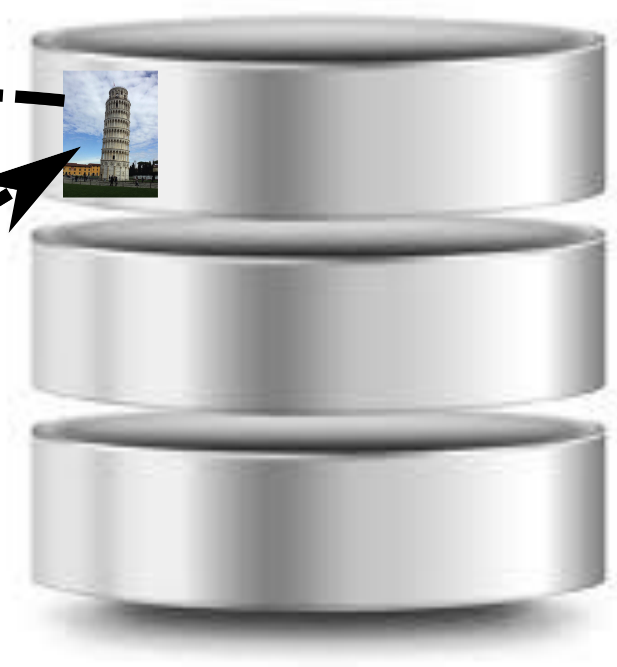
Gianpiero Costantino

Torre di Pisa

Album: Gianpiero Costantino's Photos

Shared with: Friends

Akamai

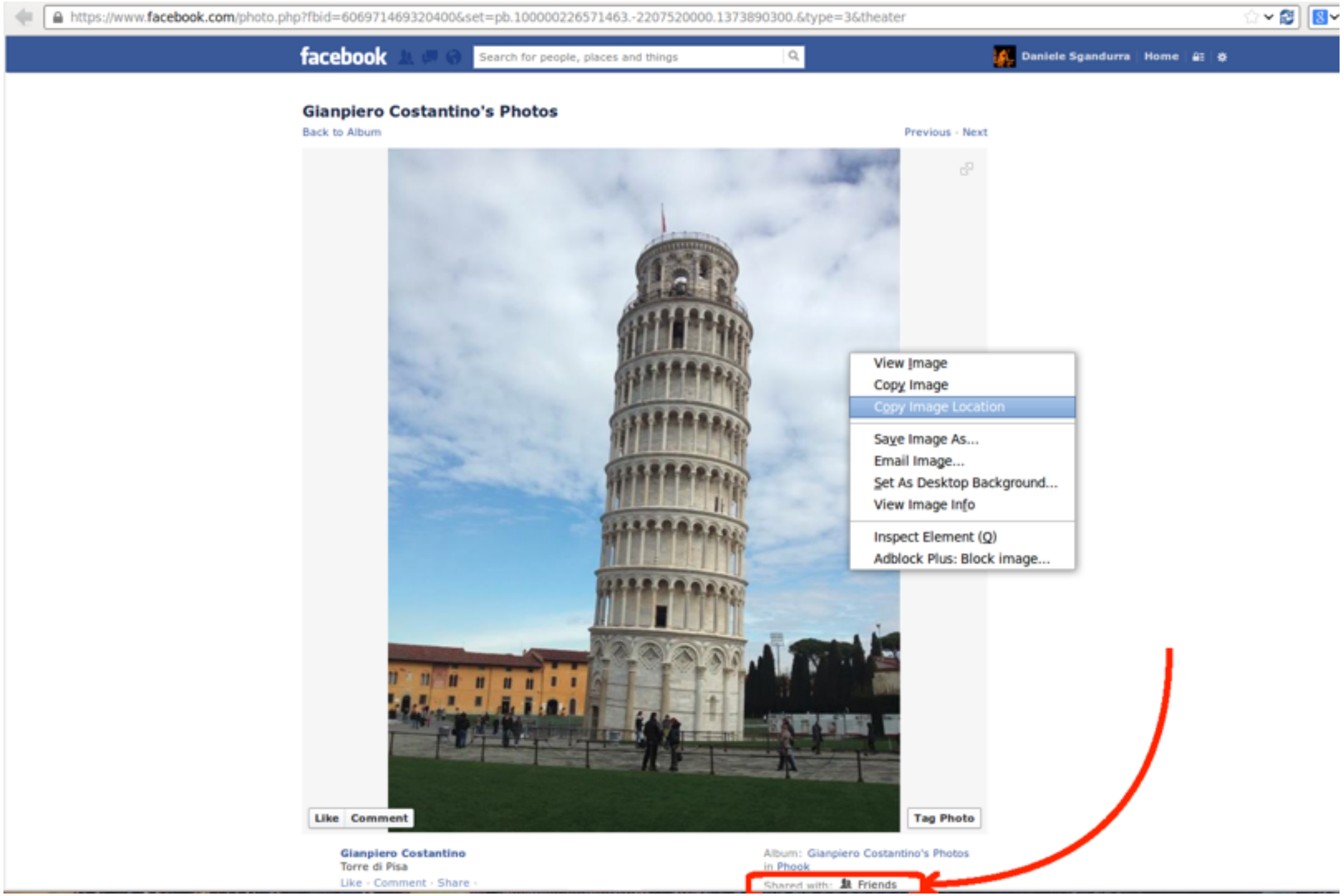


2) The photo is displayed

1) src = http//akamaihd..

This photo is available only to Friends

Case Study - A private photo (2)



https://www.facebook.com/photo.php?fbid=606971469320400&set=pb.100000226571463.-2207520000.1373890300.&type=3&theater

Gianpiero Costantino's Photos

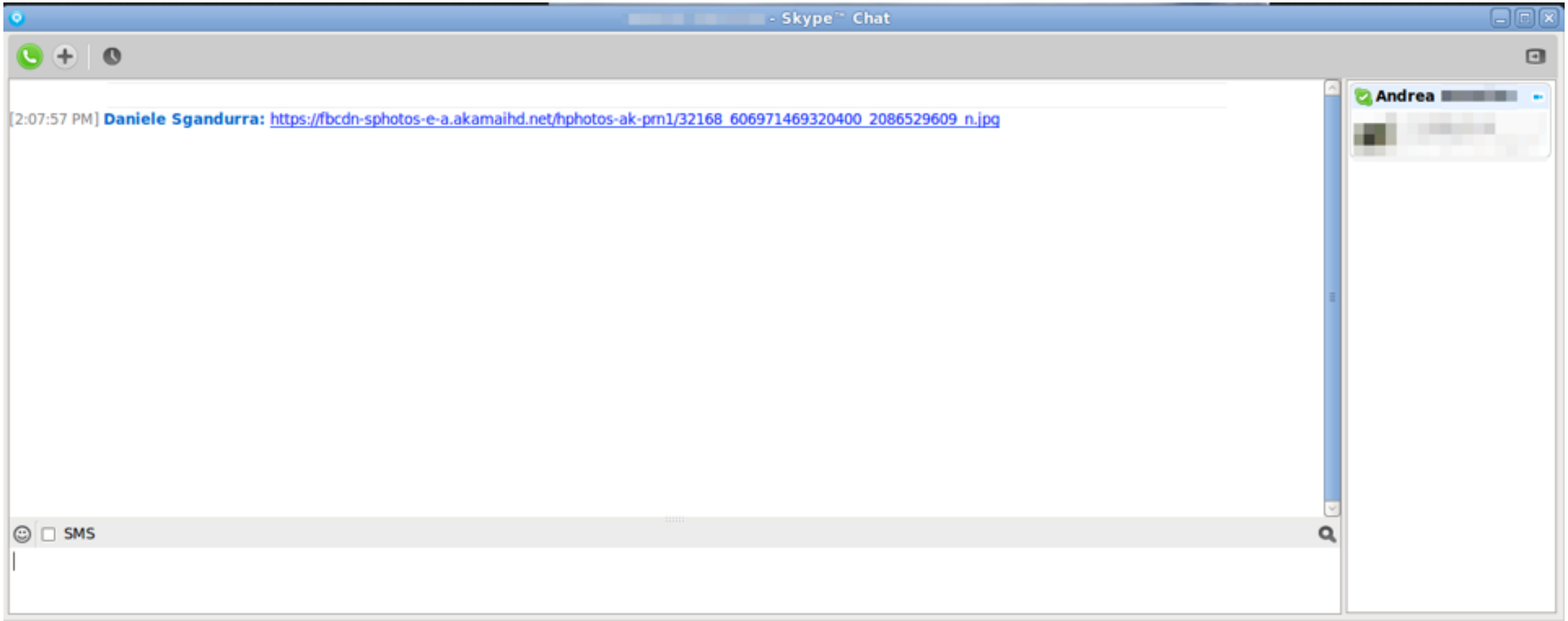
Gianpiero Costantino
Torre di Pisa

Album: Gianpiero Costantino's Photos
in Phook

Shared with: Friends

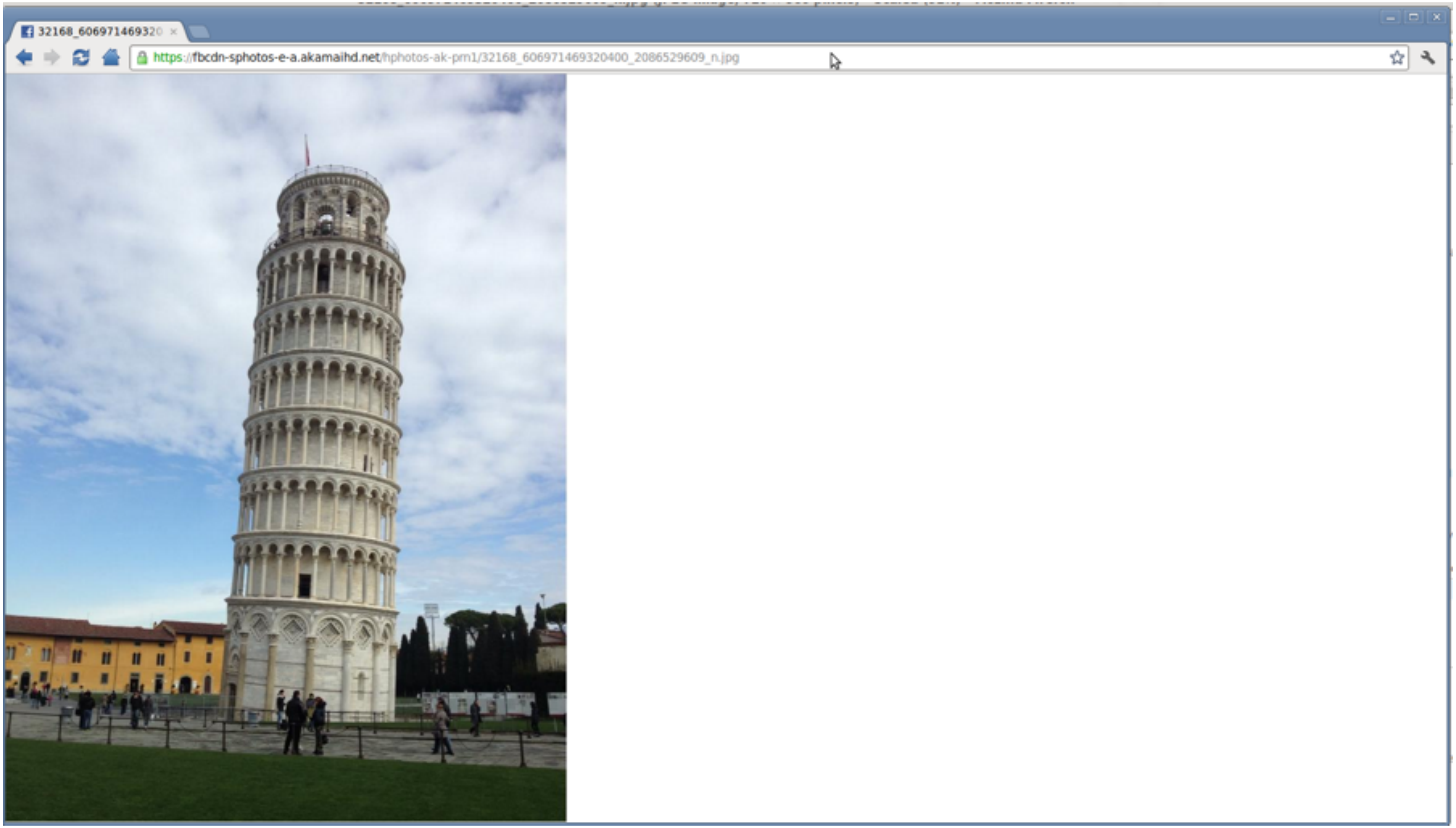
This photo is available only to Friends

Case Study - A private photo (3)



[2:07:57 PM] **Daniele Sgandurra:** https://fbcdn-sphotos-e-a.akamaihd.net/hphotos-ak-prn1/32168_606971469320400_2086529609_n.jpg

Case Study - A private photo (4)



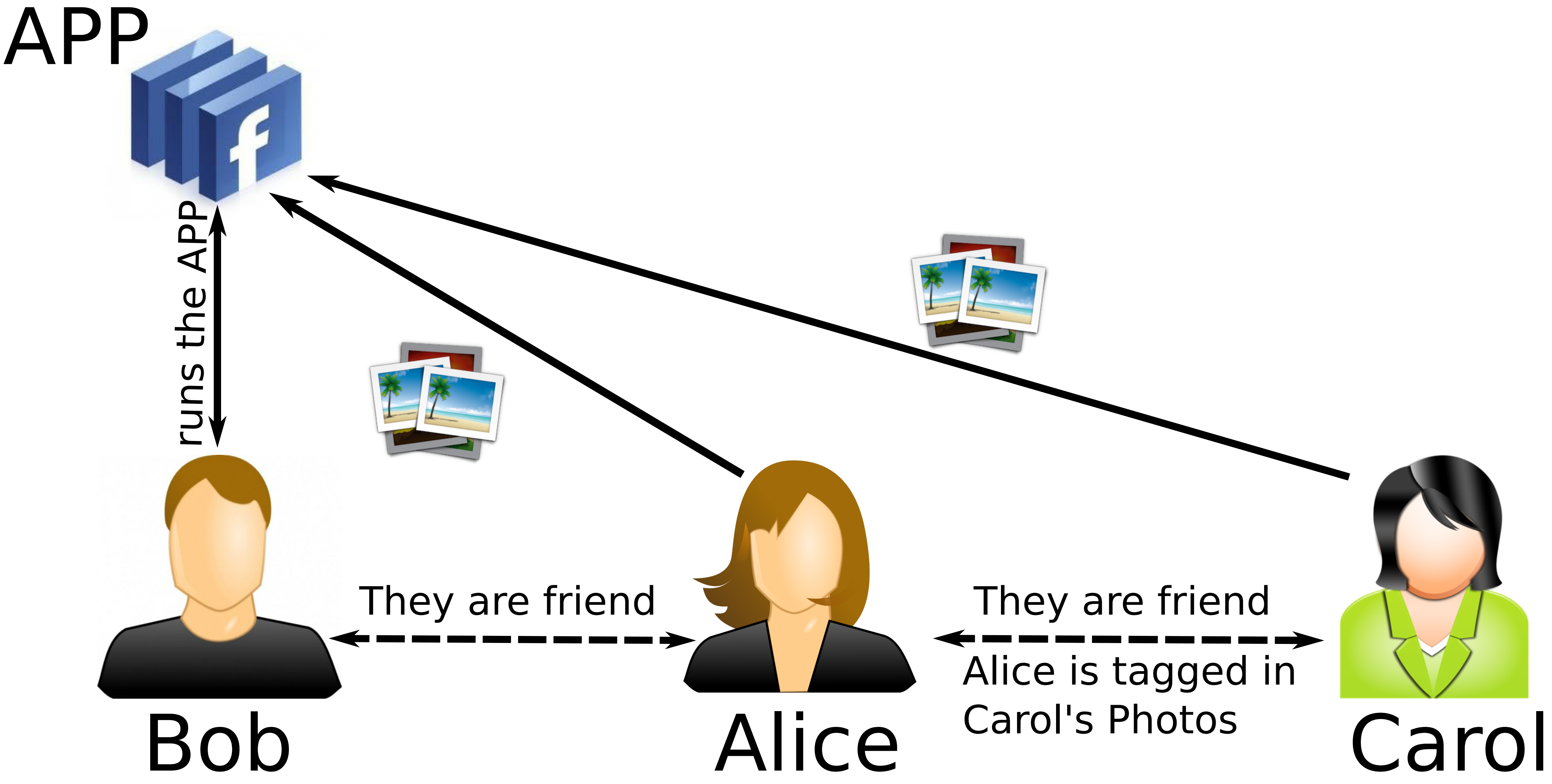
https://fbcdn-sphotos-e-a.akamaihd.net/hphotos-ak-prn1/32168_606971469320400_2086529609_n.jpg

This photo is available to Anyone

Case Study - Where is the “bug”?

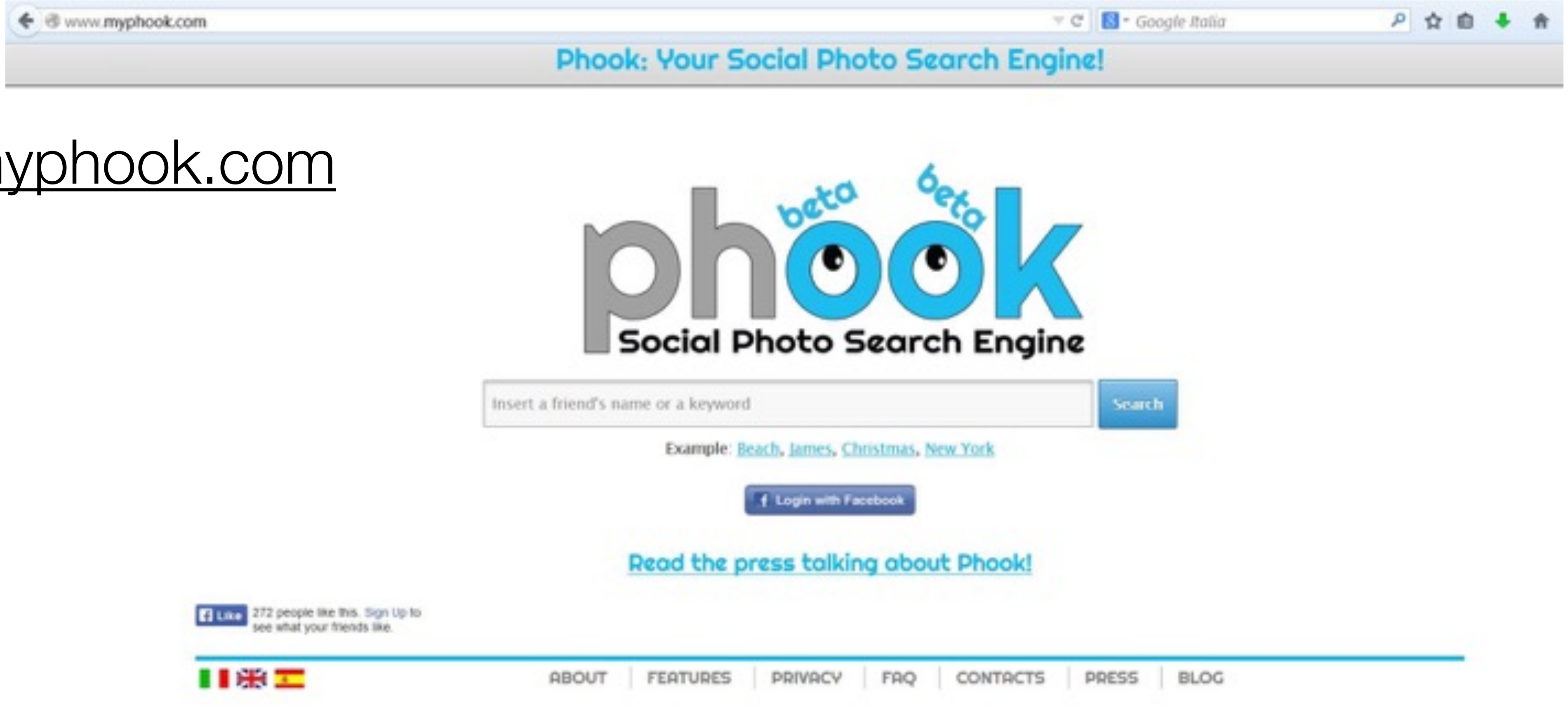
- Facebook uses a **C**ontent **D**elivery **N**etwork, i.e. Akamai, as service to store users’ photos
- Akamai does not enforce any access control to the photos
- **Any person**, connected to the Internet, will see photos of Facebook users’ just using the HTTP link

Implicit Transitive Agreement



The Phook *(Phoot-Book)* Experiment

www.myphook.com



Phook: Your Social Photo Search Engine!

Example: Beach, James, Christmas, New York

Read the press talking about Phook!

272 people like this. Sign Up to see what your friends like.

- It is a **photo-search** engine for Facebook
- It uses the *Implicit Transitive Agreement*
- More than 3500 Facebook users have joined Phook

The Phook Experiment (2)

- Phook does not download any photos, but uses only the link to Akamai
- Phook has a Database with more than **500millions** of links
- Users authorised Phook to crawl friends’ photos
- Access to photos is the same that users have set on Facebook

The Phook - Questions

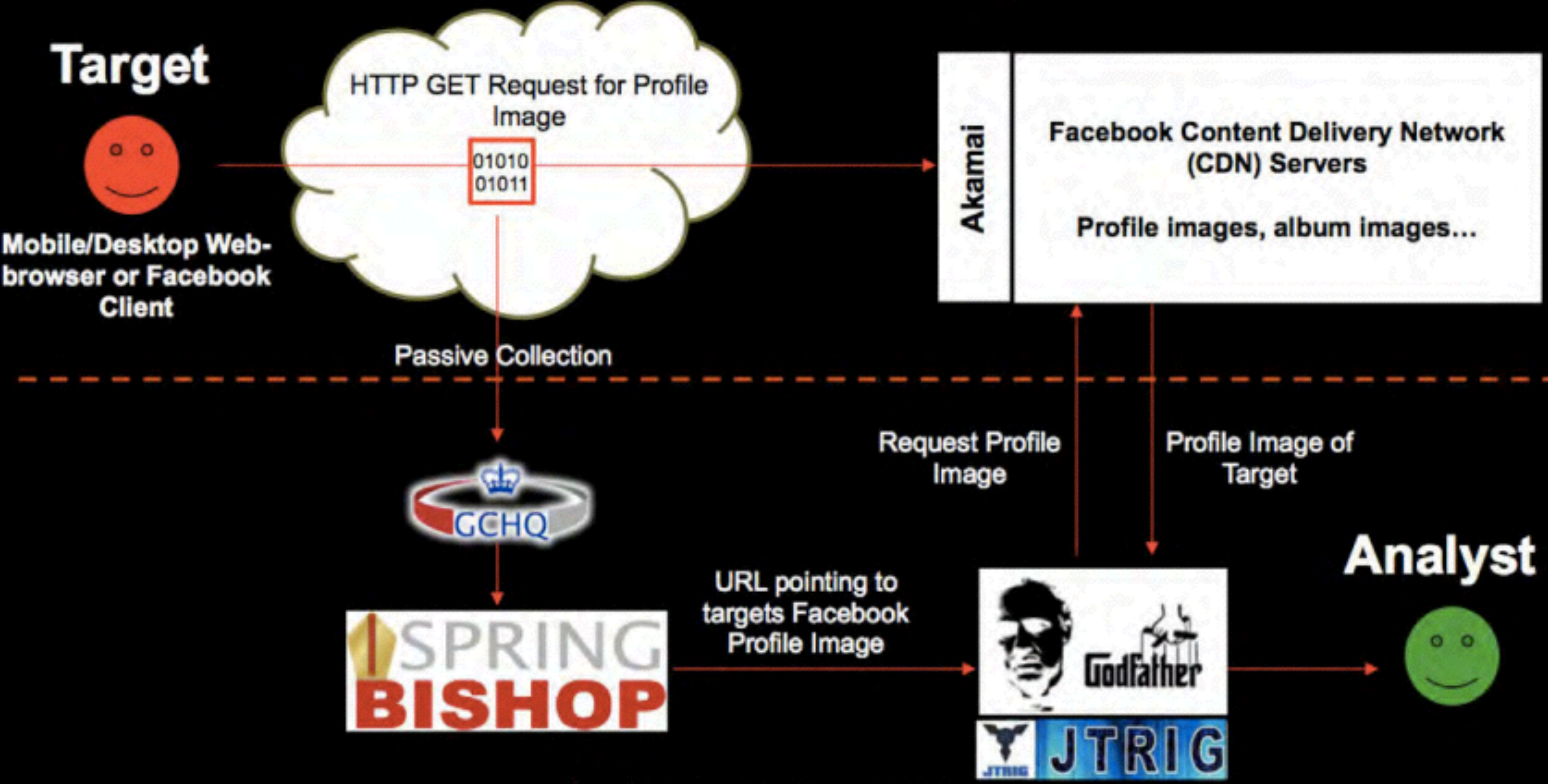
- What happens if we open the search option to the entire Database?

- Phook users **will see** photos of other Facebook users' just using the "**name**" of a person

- Not authorised users will not blocked since **Akamai does not enforce** any access control

- Now, do you think that your photos are still private?

Obtaining profile and album images



Target

Mobile/Desktop Web-browser or Facebook Client

HTTP GET Request for Profile Image

01010
01011

Akamai

Facebook Content Delivery Network (CDN) Servers

Profile images, album images...

Passive Collection

Request Profile Image

Profile Image of Target

SPRING BISHOP

URL pointing to targets Facebook Profile Image

Godfather

JTRIG

Analyst

Conclusion

- We have seen how OSNs manage our private photos
- We have seen that CDN does not enforce any access control on our private photos
- We have see how a honest Web-APP have collected millions of links…
    - What if it was developed with a malicious purpose?

“Do you will trust a bank that saves your deposit in a open safe located in a secret place?”