ACMmultimedia25

Privacy vs Multimedia Verification: A Conundrum

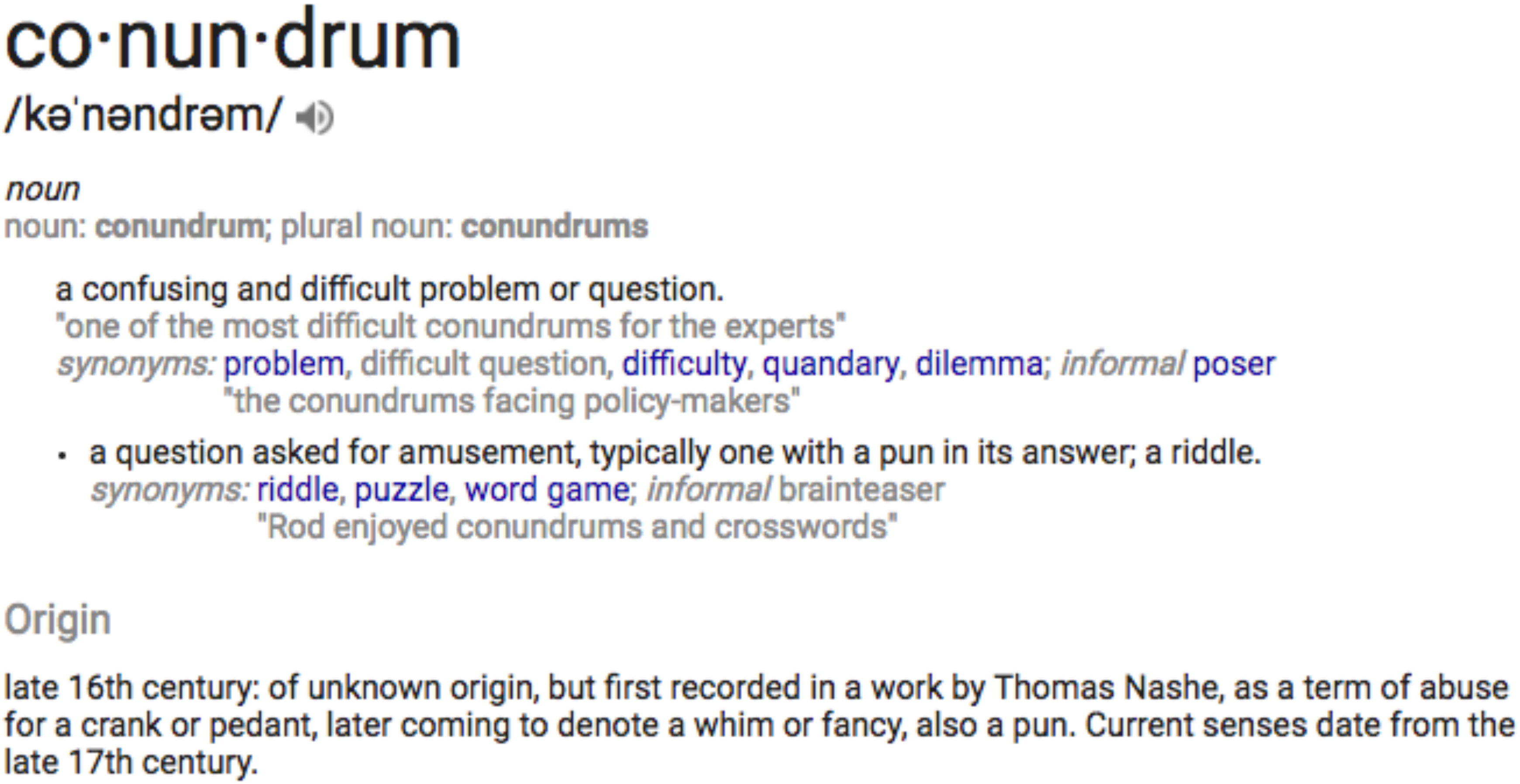
MuVer2017 Keynote

Gerald Friedland
Adjunct Assistant Professor, EECS, UC Berkeley
Principal Data Scientist, Lawrence Livermore National Lab

friedland@eecs.berkeley.edu

ACMmultimedia25

Conundrum



co·nun·drum

/kəˈnəndrəm/ 🔊

noun

noun: **conundrum**; plural noun: **conundrums**

a confusing and difficult problem or question.

"one of the most difficult conundrums for the experts"

synonyms: problem, difficult question, difficulty, quandary, dilemma; *informal* poser

"the conundrums facing policy-makers"

- a question asked for amusement, typically one with a pun in its answer; a riddle.

  synonyms: riddle, puzzle, word game; *informal* brainteaser

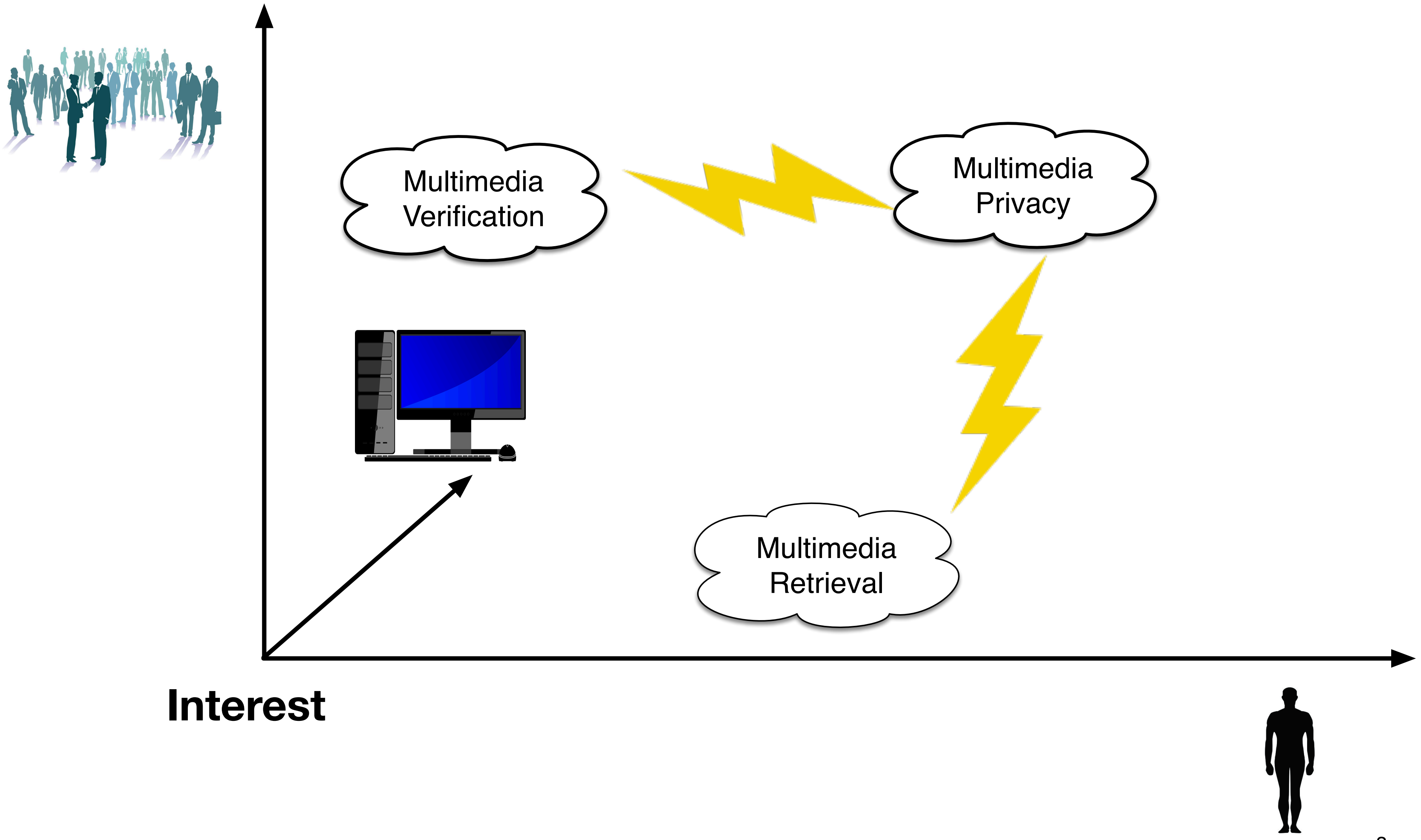
  "Rod enjoyed conundrums and crosswords"

Origin

late 16th century: of unknown origin, but first recorded in a work by Thomas Nashe, as a term of abuse for a crank or pedant, later coming to denote a whim or fancy, also a pun. Current senses date from the late 17th century.

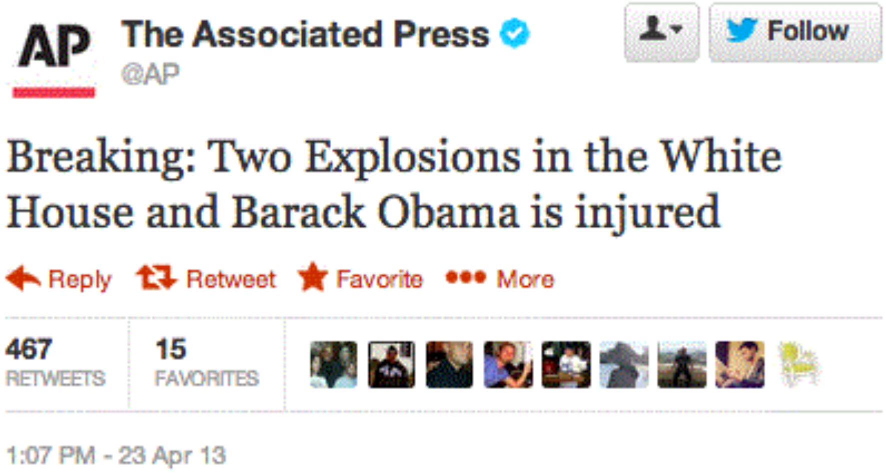
Source: google.com

Our Conundrum



ACMmultimedia25

Multimedia Verification


AP The Associated Press @AP

Follow

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

467 RETWEETS 15 FAVORITES

1:07 PM - 23 Apr 13

Given a social media post (e.g., comprising a text component, an associated piece of multimedia (image/ video) and a set of metadata originating from the social media platform), multimedia verification requires to return a decision on whether the information presented by this post sufficiently reflects the reality. The decision is often reduced to three classes: fake, real and unknown.

Multimedia Retrieval

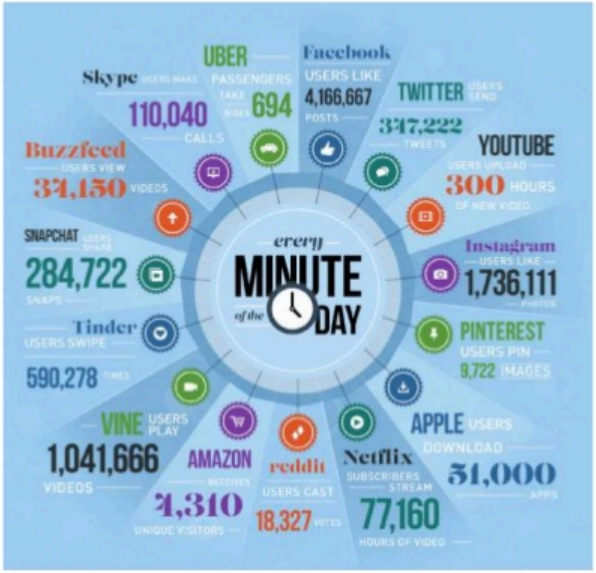
Source: LTI CS Carnegie Mellon University

See: G. Friedland: “Privacy vs. Multimedia Verification: A Conundrum”, Proceedings of ACM MuVer’17, October 27, 2017, Mountain View, CA, USA. https://doi.org/10.1145/3132384.3132389

ACMmultimedia25

Multimedia Privacy

Multimedia on the Internet Is Big!



Source:
Domosphere

Multimedia Privacy

Gerald Friedland
Symeon Papadopoulos
Julia Bernd
Yiannis Kompatsiaris

ACM Multimedia, Amsterdam, October 16, 2016

Ensuring that a multimedia post does not publish more information than intended by the user.

Social Cause for Conundrum

- Individuals want to post on the Internet and like a highly-personalized web experience.

- Industry is improving search and retrieval techniques so that people can find the posts.

- Governments improve search and retrieval to do forensics and intelligence gathering.

- Society relies on accurate information

- Individuals and Industry and Government wants to `bend reality’ in their favor.

Multimedia Privacy vs Retrieval

Hypothesis 1:

Individuals need for privacy is in agreement with society’s need for stability is in conflict with individual’s need for multimedia retrieval.

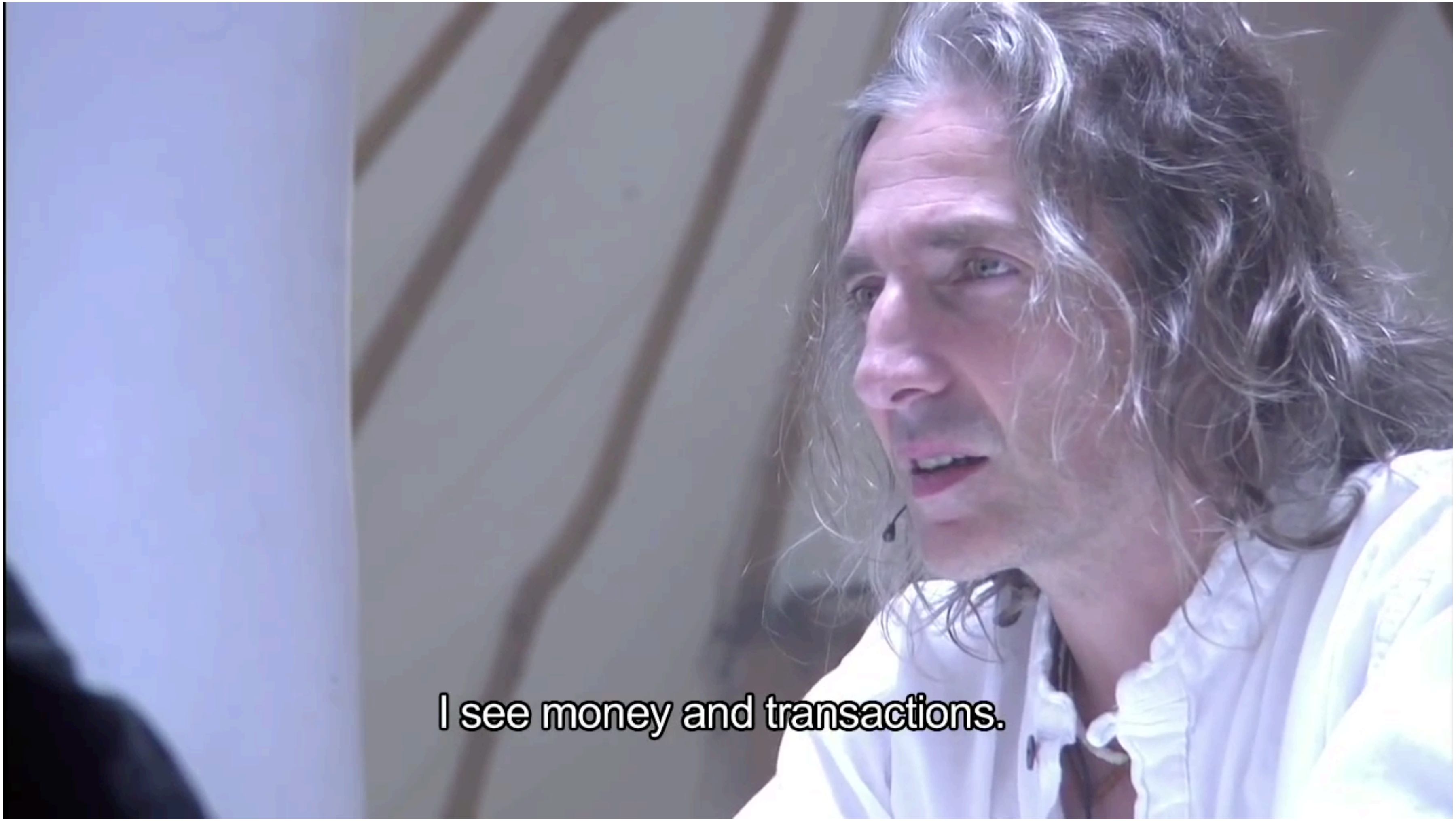
Proof as follows.

Cybercasing

Cybercasing: Using online data and services to enable real-world crimes.

G. Friedland and R. Sommer: "Cybercasing the Joint: On the Privacy Implications of Geotagging", Proceedings of the Fifth USENIX Workshop on Hot Topics in Security (HotSec 10), Washington, D.C, August 2010.

A Demonstration



Video at: https://www.youtube.com/watch?v=F7pYHN9iC9I

Threats that enable Cybercasing

Content reveals more than intended due to:

- implicit information in images and videos
- unexpected metadata
- Linkage of sites and inference
- De-anonymization

= Information used for retrieval.

Multimedia Privacy vs Retrieval

Therefore:

Individuals need for privacy is in agreement with society’s need for stability is in conflict with individual’s need for multimedia retrieval.

Q.E.D.

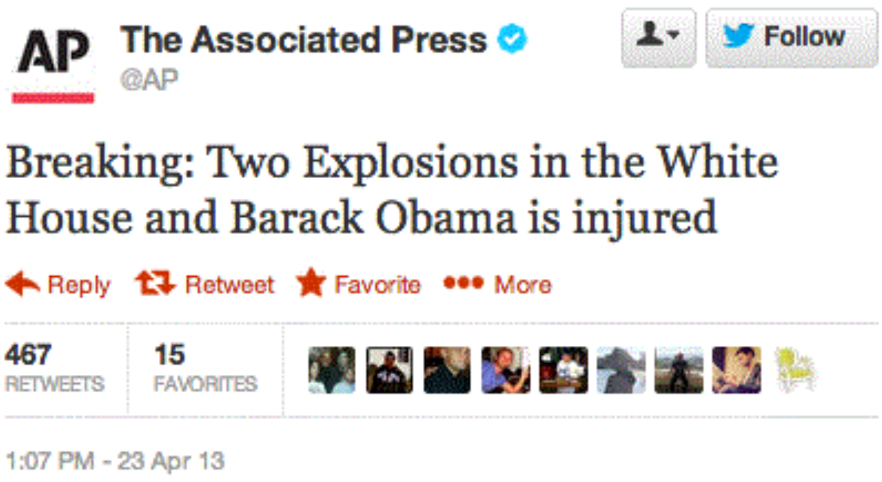
Multimedia Privacy vs Verification

Hypothesis 2:

Individuals need for privacy is in conflict with society’s need for multimedia verification.

Proof as follows.

Twitter Metadata



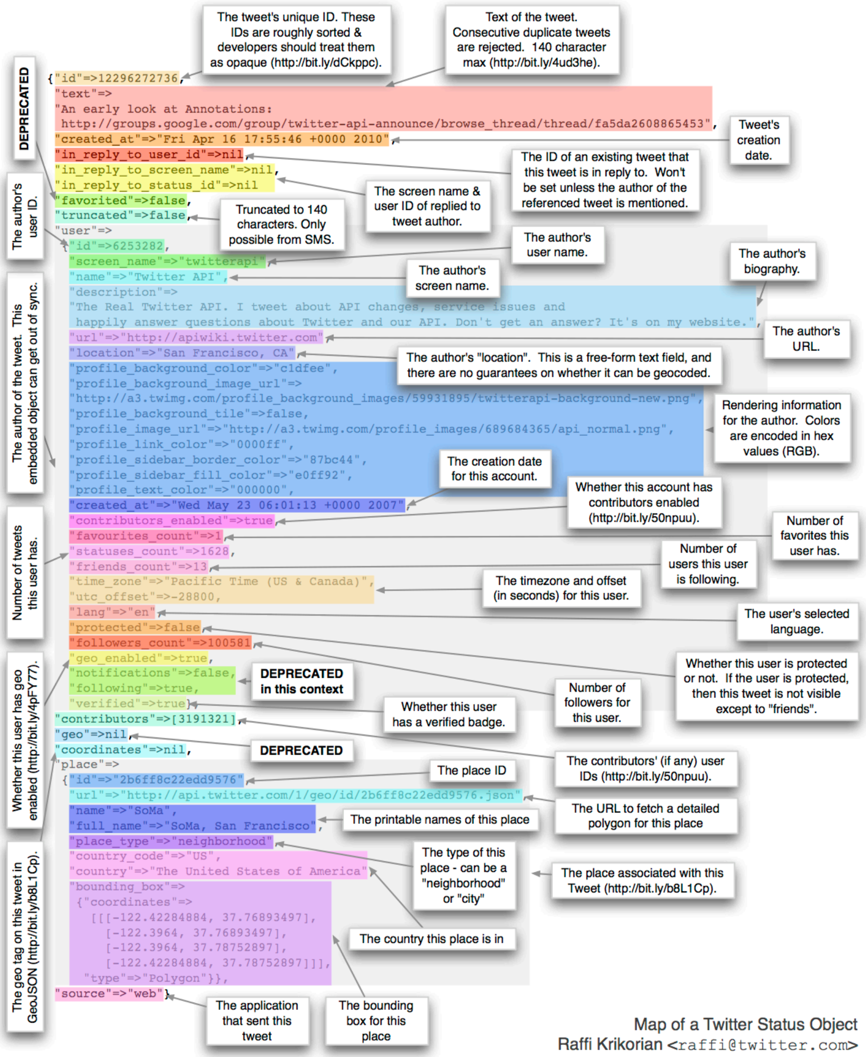
The Associated Press
@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

467 RETWEETS
15 FAVORITES

1:07 PM - 23 Apr 13

Source: twitter.com



```
{"id"=>12296272736,
 "text"=>
 "An early look at Annotations:
  http://groups.google.com/group/twitter-api-announce/browse_thread/thread/fa5da2608865453",
 "created_at"=>"Fri Apr 16 17:55:46 +0000 2010",
 "in_reply_to_user_id"=>nil,
 "in_reply_to_screen_name"=>nil,
 "in_reply_to_status_id"=>nil
 "favorited"=>false,
 "truncated"=>false,
 "user"=>
  {"id"=>6253282,
  "screen_name"=>"twitterapi",
  "name"=>"Twitter API",
  "description"=>
  "The Real Twitter API. I tweet about API changes, service issues and
   happily answer questions about Twitter and our API. Don't get an answer? It's on my website.",
  "url"=>"http://apiwiki.twitter.com",
  "location"=>"San Francisco, CA",
  "profile_background_color"=>"c1dfee",
  "profile_background_image_url"=>
  "http://a3.twimg.com/profile_background_images/59931895/twitterapi-background-new.png",
  "profile_background_tile"=>false,
  "profile_image_url"=>"http://a3.twimg.com/profile_images/689684365/api_normal.png",
  "profile_link_color"=>"0000ff",
  "profile_sidebar_border_color"=>"87bc44",
  "profile_sidebar_fill_color"=>"e0ff92",
  "profile_text_color"=>"000000",
  "created_at"=>"Wed May 23 06:01:13 +0000 2007",
  "contributors_enabled"=>true
  "favourites_count"=>1
  "statuses_count"=>1628,
  "friends_count"=>13
  "time_zone"=>"Pacific Time (US & Canada)",
  "utc_offset"=>-28800,
  "lang"=>"en"
  "protected"=>false
  "followers_count"=>100581
  "geo_enabled"=>true,
  "notifications"=>false,
  "following"=>true,
  "verified"=>true},
 "contributors"=>[3191321],
 "geo"=>nil,
 "coordinates"=>nil,
 "place"=>
  {"id"=>"2b6ff8c22edd9576",
  "url"=>"http://api.twitter.com/1/geo/id/2b6ff8c22edd9576.json"
  "name"=>"SoMa",
  "full_name"=>"SoMa, San Francisco",
  "place_type"=>"neighborhood"
  "country_code"=>"US",
  "country"=>"The United States of America"
  "bounding_box"=>
   {"coordinates"=>
     [[[-122.42284884, 37.76893497],
       [-122.3964, 37.76893497],
       [-122.3964, 37.78752897],
       [-122.42284884, 37.78752897]]],
    "type"=>"Polygon"}},
 "source"=>"web"}
```

The tweet's unique ID. These IDs are roughly sorted & developers should treat them as opaque (http://bit.ly/dCkppc).

Text of the tweet. Consecutive duplicate tweets are rejected. 140 character max (http://bit.ly/4ud3he).

Tweet's creation date.

DEPRECATED

The ID of an existing tweet that this tweet is in reply to. Won't be set unless the author of the referenced tweet is mentioned.

The screen name & user ID of replied to tweet author.

Truncated to 140 characters. Only possible from SMS.

The author's user ID.

The author's user name.

The author's screen name.

The author's biography.

The author of the tweet. This embedded object can get out of sync.

The author's URL.

The author's "location". This is a free-form text field, and there are no guarantees on whether it can be geocoded.

Rendering information for the author. Colors are encoded in hex values (RGB).

The creation date for this account.

Whether this account has contributors enabled (http://bit.ly/50npuu).

Number of favorites this user has.

Number of tweets this user has.

Number of users this user is following.

The timezone and offset (in seconds) for this user.

The user's selected language.

Whether this user is protected or not. If the user is protected, then this tweet is not visible except to "friends".

Number of followers for this user.

Whether this user has geo enabled (http://bit.ly/4pFY77).

DEPRECATED in this context

Whether this user has a verified badge.

DEPRECATED

The contributors' (if any) user IDs (http://bit.ly/50npuu).

The place ID

The URL to fetch a detailed polygon for this place

The printable names of this place

The type of this place - can be a "neighborhood" or "city"

The place associated with this Tweet (http://bit.ly/b8L1Cp).

The geo tag on this tweet in GeoJSON (http://bit.ly/b8L1Cp).

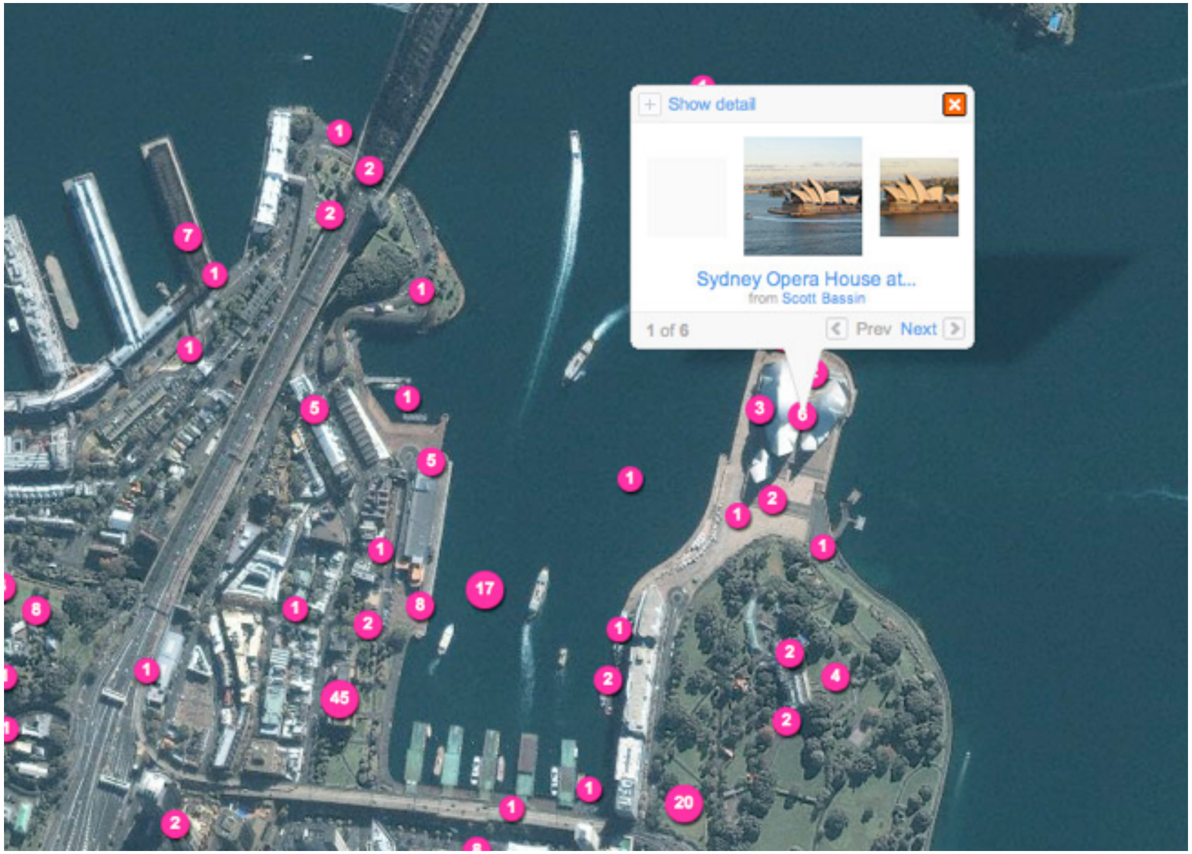
The country this place is in

The application that sent this tweet

The bounding box for this place

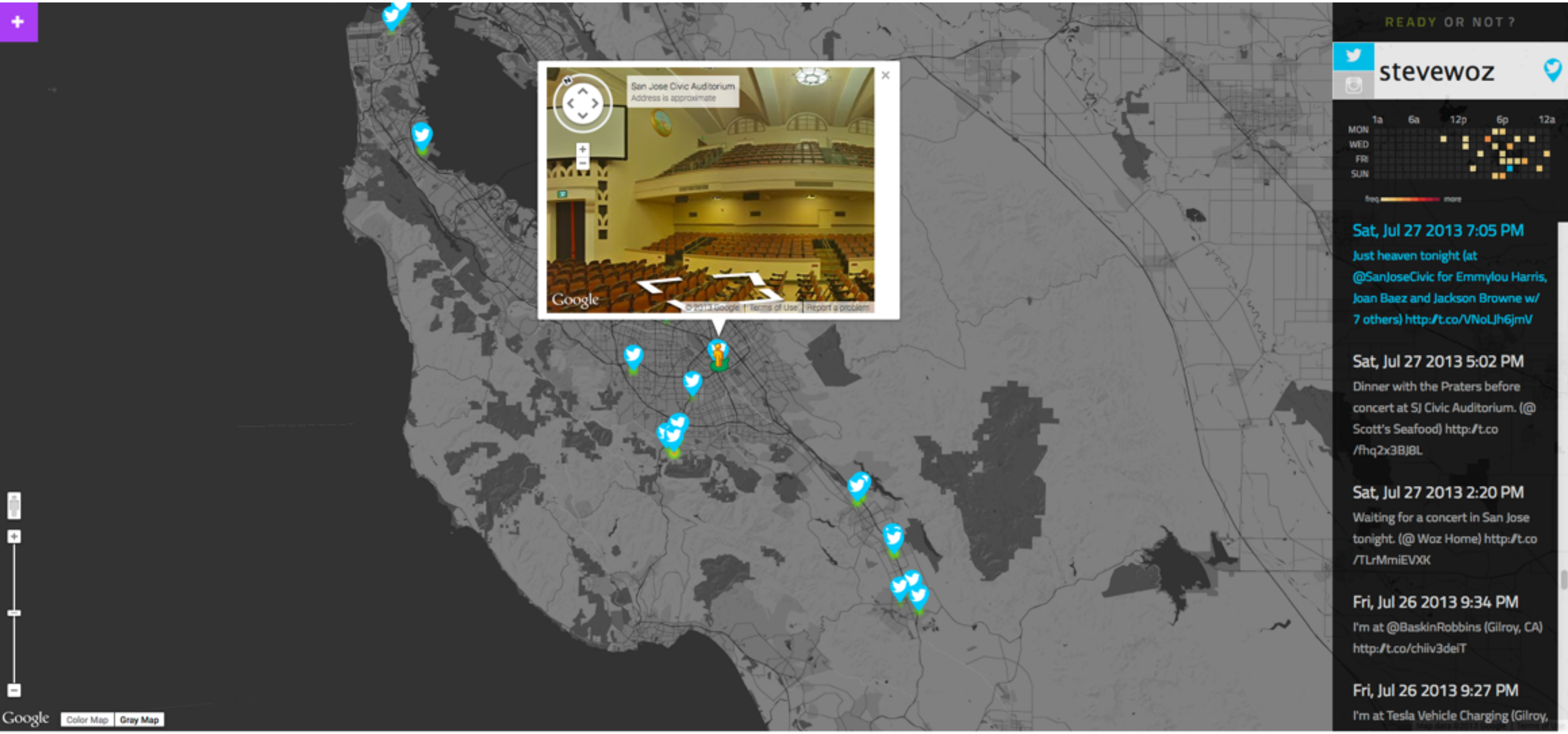
Map of a Twitter Status Object
Raffi Krikorian <raffi@twitter.com>
18 April 2010

Geo-Tagging



Allows easier clustering of photo and video series as well as additional services.

Ready Or Not?!?



Sat, Jul 27 2013 7:05 PM
Just heaven tonight (at @SanJoseCivic for Emmylou Harris, Joan Baez and Jackson Browne w/ 7 others) http://t.co/VNoLJh6jmV

Sat, Jul 27 2013 5:02 PM
Dinner with the Praters before concert at SJ Civic Auditorium. (@ Scott's Seafood) http://t.co/fhq2x3BJ8L

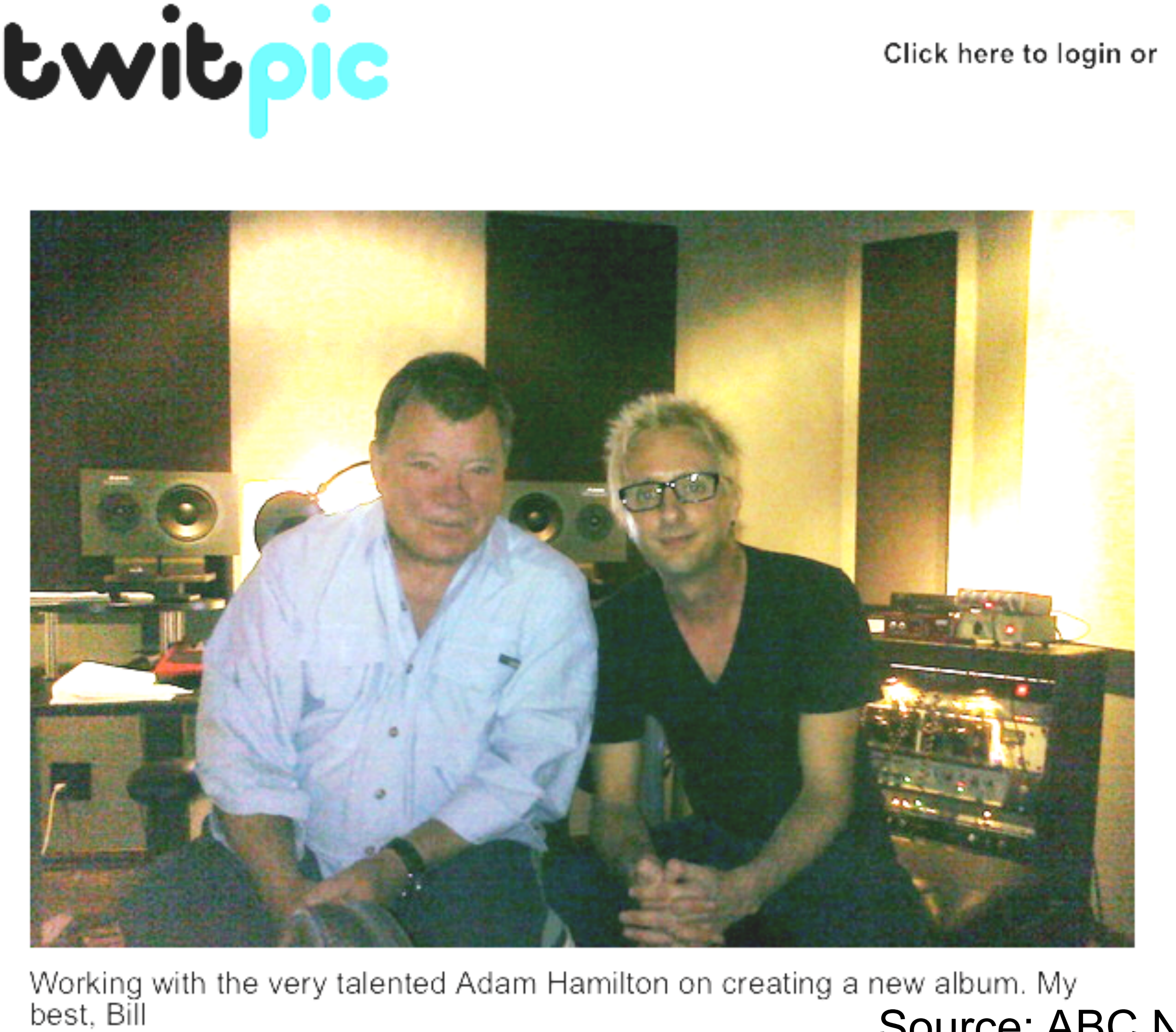
Sat, Jul 27 2013 2:20 PM
Waiting for a concert in San Jose tonight. (@ Woz Home) http://t.co/TLrMmiEVXK

Fri, Jul 26 2013 9:34 PM
I'm at @BaskinRobbins (Gilroy, CA) http://t.co/chiiv3deiT

Fri, Jul 26 2013 9:27 PM
I'm at Tesla Vehicle Charging (Gilroy,

http://teachingprivacy.org

Celebrities unaware of Geo-Tagging

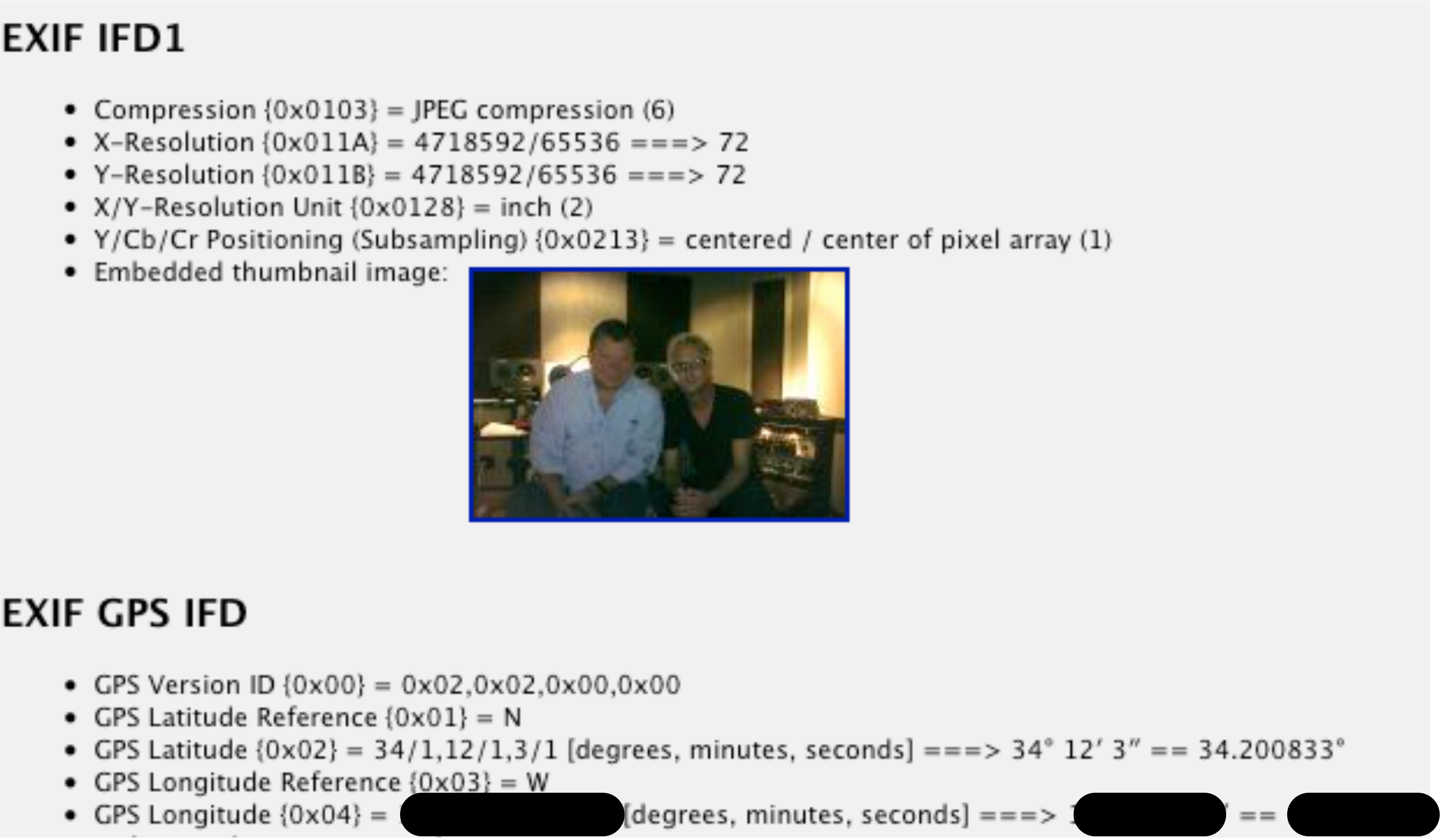


Click here to login or

Working with the very talented Adam Hamilton on creating a new album. My best, Bill

Source: ABC News

Celebrities unaware of Geo-Tagging



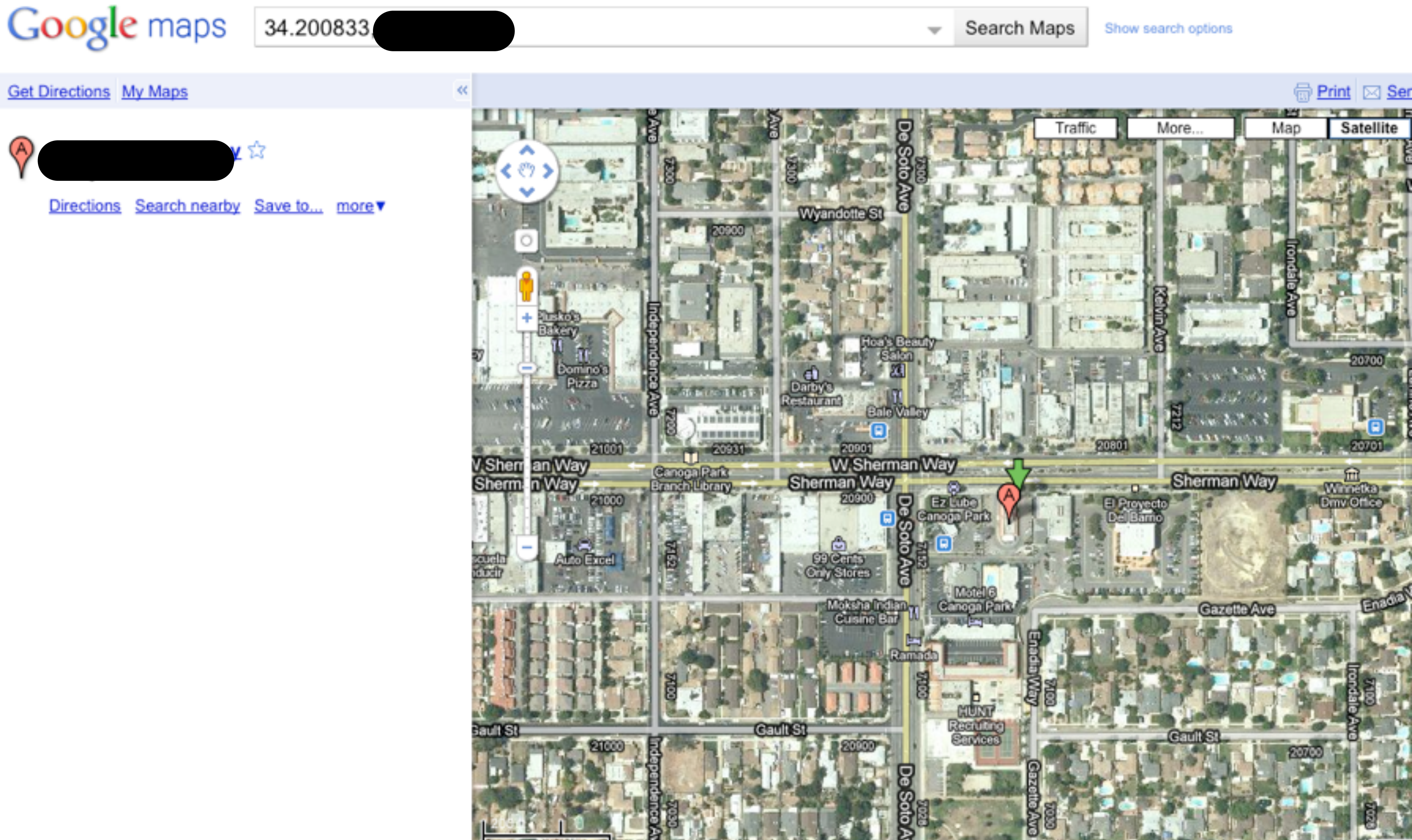
EXIF IFD1

- Compression {0x0103} = JPEG compression (6)
- X-Resolution {0x011A} = 4718592/65536 ===> 72
- Y-Resolution {0x011B} = 4718592/65536 ===> 72
- X/Y-Resolution Unit {0x0128} = inch (2)
- Y/Cb/Cr Positioning (Subsampling) {0x0213} = centered / center of pixel array (1)
- Embedded thumbnail image:

EXIF GPS IFD

- GPS Version ID {0x00} = 0x02,0x02,0x00,0x00
- GPS Latitude Reference {0x01} = N
- GPS Latitude {0x02} = 34/1,12/1,3/1 [degrees, minutes, seconds] ===> 34° 12′ 3″ == 34.200833°
- GPS Longitude Reference {0x03} = W
- GPS Longitude {0x04} = [redacted] [degrees, minutes, seconds] ===> [redacted] == [redacted]

Google Maps shows Address...



Google maps

34.200833[redacted]

Search Maps

Show search options

Get Directions | My Maps

[redacted] ☆

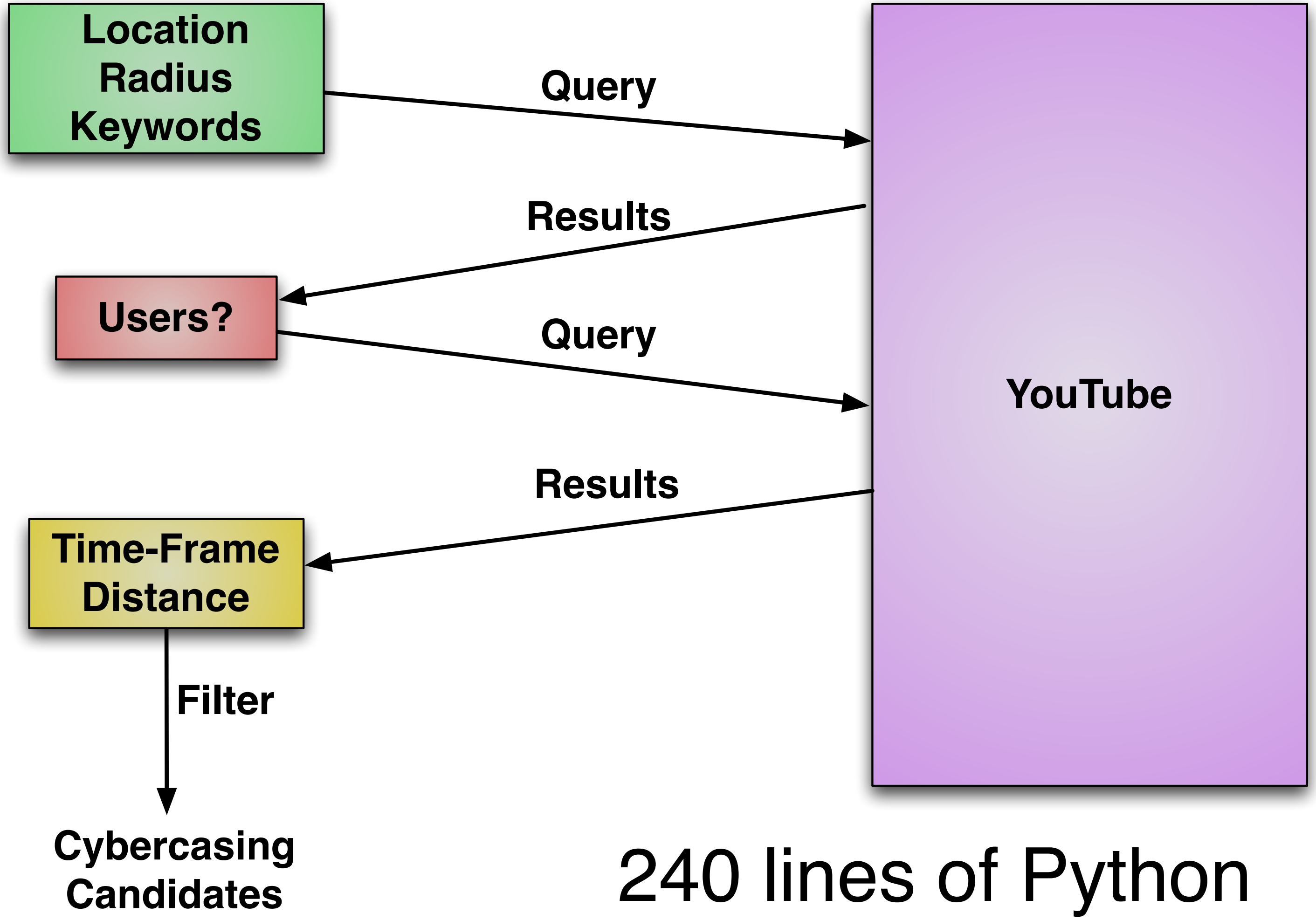
Directions Search nearby Save to... more▼

ACMmultimedia25

Case Study: YouTube

Can we find homes of people currently on vacation using YouTube?

Cybercasing on YouTube



240 lines of Python

Cybercasing on YouTube

Input parameters

Location: `37.869885,-122.270539`
Radius: `100km`
Keywords: `kids`
Distance: `1000km`
Time-frame: `this_week`

Cybercasing on YouTube

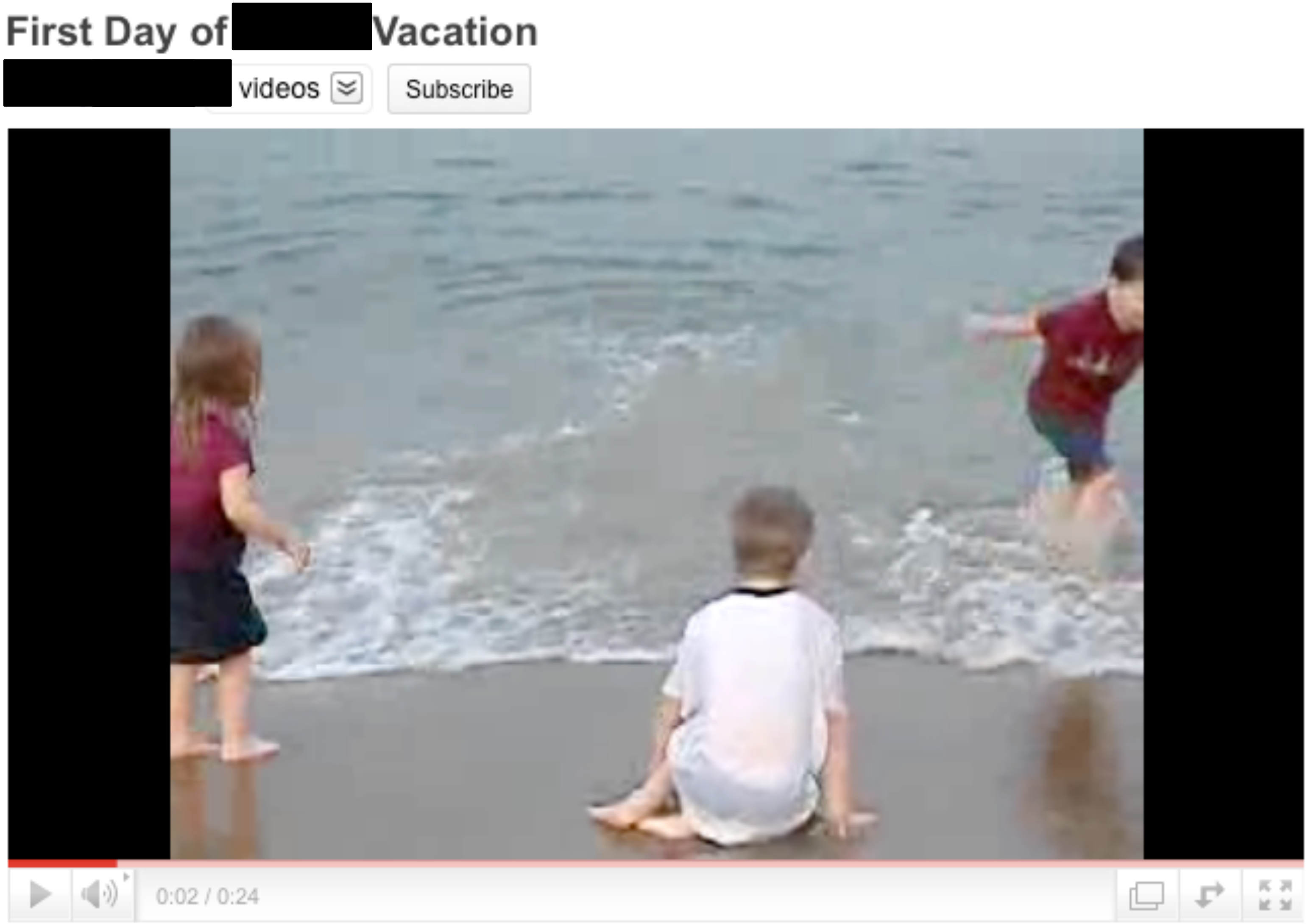
Ou

In

➡

➡

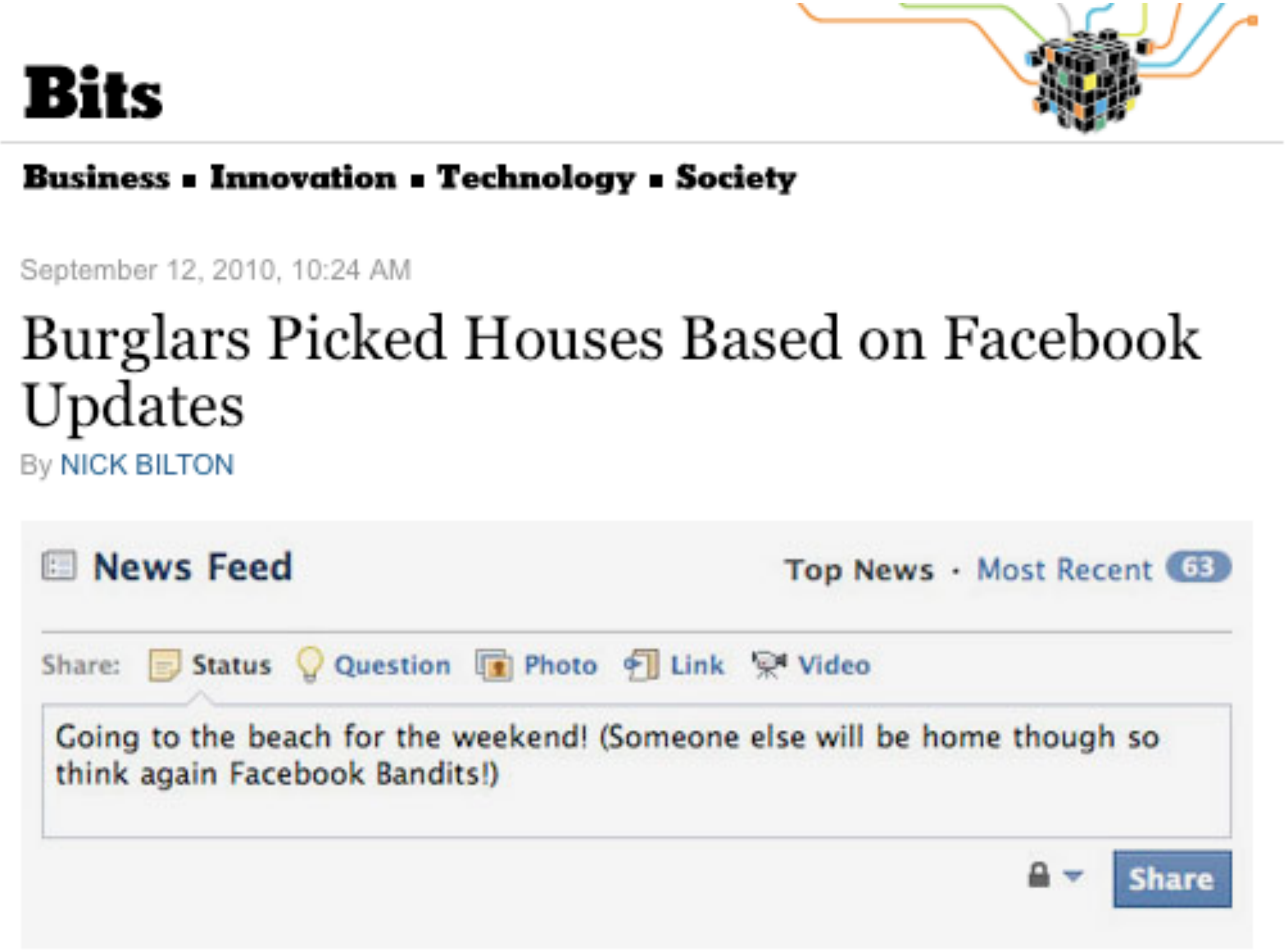
➡



First Day of [redacted] Vacation

[redacted] videos

The Threat is Real!



Bits

Business ▪ Innovation ▪ Technology ▪ Society

September 12, 2010, 10:24 AM

Burglars Picked Houses Based on Facebook Updates

By NICK BILTON

News Feed
Top News · Most Recent 63
Share: Status Question Photo Link Video

Going to the beach for the weekend! (Someone else will be home though so think again Facebook Bandits!)

Illustration by Nick Bilton/The New York Times

Multimedia Privacy vs Verification

Therefore:

Individuals need for privacy is in conflict with society’s need for multimedia verification.

Q.E.D.

Multimedia Privacy vs Verification

Hypothesis 3:

Individuals’ need for privacy is in conflict with computers’ abilities to automatize multimedia verification and retrieval.

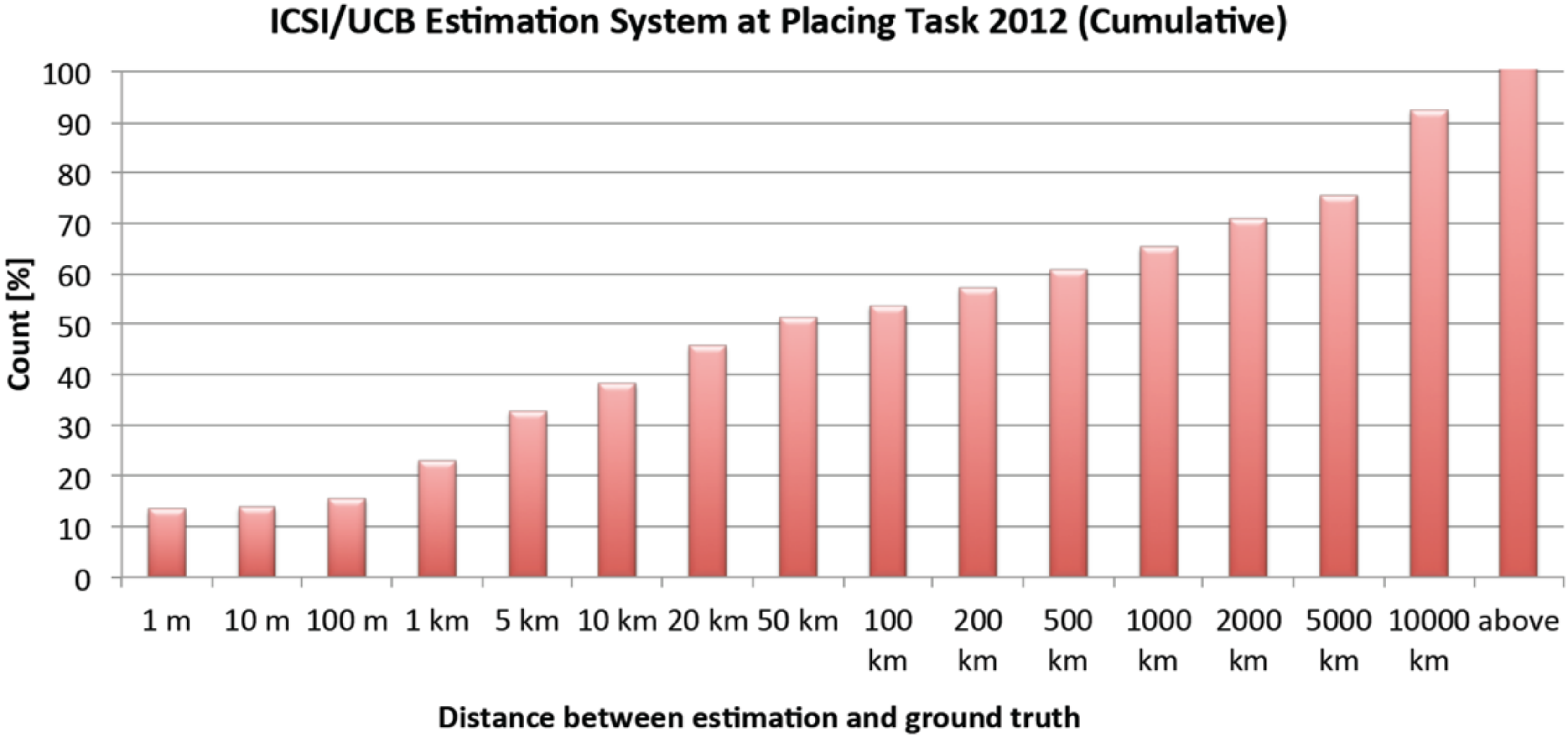
Proof as follows.

ACMmultimedia25

MediaEval Benchmark

MediaEval Benchmarking Initiative for Multimedia Evaluation

The "multi" in multimedia: speech, audio, visual content, tags, users, context



J. Choi, G. Friedland, V. Ekambaram, K. Ramchandran: "Multimodal Location Estimation of Consumer Media: Dealing with Sparse Training Data," in Proceedings of IEEE ICME 2012, Melbourne, Australia, July 2012.

ACMmultimedia25

YouTube Cybercasing Revisited

	Old Experiment	No Geotags
Initial Videos	1000 (max)	107
User Hull	~50k	~2000
Potential Hits	106	112
Actual Targets	>12	>12

Accuracy with Geo-Tags vs Multimodal Location Estimation

J. Choi, G. Friedland: “Semantic Computing and Privacy: A Case Study using Inferred Geo-Location”, International Journal Semantic Computing 05, 79 (2011).

Anonymity vs Multimedia Verification

Idea: Can one link videos across acounts?

(e.g. YouTube linked to Facebook vs anonymized dating site)

Dataset

- Test videos from Flickr (~40 sec)
- 121 users to be matched, 50k trials
- 70% heavy noise
- 50% speech
- 3% professional content

H. Lei, J. Choi, A. Janin, and G. Friedland: "Persona Linking: Matching Uploaders of Videos Across Accounts", at IEEE International Conference on Acoustic, Speech, and Signal Processing (ICASSP), Prague, May 2011.

Matching Users based on Flickr

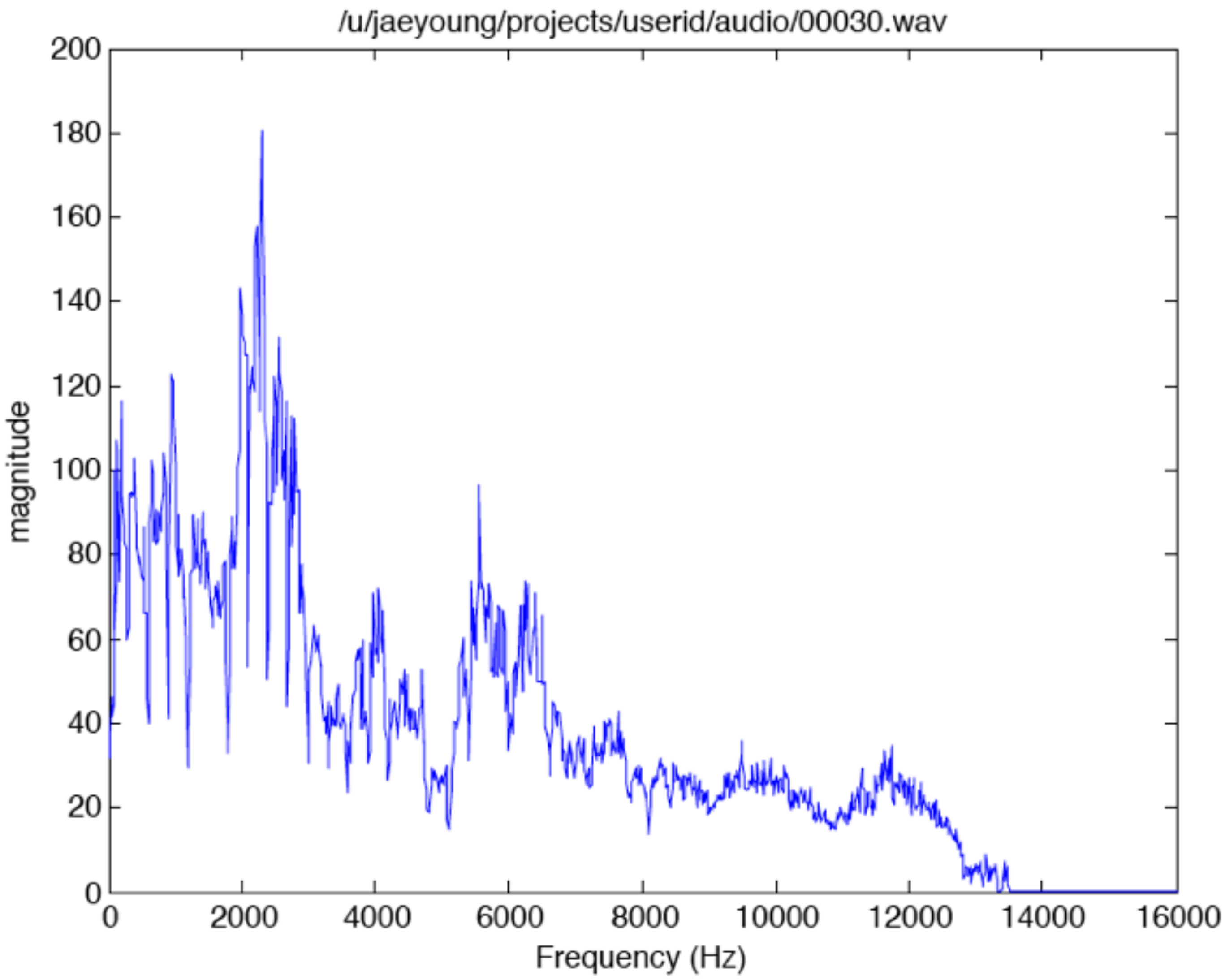
Algorithm:

1) Take the 10 seconds of the sound track of a video

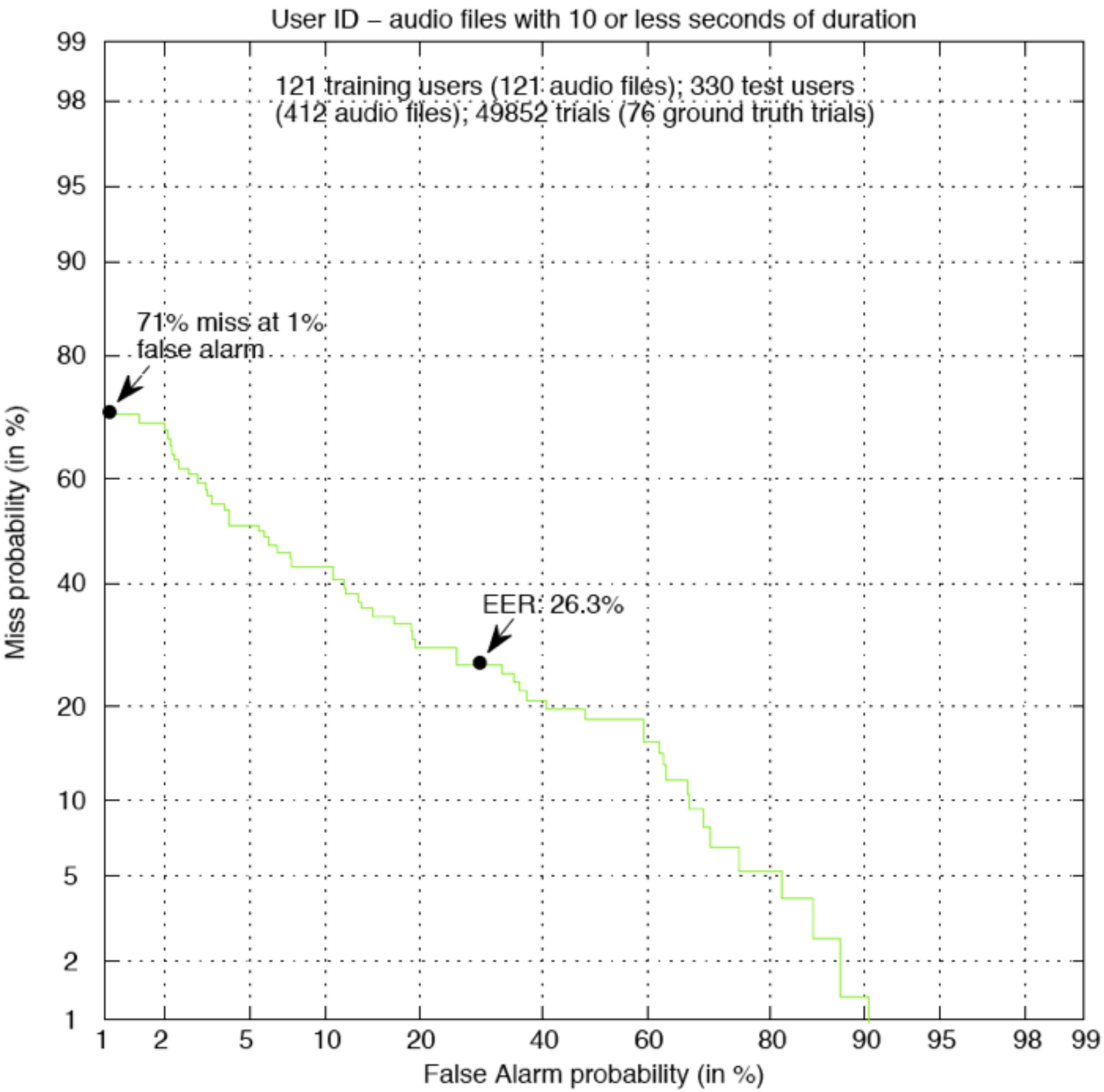
2) Extract the Spectral Envelope

3) Compare using Manhattan Distance

Spectral Envelope



User ID on Flickr videos



Persona Linking using Internet Videos

Result:

On average having 40 seconds in the test and training set leads to a 99.2% chance for a true positive match!

ACMmultimedia25

Multimedia Privacy vs Verification

Therefore:

Individuals’ need for privacy is in conflict with computers’ abilities to automatize multimedia verification and retrieval.

Q.E.D.

Conclusion

- Multimedia Retrieval and Verification have a conflict of interest with Multimedia Privacy on individual, societal and computational level.

- As technology is developed on both sides, it creates an arms race. Where will it end?

- Need research and education to prevent disaster?

Thank You!

Questions?

Work together with:

Jaeyoung Choi, Luke Gottlieb, Robin Sommer, Howard Lei, Adam Janin, Oana Goga, Nicolas Weaver, Dan Garcia, Julia Bernd, and others.

Thank You!

Acknowledgements: This material is based upon work supported by the US National Science Foundation under Grant No. CNS-1065240 and CNS-1514509. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.