

ETHICOMP 2011
Sheffield 16 sept 2011

Face Recognition and Privacy enhancing techniques

Alberto Cammozzo

*Fellow, Technology and Innovation workgroup
for Public Administration, University of Padova*

Founder, TagMeNot.info



Face recognition is an HOT topic



Google

Google warns against facial recognition database

Google's Executive Chairman Eric Schmidt has warned Governments against 'foolish' legislation – and said facial recognition is too creepy even for Google



Eric Schmidt: 'I am incredibly optimistic about what is going to be possible in the next decade, we have spent our whole career getting to this point' Photo: AFP

Follow us on... [facebook](#) [twitter](#) [RSS](#)

SPONSORED FEATURES

TECHNOLOGY MOST VIEWED

TODAY PAST WEEK PAST MONTH

1. El Shaddai: Ascension of the Metatron review
2. Student facing extradition to US over TV website is bailed
3. Millions of Hotmail users cut off by Microsoft 'cloud' failure
4. Dead Island review
5. Samsung loses appeal against Galaxy Tab ban

TECHNOLOGY CHOICE

Playing God: video games with religious themes



With the Enoch-inspired El Shaddai: Ascension of the Metatron out next

Sign in with       or [Create a New Account.](#)[PCWorld](#) » [Blogs](#) » [Today @ PCWorld](#)

Recommend:



Email

86 Comments [Print](#)

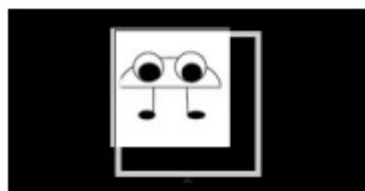
TODAY @ PCWORLD

Why Facebook's Facial Recognition is Creepy

By Sarah Jacobsson Purewal, PCWorld Jun 8, 2011 5:46 AM

I'm not sure if you've heard the news, but Facebook is officially getting super-creepy. Facebook announced Tuesday that it will be [implementing facial recognition technology](#) for all users in the next few weeks, semi-automating the photo-tagging process.

Sure, you can "opt-out" of the service, but it's a pretty weak consolation. After all, opting out won't keep Facebook from gathering data and recognizing your face--it'll just keep people from tagging you automatically.



The new facial recognition technology, which was announced in December but only introduced to a small test group, is basically Facebook's way of creating a huge, photo-searchable database of its users. And yes, [it's terrifying](#).

**Subscribe to the Windows News
Newsletter** - weekly[See All Newsletters »](#)

Similar Articles:

[Why Facebook Facial Recognition is Creepy: Redux](#)[Facebook Photo Tagging Guide](#)[Facebook Facial Recognition Security Firm Issues Alert](#)[Facebook Facial Recognition Quiet Rise and Danger](#)[Facebook's Facial Recognition Flops](#)

News and Views » Straight Talk

ICBC offers facial-recognition technology to Vancouver police's riot investigation



Michael Caswell

A fire burns on the street during the Stanley Cup riot.



131



0



Like

12

Comments (16) 

By **Stephen Hui**, June 17, 2011

Since 2009, the Insurance Corporation of B.C. has used [facial-recognition technology](#) to catch theft and fraud related to driver licences.

Now, the Crown corporation is offering to let Vancouver police use this technology for a very different purpose—to nab [rioters](#) who committed crimes in the wake of the Canucks' Stanley Cup loss.

Vancouver Listings

Movies

Music

Dining

Arts

Clubs

Events






search listings

GO

Most Popular

Viewed

Commented

1. Ke\$ha misses the mark on a cartwheel at Vancouver concert
2. Ke\$ha refreshingly real in Vancouver
3. Vancouver prepares to turn parks into earthquake response areas
4. RBC GranFondo Whistler bike ride to bring traffic closures on September 10
5. Gwynne Dyer: The real potential for naval conflicts around the world  Comments (1)
6. Vancouver lawyer Gail Davidson seeks Dick Cheney's arrest  Comments (30)
7. Even big pubes aren't funny in Bucky Larson: Born to Be a Star
8. Dick Cheney demonstration planned in Vancouver  Comments (8)
9. Your horoscope for September 8 to 14, 2011  Comments (1)
10. 6.4-magnitude earthquake off Vancouver Island felt in Metro Vancouver  Comments (6)



Face recognition technology fails to find UK rioters

› 18 August 2011 by [Niall Firth](#)

› Magazine issue [2826](#). [Subscribe and save](#)

› For similar stories, visit the [Crime and Forensics](#) Topic Guide

THE response was as aggressive and swift as the riots themselves. Within a few hours of the worst of last week's looting across London and other English cities, attempts were being made to use CCTV footage to track down the individuals who had plundered shops and destroyed buildings.

But those raised on a diet of TV police dramas who expected crack law enforcement teams to simply plug the footage into a computer and then print out a list of suspects are going to be disappointed. The poor quality of most CCTV footage makes it almost impossible to trust standard automated facial recognition techniques.

One of the most common methods used to help identify an individual from camera footage is photoanthropometry, which uses "proportionality indices" to compare a picture of a suspect on a police database, say, with a CCTV image. Key points on a person's face - such as the chin, edge of the nose, or centre of the top lip - are marked and the distance between them measured. Someone experienced with this technique can then judge whether the two faces match.



PRINT



SEND



SHARE



Police want to identify these men (Image: Metropolitan Police/AP/PA)

This week's issue

Subscribe



10 September 2011



ARTICLE

COMMENTS (53)

MORE REUTERS RESULTS FOR:

"moris mobile offender police"

Reuters Mobile

Tue, Apr 27 2010

Police to begin iPhone iris scans amid privacy concerns

Wed, Jul 20 2011

Follow Reuters



Facebook



Twitter



RSS



YouTube

MOST POPULAR

READ

- 1 Egyptian protesters pull down Israel embassy wall
09 Sep 2011
- 2 Microsoft lines up its big swing at tablets
07 Sep 2011



ians online for

ands to three

after embassy

Police to begin iPhone iris scans amid privacy concerns

[Recommend](#)

[f](#) 3351 recommendations. [Sign Up](#) to see what your friends recommend.



By Zach Howard

CONWAY, Mass | Wed Jul 20, 2011 2:59pm EDT

(Reuters) - Dozens of police departments nationwide are gearing up to use a tech company's already controversial iris- and facial-scanning device that slides over an iPhone and helps identify a person or track criminal suspects.

[Tweet](#) 687

[in](#) Share 92

[f](#) Share this

[+1](#) 22

[Email](#)

[Print](#)

Related News

[Cameron "regrets" hiring scandal-hit tabloid editor](#)

Wed, Jul 20 2011

[Special report: With Alzheimer's in the genes, when do you test?](#)

Wed, Jul 20 2011

[Special Report: Murdoch affair spotlights UK's dirty detectives](#)

Wed, Jul 20 2011

["Humble" Murdoch defends record, attacked by protester](#)

Tue, Jul 19 2011

Press Release

About Gatwick

Business Opportunities

Gatwick Performance

Sustainability

Investment

Investor Relations

Media Centre

Gatwick blog



Speeches & presentations



Press releases



More passengers embracing hi-tech border controls at Gatwick Airport 6 September 2011

More passengers travelling to the UK via Gatwick Airport are opting to use the hi-tech **facial recognition** gates to clear border control.

The e-Passport gates at the airport's North Terminal were used by 289,604 passengers between April 2010 and the end of March 2011, an average of 24,133 per month. But since April 1 this year until the end of July an average of 43,068 passengers have used the e-Passport gates each month.

The state-of-the-art gates, which can be used by anyone with a UK or European 'chipped' passport who is aged 18 or over, use **facial recognition** technology to compare the passenger's face to the digital image recorded in their passport. Their details are then automatically checked against the UK Border Agency systems and watchlists – just as if they were seen by an officer. Once the checks are made, the gates open automatically to allow the passenger through the border.

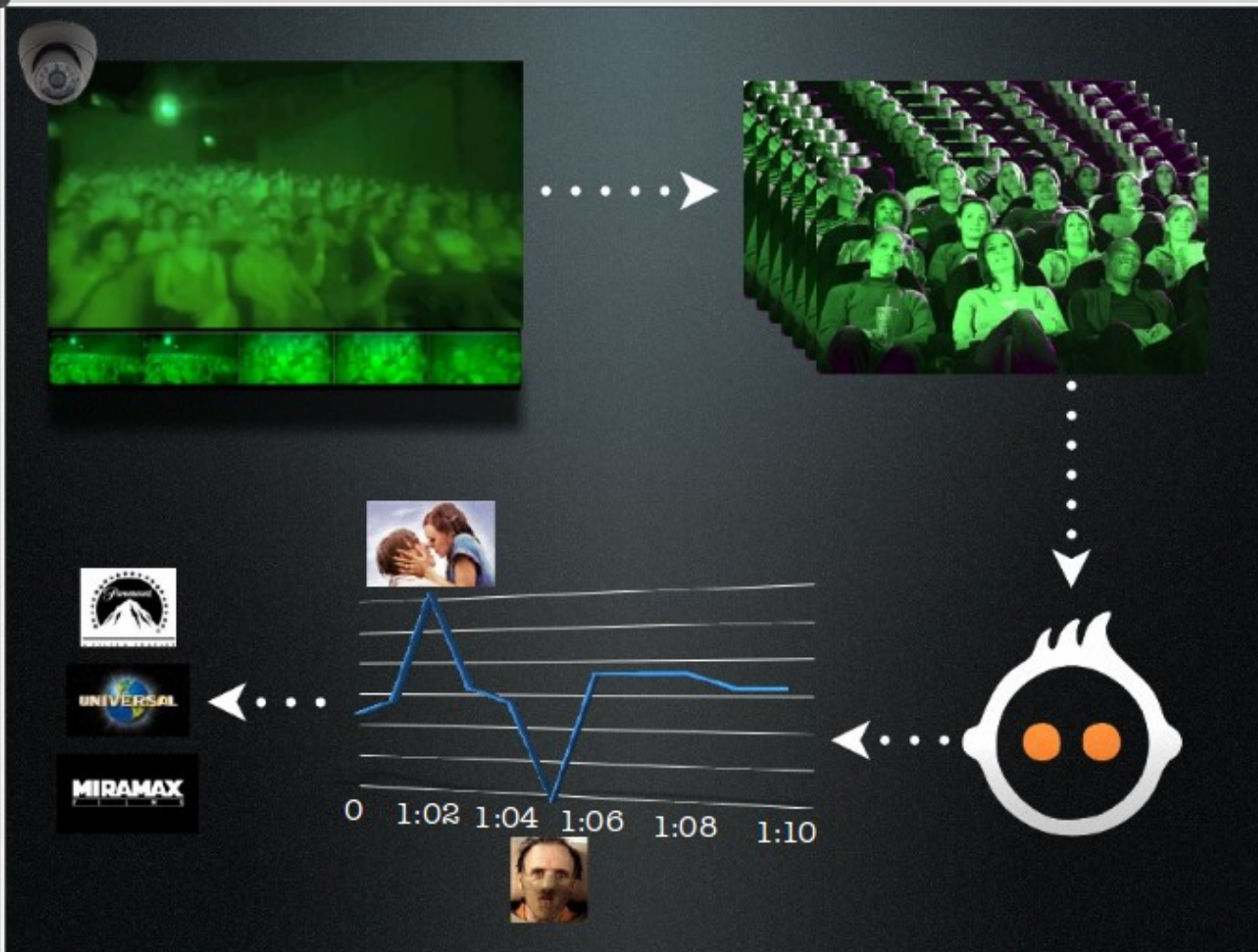
The system is monitored at all times by officers from the UK Border Agency and anyone rejected by the gates will be sent to an alternative channel to have their passport checked.

Carole Upshall, UK Border Agency director Border Force South and Europe, said:



@Facialytics New York
 Using Facial Detection and Infrared Cameras to analyze
 and chart audience reactions, moment by moment, at
 movie screenings and performances
<http://www.facialytics.org>

t x



Facialytics

 DOWNLOAD
  PRINT
  MOBILE
  COLLECTIONS
 

Info and Rating

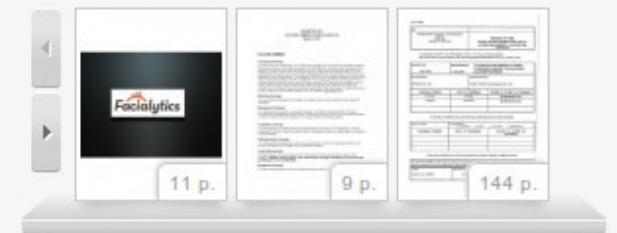
☐ Benjamin Popper

+ Follow

Share & Embed

 FACEBOOK
  TWITTER
  BUZZ
  EMBED

More from this user



Add a Comment

DAILY IDEAS

DESIGN

DIGITAL

NEED TO KNOW

bing



RELATED POSTS



RFID-Equipped Ice Cream Scoopers Update Flavor...



Future of Mobile Tagging: Scan-To-Pay



Red Bull Creation Project Roundup [Pics]



Grant McCracken: Making Culture, Provoking Culture



Ask a PurpleList Expert about this idea.



UNILEVER'S SMILE-ACTIVATED ICE CREAM MACHINE

By Paloma Vazquez on June 22, 2010



112

Comments

Unilever revealed an ice cream vending machine to the global advertising community yesterday at Cannes. Branded "Share Happy", it's already been billed as the world's first smile-activated vending machine, and as "an ice cream truck for the digital age". Ultimately, the vending machine offers a unique brand experience as part of Unilever's new ice cream mission to encourage people everywhere to share life's small moments of happiness.

How it works: an "attractor screen" uses augmented reality to compel passer-by's towards the machine. The person is then prompted to smile, with the 'smile-o-meter' measuring his or her grin; facial recognition technology will gauge the individual's age, gender and emotion. Those with big enough grins are awarded free ice cream, which they can select from the touch-screen interface on the machine. A photo is taken and uploaded onto Facebook – with the person's permission.

LATEST STORIES

EVENTS

REPORTS

VIDEOS

Q&A

About

Advertise

Contact

Consulting

32,572



Like

10K



12,404

Add email to join 17,580 newsletter subscribers



NEED TO KNOW

bing

Luxury Vending Machine Sells Diamond Bracelets

Product Of The Week: Angry Birds Speakers

Amazon's New Convenience Store Delivery Lockers

4chan Spins Off A More Mainstream Image Board

Zegna's 3D iPad App Creates Immersive Shopping Experience

Reebok Classics X Lauryn Hill [Video]

Store Offers Fashion Shopping For Couples

IKEA Trials MÄNLAND, A Male Crèche With TV & Games

Twitter Rebrands Itself As A Business With New Commercial And Advertising

Product Of The Week: Pantone's Color-Customized Thumbdrives

Get this weeks Need to Know report...

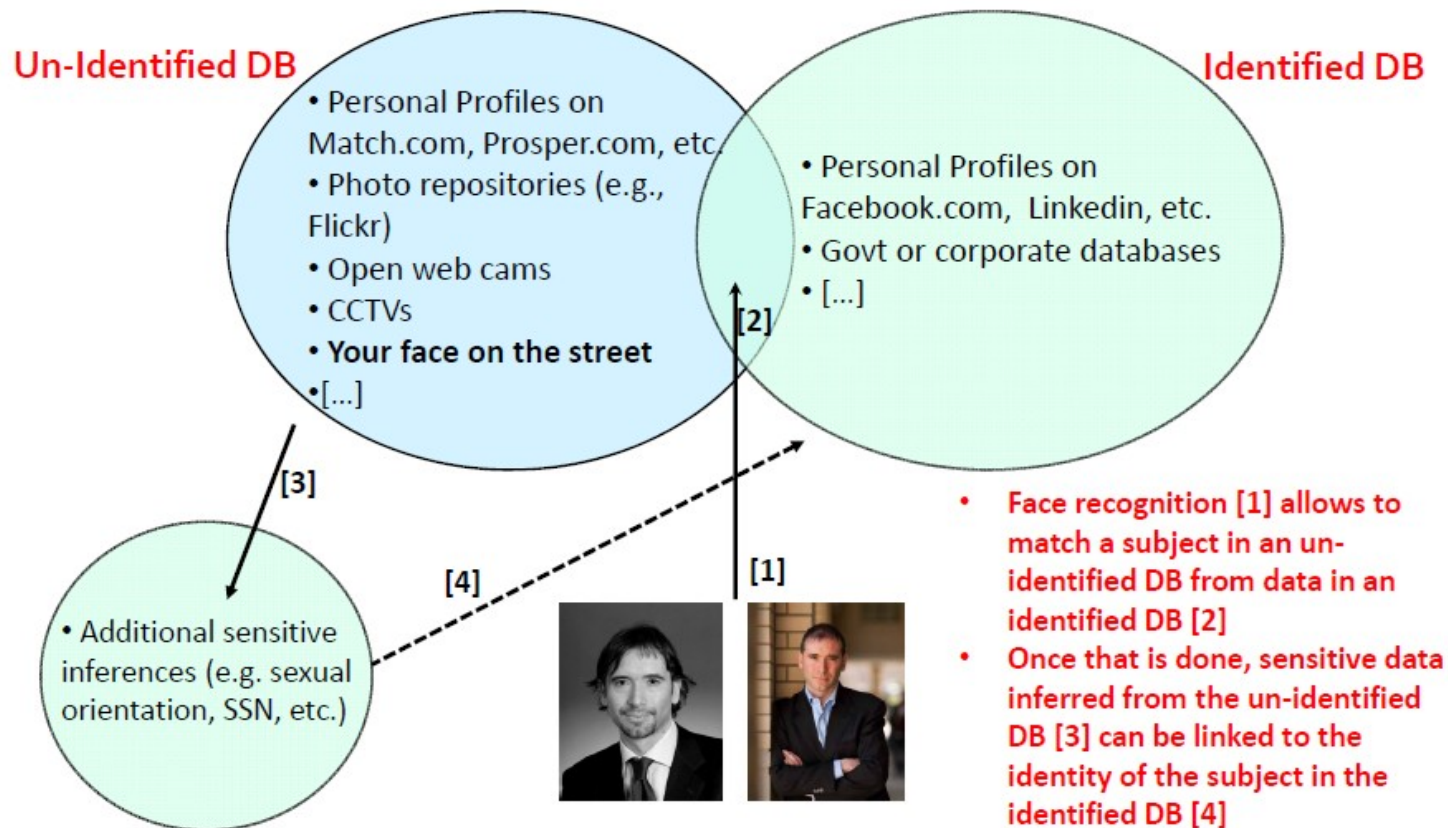
TOPICS

Advertising, Branding & Marketing

Re-Identification from faces

Alessandro Acquisti @Blackhat 2011

In a nutshell



And so on...



@DontTag

*for updates on
#faceRecognition*

Paper Index



1. **What** is Face recognition, its use in social networks: a suggested taxonomy
2. Face recognition **issues** and *contextual integrity* [Nissenbaum 2004]
3. How to **oppose** face recognition: technologies and techniques
4. Conclusions: privacy-by-design and transparent technology architectures

Index

1. What is Face recognition, its use in social networks: a suggested taxonomy
2. Face recognition issues and *contextual integrity* (Nissenbaum 2004)
3. How to oppose face recognition: technologies and techniques
4. Conclusions: privacy-by-design and transparent technology architectures

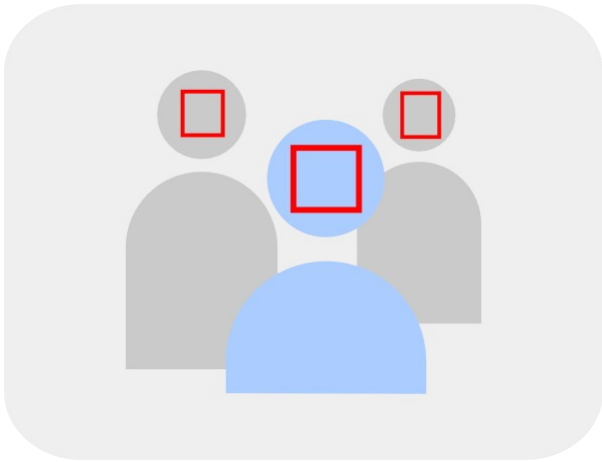


What is “Face Recognition”?

{ Facial | face } { recognition | processing }

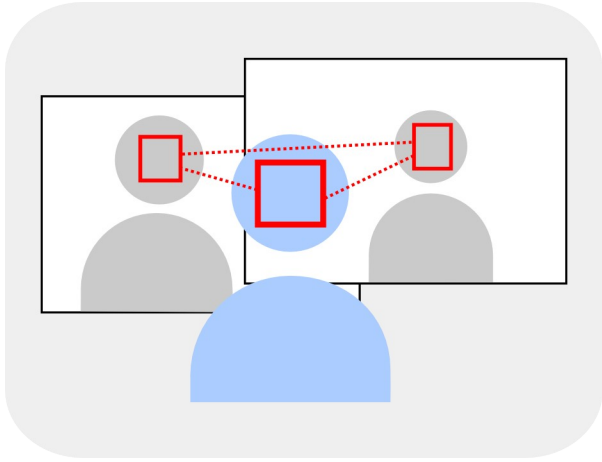
- 1) Face **detection**
- 2) Face **matching**
- 3) **Identity** association
- 4) Face **identification** or verification

Detection



- Detects sex, age, mood
- *Intentions* recognition
- **NO** facial feature or template storing
- Digital Cameras
- Digital signage/
DOOH (billboards)
- Privacy protection
 - Google streetview blurring
 - Human rights activists cameras

Matching



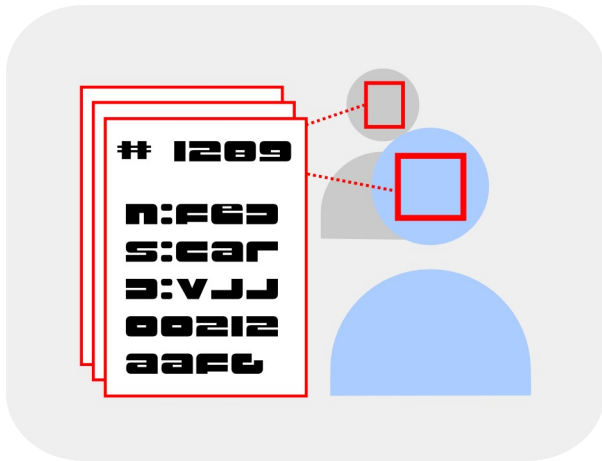
- **Matches** the same face appearing in different pictures
- **Stores** *features* or *templates* unique to each face

- Surveillance CCTV systems
- Facial search engine on public/private pictures
 - Face.com
 - Google Picasa
 - Facebook tag suggestion
 - Astonishing Tribe
 - Recognizr (unreleased)

Taxonomy of FR matching in SNs

store and match <i>activities</i>	matching <i>scope</i>	face signature generation <i>initiative</i>	Examples
joint	unrestricted access to <i>storage provider</i> data	by default	<i>none known so far</i>
	restricted to <i>user</i> data	by default	<i>Facebook tag suggestion, Google Picasa face matching</i>
		initiated by user	<i>none known so far</i>
disjoint	unrestricted access to <i>publicly available</i> data	initiated by third party	<i>Google (unreleased)</i>
	restricted by <i>user's</i> credentials	initiated by user	<i>Face.com photo tagger, PittPatt.com (acquired by G) Viewdle Social Camera, Astonishing Tribe Recognizr (unreleased)</i>

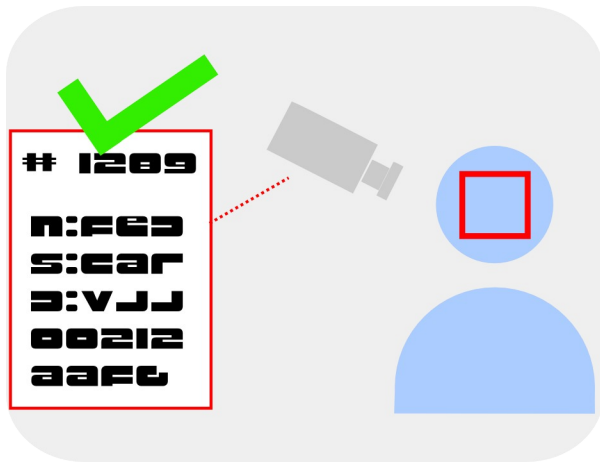
Identity Association



- Links personal data to reference face template
= *enrollment*

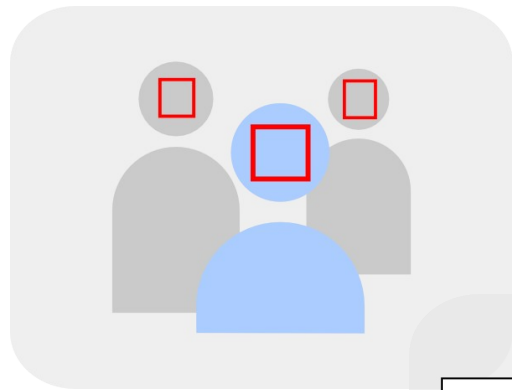
- Enrollment:
 - Overt/Covert
 - Cooperative/non-cooperative
- Social networks: *tagging*
- *Tagging*
 - Self
 - By others
- Automatic *tag suggestions*

Identity Verification

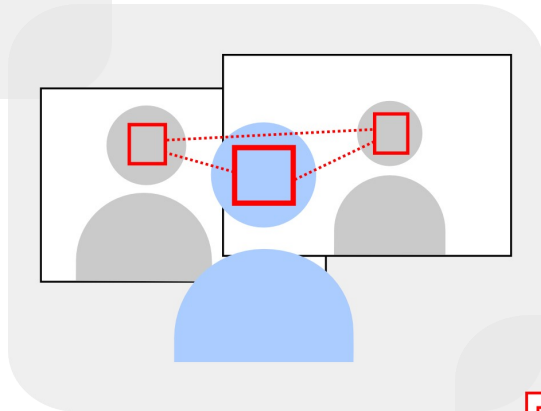


- Match a face against a reference template linked to identity information

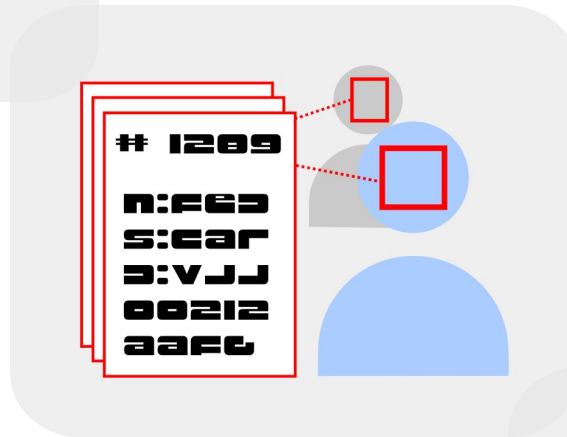
- Access control
- Time attendance
- Border processing
- Police *Offender Recognition*
- Casinos: problem gamblers identification
- VIP lists
- PC webcam login



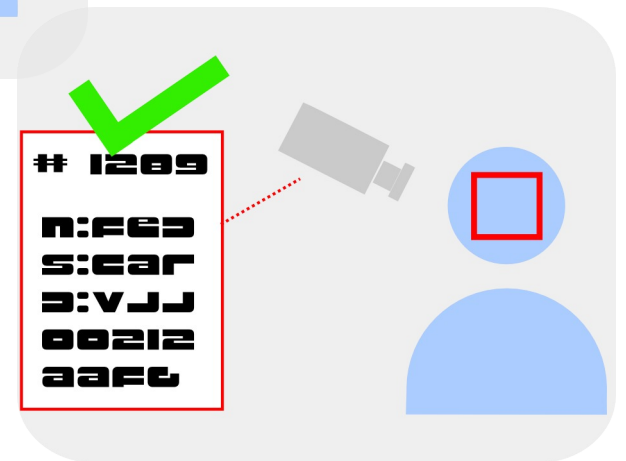
+ features storage



+ enrolment

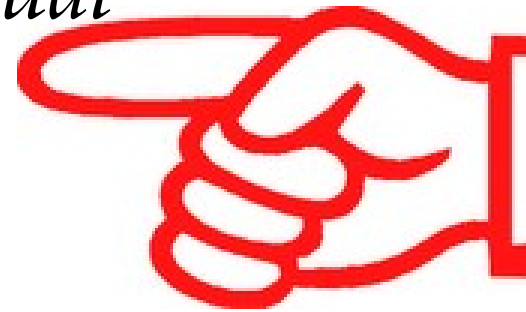


+ unique identity



Index

1. What is Face recognition, its use in social networks: a suggested taxonomy
2. Face recognition issues and *contextual integrity* (Nissenbaum 2004)
3. How to oppose face recognition: technologies and techniques
4. Conclusions: privacy-by-design and transparent technology architectures



What are the main issues?

1. Unintended use
2. Data retention
3. Context puncturing/leakage
4. Information asymmetry

1. Unintended use

[e.g.

Your graduation party pictures available to recruiters]

unauthorized secondary use [Smith, Milberg, Burke 1996]

function creep [Woodward 1997]

identity theft

2. Data retention



I had to! On the Internet nobody forgets you're a dog!

3. Context leakage

- Nissenbaum 2004 “contextual integrity”

*Almost everything happens in a **context** not only of place but of politics, convention, and cultural expectation.*

Norms of appropriateness dictate what information about persons is appropriate [...] to reveal in a particular context

Common practices are understood to reflect norms of appropriateness and flow, and breaches of these norms are held to be violations of privacy.

- Public places are contexts of anonymity!
Nobody wears a name tag in public.

3. *Information asymmetry*

- Pagallo 2008

In new surveillance technologies the controller has access to information about the controlled that the controlled himself ignores

- Pictures taken in public and stored in public repositories can be used for re-identification and even verification
- False positives may lead to reputation damage
- *Interoperability* of FR systems (template exchange)

Index

1. What is Face recognition, its use in social networks: a suggested taxonomy
2. Face recognition issues and *contextual integrity* (Nissenbaum 2004)
3. How to oppose face recognition: technologies and techniques
4. Conclusions: privacy-by-design and transparent technology architectures



Design



Apr 25, 2011

"Pixelhead" Masks Your Face From Google's Roving Cameras



Tweet



Like

31

Surveillance chic for the fashion-conscious paranoid,
courtesy of artist Martin Backes.

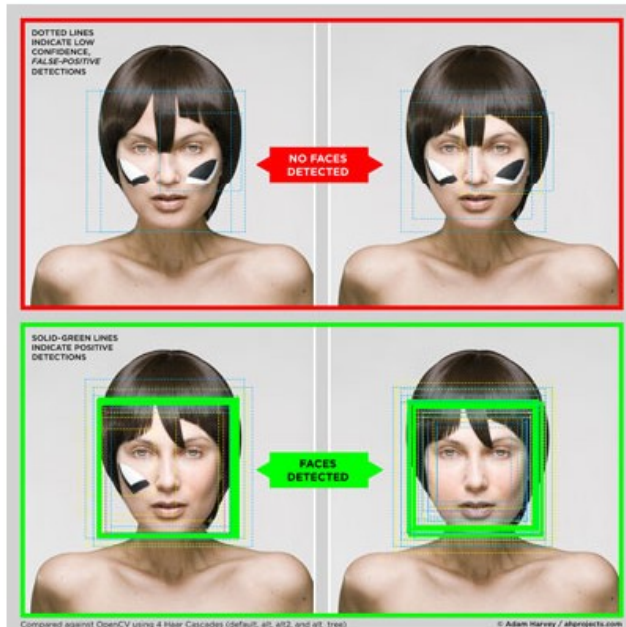
Fashion

Anrealage <http://www.superfuture.com/supertalk/showthread.php?t=273378>





[Collaboration with DIS Magazine](#)
Look #2



First test shoot: Look #1 ([Enlarge](#))



Camouflage from Computer Vision

by Adam Harvey | ahprojects.com | [Email](#)
Location: 63 Flushing Ave. Brooklyn, NY

Introduction

CV Dazzle is camouflage from computer vision (CV). It is a form of expressive interference that combines makeup and hair styling (or other modifications) with face-detection thwarting designs. The name is derived from a type of camouflage used during WWI, called [Dazzle](#), which was used to break apart the gestalt-image of warships, making it hard to discern their directionality, size, and orientation. Likewise, the goal of CV Dazzle is to break apart the gestalt of a face, or object, and make it undetectable to computer vision algorithms, in particular face detection.

And because face detection is the first step in automated facial recognition, CV Dazzle can be used in any environment where automated face recognition systems are in use, such as Google's Picasa, Flickr, or Facebook ([see CV Dazzle vs PhotoTagger by Face.com](#)).

Project Overview

This project began as a thesis proposal at the Interactive Telecommunications Program at New York University in the spring of 2010 with the primary objective of thwarting face detection under the guise of high-fashion aesthetics. While there are several obvious approaches to hiding from face detection, some of these known vulnerabilities have already been addressed by impracticality (sunglasses are a known occlusion) or state laws ([wearing masks in public can be illegal](#)). Instead, this project explored ways of hiding in plain sight using non-obvious, inconspicuous, and unconstrained solution. As such, it aims to be deceptively fashionable and functionally deceptive.

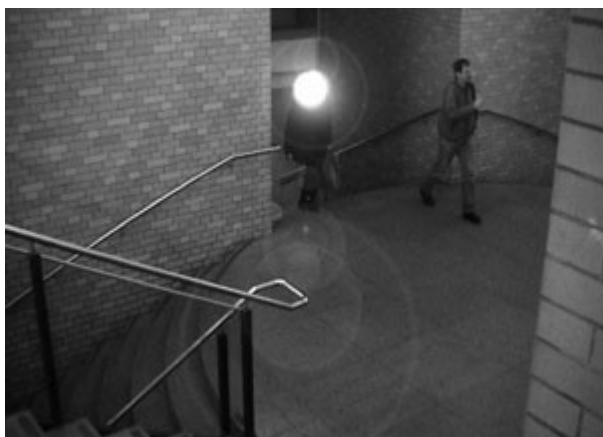
Objective

CV Dazzle is an antagonistic technology. It opposes the mainstream push towards the widespread adoption of face recognition. Several studies have proven that it's now easily possible to identify people in public using an image of someone's face and social network data (see ["Anonymous no more"](#) for one example). Of course, this is just a preview. Facial recognition is the fastest growing biometric

Makeup

Hacktivism: IR CCTV blinding

<http://whereismydata.wordpress.com/2008/07/27/ir-used-to-defeat-cctv/>



IR used to defeat CCTV

July 27, 2008 — 585

We are repeatedly told the CCTV is here to protect us from the worst of the worlds offenders, including terrorists and international criminals. Despite the obvious flaw in the argument that suicide bombers are not bothered if they are filmed blowing themselves up (especially as they normally release videos to that effect shortly afterwards anyway), there is the additional issue that if a person wants to hide their face from a standard CCTV camera it is incredibly easy.

A person can hide their face with a beard, material (mask/bandanna/etc), or they can go slightly more high tech and use infrared lights.

A single point source of a IR Laser, if pointed directly at CCTV camera will flare the camera, however that involves a laser and the user to point and hold the laser directly at the camera. However, if the individual uses an array of IR LEDs then the effect is the same, as a single directed laser.

The idea is relatively simple, the user places IR LEDs in a "head torch", such as the one pictured inset. IR LEDs can be bought for just 79p and LED head torches can be bought for just under £5. IR – **Infrared** – with a range of 750nm to 1mm has a range below the human eye, but can still be detected by CCTV cameras.



Below are the effects of using this type of technology. There are flaws in this anti-CCTV devices. The LEDs need to be powerful enough, and the CCTV camera needs to not have an IR filter. It is also possible, to enhance the blue green spectrum after the incident to try and recover a better image.



COMPUTING / EMBEDDED SYSTEMS

NEWS

Computerized Face-Recognition Technology Is Still Easily Foiled by Cosmetic Surgery

In the first test of face-recognition technology vs. cosmetic surgery, face recognition loses

By WILLIE D. JONES / SEPTEMBER 2009

Email Print Share



Photo: Stephanie Wolfsteiner/Getty Images

[click to enlarge](#)

For years, developers of face-recognition algorithms have been battling the effects of awkward poses, facial expressions, and disguises like hats, wigs, and fake moustaches. They've had some success, but they may be meeting their match in plastic surgery.

Surgery

Technological responses

(privacy by design)

- [Erkin et al., 2009]:
Store/match decoupling: *hide the biometric data as well as the authentication result from the server that performs the matching*
- [Newton, Sweeney, and Malin, 2005]
image de-identification: *de-identifying algorithm that makes identification ineffective while preserving most facial details in the pictures*
- [Boult, 2006]
encryption: *encrypt biometric tokens (such as face template) hiding user's identity and allowing token revocation*

Index

1. What is Face recognition, its use in social networks: a suggested taxonomy
2. Face recognition issues and *contextual integrity* (Nissenbaum 2004)
3. How to oppose face recognition: technologies and techniques
4. Conclusions: privacy-by-design and transparent technology architectures



Conclusions

- *Privacy Chernobyl* scenario:
Disjoint and unrestricted FR by default.
Can lead to ubiquitous identification and surveillance by anyone [Rosen 2011]
- Is privacy by design adopted in SN face recognition applications?

Joint face matching could be restricted to user data and initiated by user, but neither Google nor FB followed this approach (FR by default on all pictures)

Thank you

Alberto @ cammozzo.com