

e-privacy 2012

Milano, 22 june 2012

Face Recognition and Privacy enhancing techniques

Alberto Cammozzo

Founder, TagMeNot.info



Face recognition was an an HOT topic in 2011

What happened then?

Recommend:     [Email](#) 86 Comments [Print](#)

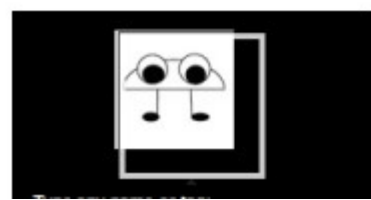
TODAY @ PCWORLD

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

Enter e-mail

[See All Newsletters »](#)

Similar Articles:

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

The Telegraph

Search - enhanced by Google

HOME NEWS SPORT FINANCE COMMENT BLOGS CULTURE TRAVEL LIFESTYLE FASHION **TECH** Dating Jobs

Technology News | Technology Companies | Technology Reviews | Video Games | Technology Video | Mobile App Reviews | Blogs

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

There is no way to prevent your friends' from tagging you on their profiles (timelines), however you can easily remove tagged items from your profile (timeline).

The screenshot shows the Facebook Help Center interface. At the top, there is a blue header with 'facebook HELP CENTER' on the left, a search bar in the middle, and 'Back to Facebook' on the right. Below the header is a left-hand navigation menu with categories: Basics, Manage Your Account, Something's Not Working, Report Abuse or Policy Violations, Ads and Business Solutions, Apps, Games and Credits, Safety Center, and Community Forum. The main content area displays the FAQ title 'Can I prevent myself from being tagged on someone's profile (timeline) as a coworker or classmate?' with a language dropdown set to 'English (US)'. Below the title is a breadcrumb trail: 'Basics » Manage Your Account » Friends'. The answer text states: 'There is no way to prevent your friends' from tagging you on their profiles (timelines), however you can easily remove tagged items from your profile (timeline)'. At the bottom of the answer is a 'Was this answer helpful?' section with 'Yes' and 'No' buttons.

<https://www.facebook.com/help/?faq=195516353827606>



June 2012

Facebook has acquired Face.com!

Our mission is and has always been to find new and astonishing ways to make face recognition a fun, engaging part of people's lives, and incorporate remarkable technology into everyday consumer products. With Facebook, we'll get to continue to pursue that mission - we couldn't be more excited. [Read more](#)



[About](#) | [FAQ](#) | [Contact](#) | [Blog](#) | [Press](#) | [Jobs](#) | [Research](#) | [Developers](#)

The world's largest and most accurate face recognition platform

CHECK OUT OUR FREE **API** >



Face Recognition Camera

Tagging your Facebook friends has never been easier!



search Straight.com



Vancouver: ☀ 17°C



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



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



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 pubs 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

Rioter gets five years for looting shop and attacks on police cars



Saunders: Seen riding a bike in Mare Street on CCTV and then used a cycle lock to damage two police vehicles 1 of 1

Top stories in News

London bus strike: Boris Johnson says 'knock dispute on the head'



Patients' fury at striking doctors - But four out of five London GPs refuse to join pensions protest

Doctors' strike sees one in ten procedures and appointments rescheduled

Most Read Commented Shared



London bus strike: bosses locked in talks with union in bid to stop industrial action



Action, goals... and WAGS: Euro 2012 in pictures



News pictures of the day



Birthday boy... Prince William turns 30



Marble Arch cordoned off after man's body is found

ARTICLE

COMMENTS (53)

July 2011

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



Police to begin iPhone iris scans amid privacy concerns

Recommend

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

Share 92

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

Robocop becomes reality with Spain's Ex-Sight

By Jennifer Riggins | April 16, 2012, 4:33 AM PDT



SCREEN SHOT OF ACTIVEX RUNNING

ALICANTE—The cyborg facial recognition of Robocop becomes a reality as [Spain's Ex-Sight technology](#) equips police officers with the ability to scan 100,000 faces per second. They can then cross these images with those in a database and, in moments, identify suspects.

The first widespread implementation of this technology is with the Brazilian police getting ready for the next World Cup and the 2016 Summer Olympics. "The military police have a database of suspicious people they connect with our software, and our software runs inside the control center in every stadium," says Elazar Lozano Vidal, of Ex-Sight Spain. There are cameras at each

SmartPlanet Weekly Newsletter

A weekly review of the best stories, one from each blog, delivered every Friday.

[Subscribe Today](#)

Facebook Activity

[Sign Up](#)

Create an account or [log in](#) to see what your friends are doing.



[New York to London in an hour - by train | SmartPlanet](#)

1,558 people recommend this.

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:



ShanghaiDaily.com

Username Sign in

[Subscribe](#) | [Forget username/password](#)

[Metro](#) | [Business](#) | [National](#) | [World](#) | [Sports](#) | [Feature](#) | [Opinion](#) | [VIBE](#) | [iDEAL](#) | [PDF](#) | [Gallery](#) | [HD](#) | [Live in Shanghai](#)

[Opinion](#) | [Book review](#) | [Chinese perspectives](#) | [Foreign perspectives](#) | [Shanghai Daily columnists](#) | [View all categories](#)

Latest News: [Russia acknowledges military-technical ties with Syria \[21:29\]](#)

[RSS](#) | [MMS Newspaper](#) | [Newsletter](#)

[Metro](#) | [Traffic](#)

Railway to use face recognition technology

By Zha Minjie | 2012-4-15 | NEWSPAPER EDITION

THE Beijing-Shanghai high-speed railway plans to use a facial identification system at three key stations to help police detect and catch fugitives.

Media reports said yesterday the project's bidding process will start soon. The system will be set up at Shanghai Hongqiao Railway Station, Tianjin W. Railway Station and Jinan W. Railway Station.

The equipment will be set up at security check areas in the stations, according to the China Academy of Railway Sciences.

"The quick identification system will enable the police to recognize faces via surveillance cameras and comb criminal databases on computers for the final match," authorities said.

Researchers added the technology works when people are moving and is helpful even if suspects have had cosmetic surgery.

Police said the real-name ticket purchasing system also helps them catch criminals. During the Spring Festival travel rush this year, railway police seized 375 fugitives along the rail network.

Despite the technology, police officers are still frequently seen patrolling railway stations and questioning passengers, who show their ID cards for quick identification.

In a recent hunt for a suspect who fled from southern China, police at Shanghai Hongqiao Railway Station used almost all team members to

The story appears on **Page A4**
Apr 15, 2012

Free for subscribers
[Get PDF of this page](#)
[Shopping Cart](#)

READING TOOLS

- Email Story
- Printable View
- Blog Story
- Copy Headline/URL
- Share

- SINA
- QQ
- KAIXIN001

Type your keywords | News text |

[Advanced Search](#)

[LATEST UPDATED](#) | [MOST READ](#) | [MOST EMAILED](#)

- [\[21:29\] Russia acknowledges military-technical ties with Syria](#)
- [\[21:29\] Osaka Gas to build solar power plants in western Japan](#)
- [\[21:28\] Ukraine to provide job training for older workers](#)
- [\[21:21\] 9 confirmed dead after minivan plunge in SW China](#)
- [\[21:21\] Equipment market of water sectors to see rapid growth: industrial analysis](#)
- [\[21:21\] Boat carrying 200 asylum seekers capsizes off north of Christmas Island](#)

[twitter.com/shanghaidaily](#) | [MORE](#) >>

OUR PRODUCTS >>



Home Delivery | Online Account | Amazon Kindle

iPhone App

iPad App



UAV =
Unmanned
aerial vehicle

www.dodsbir.net/selections/abs2011-1/armyabs111.htm

of 3

- Capture Page Region Ctrl+Alt+R
- Capture Visible Content Ctrl+Alt+V
- Capture Whole Page Ctrl+Alt+H
- Capture Screen Region Ctrl+Alt+P

Options

Intelligent Automation, Inc.

15400 Calhoun Drive Suite 400
Rockville, MD 20855

Phone: (301) 294-5242

PI: Roger Xu

Topic#: A11-034 **Awarded:**6/7/2011

Title: Non-cooperative Target Tracking and Identification on UAV Platform

Abstract: To achieve the goal of biometric tagging, tracking and localization (TTL) of non-cooperative high value targets based on existing UAV payloads, IAI proposes to develop an integrated real-time tracking and identification system that can automatically track and recognize non-cooperative targets (people of interest) in urban or rural environments. The proposed system is built on top of fast UAV trajectory control, innovative multiple-target tracking, and 3D imaging technologies-enhanced facial recognition approach. There are several key features in the proposed system. First, Innovative target tracking framework based on off-the-shelf target tracking module and a two-level inference engine can handle various non-cooperative target moving patterns under complex cluster environments. Second, by actively integration of target tracking and UAV control algorithms in a closed-loop, the tasks of keeping targets on track and within the sensor's FOV becomes possible. Fast sub-optimal trajectory generation and swift camera pointing control on the fly enable UAV re-acquiring track of lost targets in no time. Third, upon detection of potential targets, camera is automatically adjusted for higher resolution face image capturing, and then 3D imaging technologies enhanced facial recognition algorithm is applied to highly increase the facial recognition rate.

Progeny Systems Corporation

9500 Innovation Drive
Manassas, VA 20110

Phone: (703) 368-6107

PI: Timothy C. Faltemier

Topic#: A11-034 **Awarded:**5/13/2011

Title: Long Range, Non-cooperative, Biometric Tagging, Tracking and Location

Abstract: With the growing concerns surrounding security and terrorism around the world, biometrics has become one of the premier solutions to combat these problems. Traditionally, biometrics has been an academic problem that has been studied from the perspective of optimal environments (good lighting, cooperative subjects, single-frontal-2D / 3D photographs, etc.) and unlimited time and processing power. This form of biometric signature is considered "cooperative" and is generally not applicable to the more difficult problem of "real-world" recognition. Non-cooperative feature recognition is an important component to tracking as a method of distinguishing between tracking targets. Tracking and location determination can be accomplished easily on static platforms with controlled backgrounds and camera calibration, but has shown to be significantly more challenging on a mobile UAV platform. Innovative research is required to identify "non-cooperative" techniques that can be developed for implementation under modern battlefield conditions. In this proposal, we present a variety of algorithms and methods to perform tagging, tracking, and locating (TTL) from existing UAV platforms and sensor payloads. We will leverage our prior SBIR and academic experience in this area, fusing remote biometric feature extraction with state-of-the-art image alignment, to tag, track, and locate long-range, non-cooperative targets on diverse video sensor input.

@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>

Facialytics

DOWNLOAD PRINT MOBILE COLLECTIONS

Info and Rating

Benjamin Popper + Follow

Share & Embed

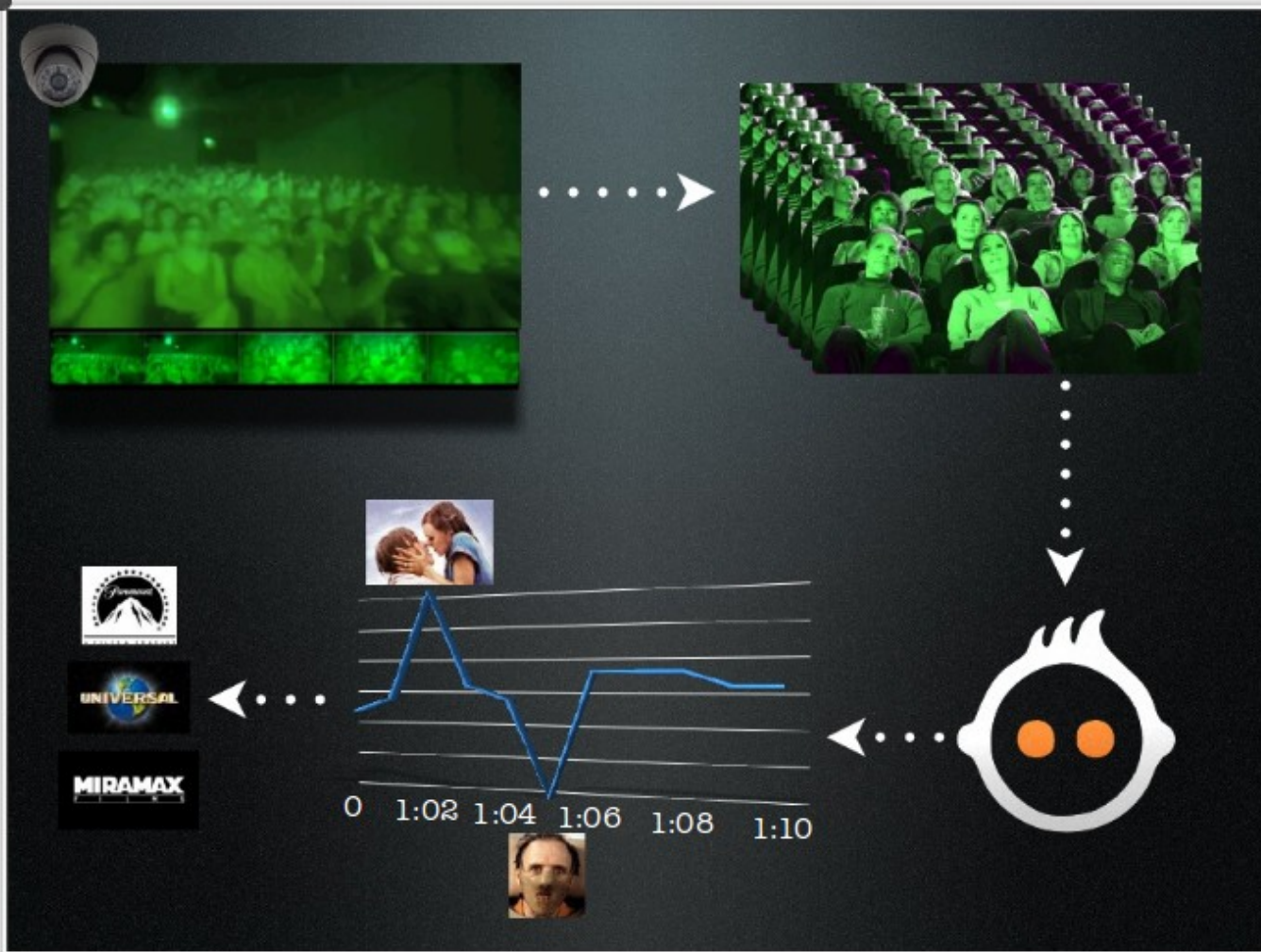
FACEBOOK TWITTER BUZZ EMBED

More from this user

Facialytics 11 p. 9 p. 144 p.

Add a Comment

Comment input field





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



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

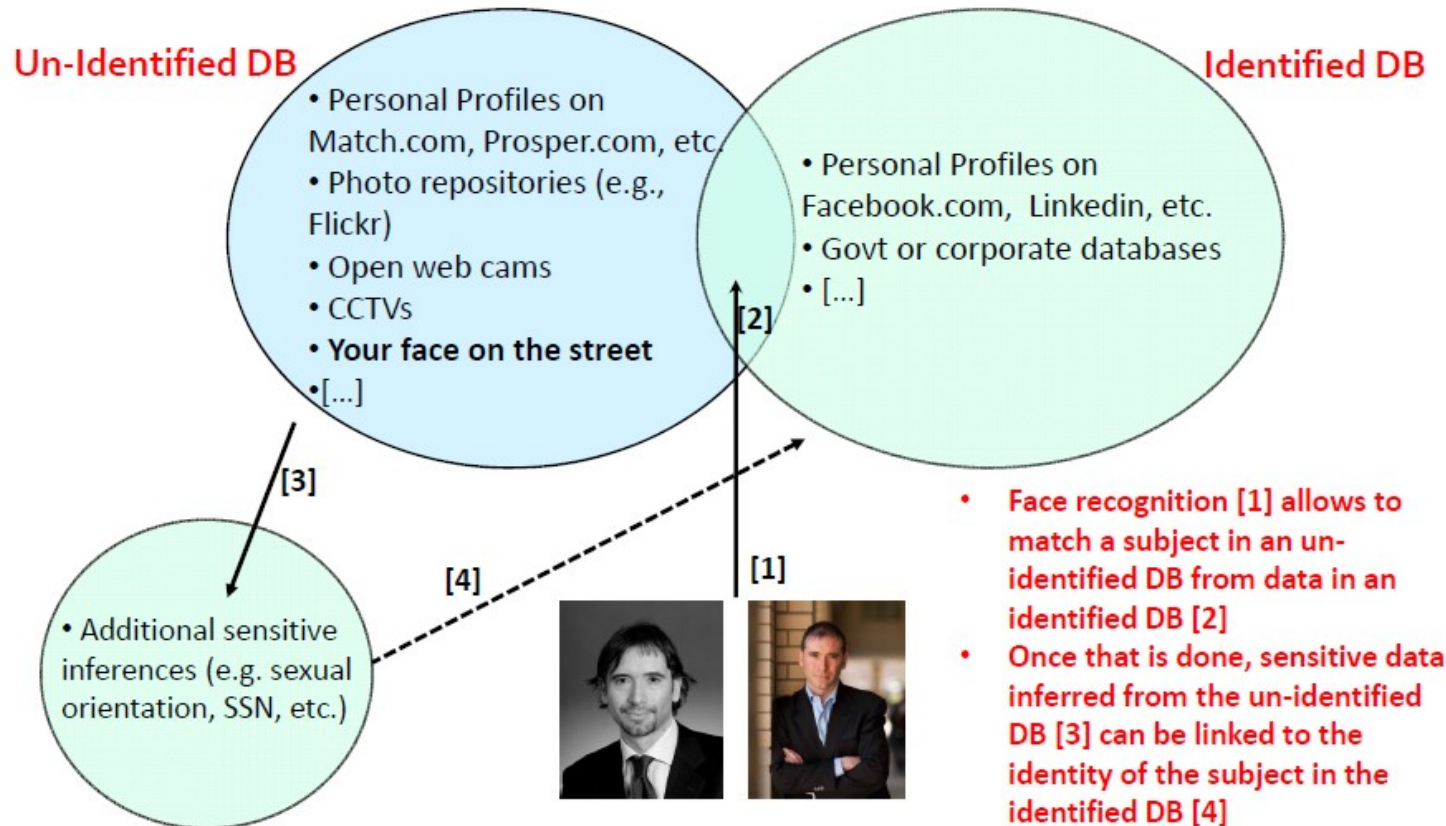
Advertising, Branding & Marketing

Re-Identification from faces

Alessandro Acquisti @Blackhat 2011

In a nutshell

Democratization of surveillance
 Faces as conduits between online and offline data
 The emergence of PPI: “personally predictable” information
 The rise of visual, facial searches
 The future of privacy in a world of augmented reality



And so on...



@DontTag

*for updates on
#faceRecognition
#faceRec*

Index

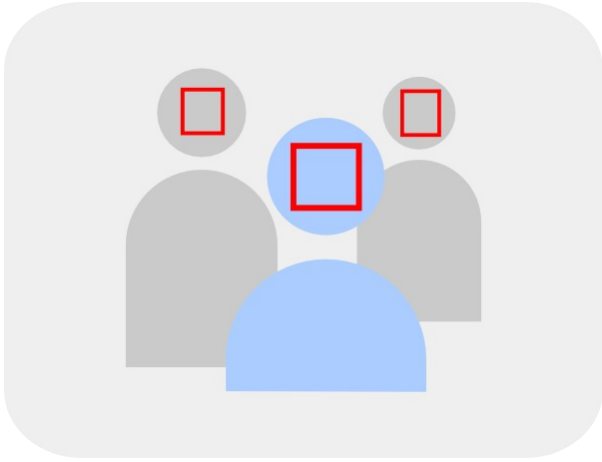
1. What is Face recognition, its use in social networks: a suggested taxonomy
2. Face recognition issues and *contextual integrity* (Nissenbaum 2004)
3. How to oppose face recognition: technologies and techniques
4. Conclusions: privacy-by-design and transparent technology architectures

What is “Face Recognition”?

{ Facial | face } { recognition | processing }

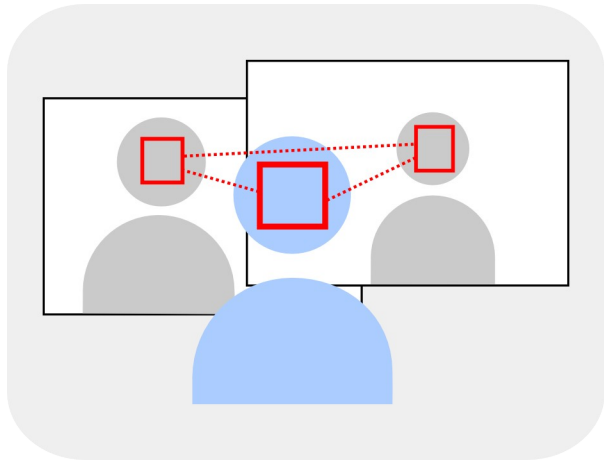
- 1) Face **detection**
- 2) Face **matching**
- 3) **Identity** association
- 4) Face **identification** or verification

Detection: “here is a face”



- 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

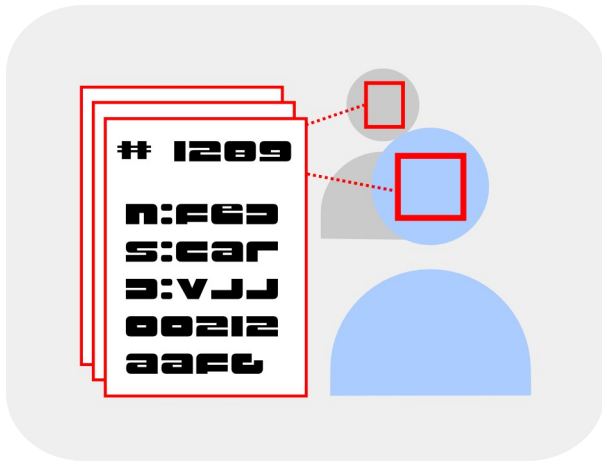
Matching: “that face, again”



- **Matches** the same face appearing in different pictures
- **Extracts and Stores** *features* or *templates* that are 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)

Identity Association: “that’s you, Bob”

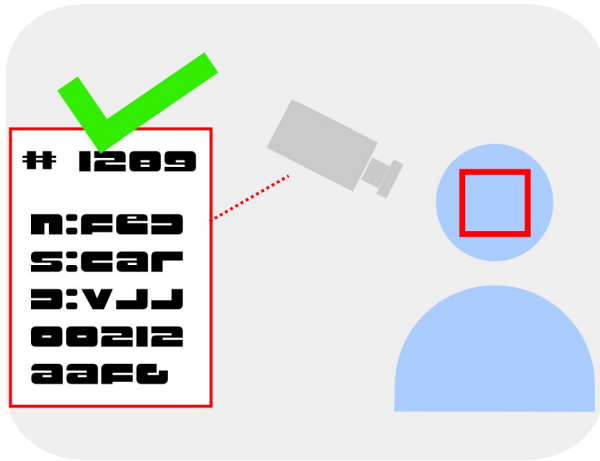


- Links personal data to reference face template
= *enrollment*

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

Identity Verification:

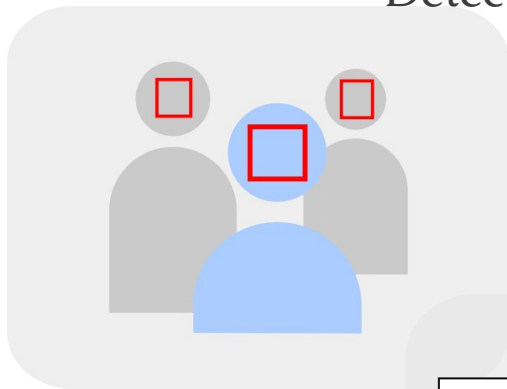
“Is that really you, Bob?”



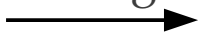
- Match a face (feature) against a reference template linked to identity information

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

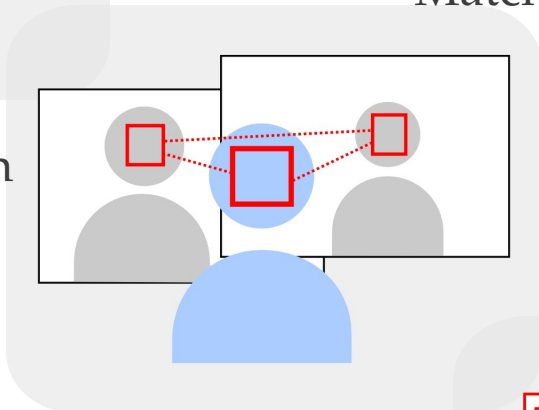
Detection



+ feature extraction
& storage



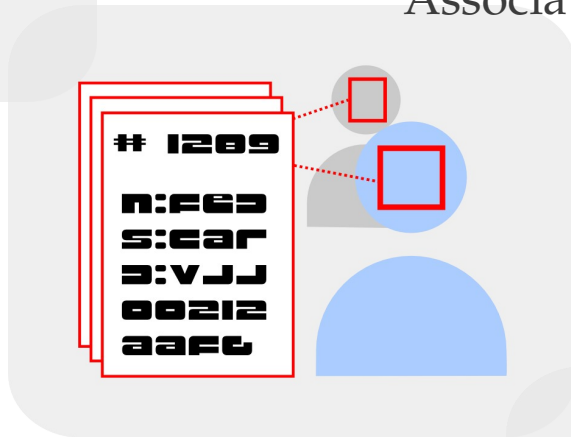
Matching



+ enrolment



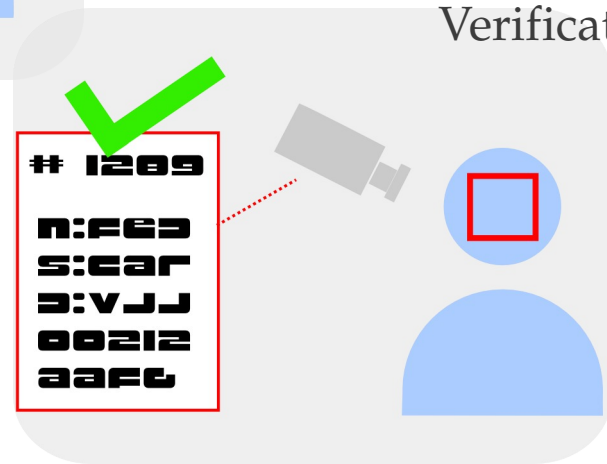
Association



+ unique identity



Verification



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]

aka

unauthorized secondary use

[Smith, Milberg, Burke 1996]

function creep

[Woodward 1997]

“identity theft”

2. Data retention



"On the Internet, nobody knows you're a dog."

2. Data retention



forgets
“On the Internet, nobody ~~knows~~ 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.

4. *Information asymmetry*

- Pagallo 2008

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

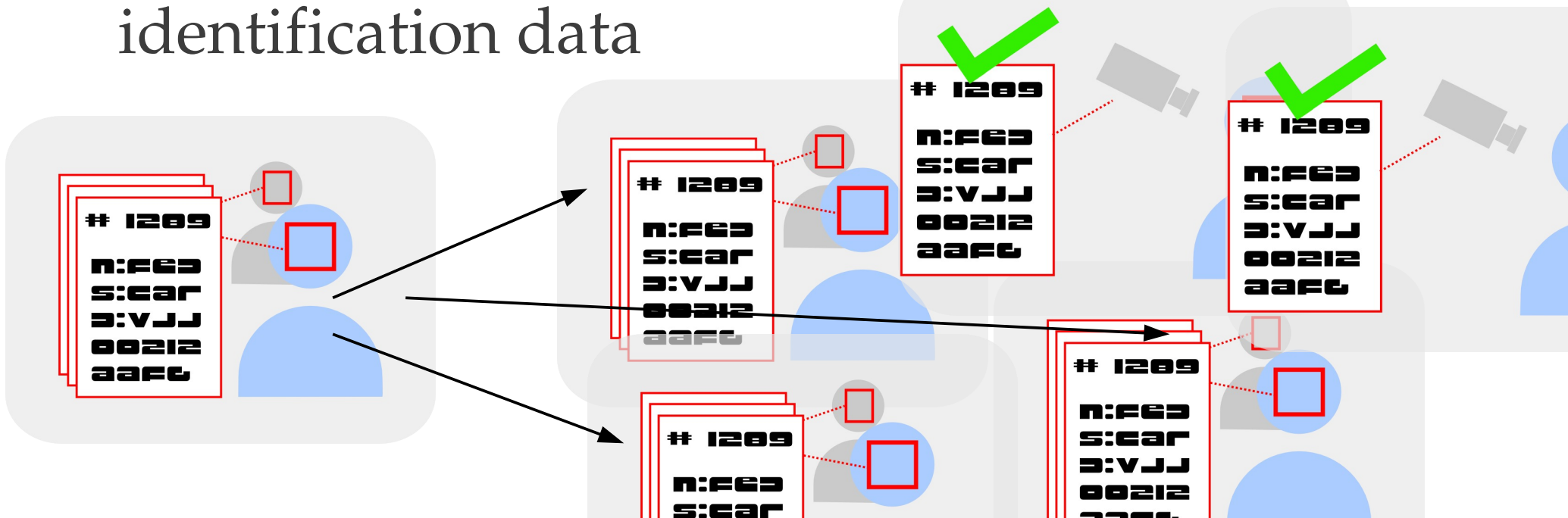
- Pictures taken in public and stored in public repositories can be used for re-identification and even verification
- False positives may lead to reputation damage

Future issue: Interoperability

- *Interoperability* of FR systems leads to features “exchange”

AND

- Security breach may expose interoperable FR identification data



New Protocol Enables Wireless and Secure Biometric Acquisition with Web Services

From **NIST Tech Beat**: May 2, 2012

Contact: [Evelyn Brown](#)
301-975-5661



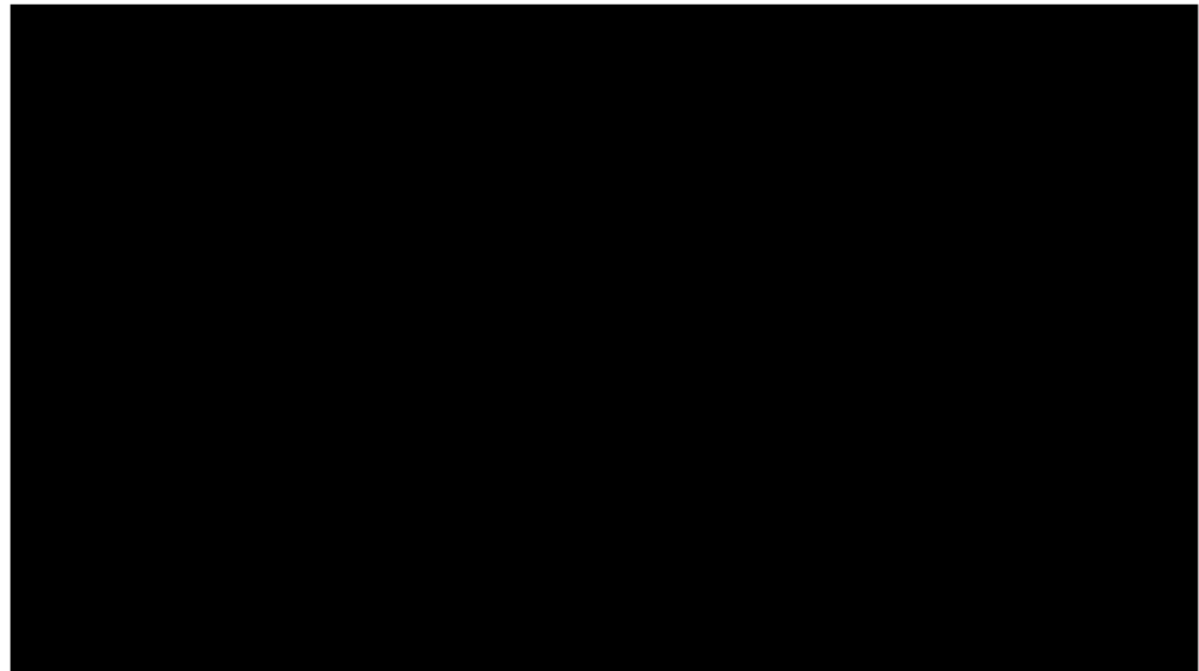
Researchers at the National Institute of Standards and Technology (NIST) have developed and published a new protocol for communicating with biometric sensors over wired and wireless networks—using some of the same technologies that underpin the web.

The new protocol, called WS-Biometric Devices (WS-BD), allows desktops, laptops, tablets and smartphones to access sensors that capture biometric data such as fingerprints, iris images and **face** images using web services. Web services themselves are not new; for example, video-on-demand services use web services to stream videos to mobile devices and televisions.

The WS-Biometric Devices protocol will greatly simplify setting up and maintaining secure biometric systems for verifying identity because such biometric systems will be easier to assemble with interoperable components compared to current biometrics systems that generally have proprietary device-specific drivers and cables. WS-BD enables interoperability by adding a device-independent web-services layer in the communication protocol between biometric devices and systems.

Remember the last time you bought a new computer only to learn that you then had to upgrade your printer and find the appropriate drivers? For system owners, the difficulty of upgrading devices on a biometric system can mean significant costs. Using the WS-BD protocol eliminates that problem.

"This would be useful to many organizations that house biometric systems, including border control and customs agencies," explained computer scientist Kevin Mangold. Using current biometric systems, when one biometric sensor breaks, it can be expensive and time-consuming to find a replacement because manufacturers often change product lines and phase out previous generation devices. A few broken devices could entail having to rebuild the entire system, upgrade devices and drivers that may be incompatible with host operating systems, and retrain personnel, he said.



[cookie disclaimer/privacy policy](#) | [download .mp4](#) | [descriptive text for the visually impaired](#)

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



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>





Makeup

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.

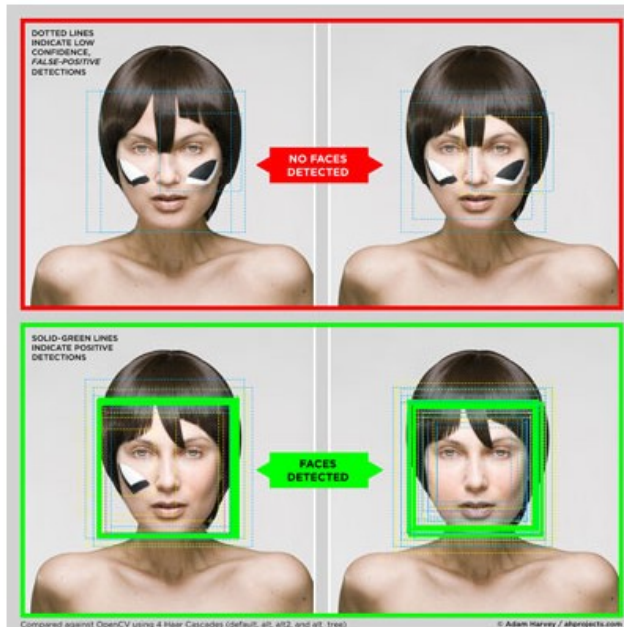
Objective

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



[Collaboration with DIS Magazine](#)

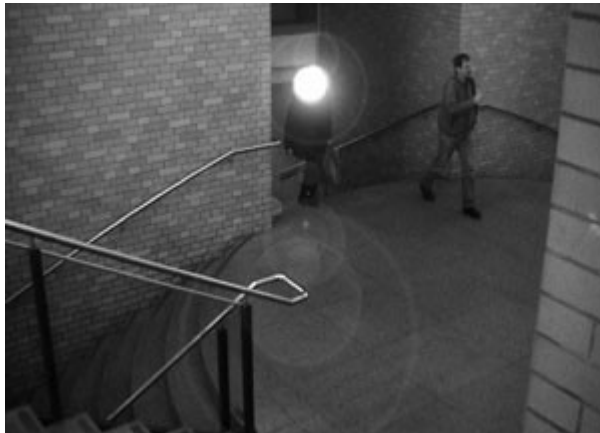
Look #2



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

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.



Surgery

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.

TagMeNot.info



TagMeNot.info

NO PERSONAL DETAILS ONLINE PLEASE!
I DON'T WANT MY FACE ON THE WEB
I DON'T WANT TO BE TAGGED.

What is TagMeNot?

Opt-out for pictures taken in public

TagMeNot is a pre-emptive, anticipatory, vendor independent, and free opt-out technology for pictures taken in public places

The TagMeNot is a QR-Code that links to the site TagmeNot.info, where your will of not being tagged and recognized is clearly stated and could not be ignored

Uses

1. Stick a TagmeNot out of your house and make **Google Street View** and **MS Streetside** know you are opting-out
2. Avoid tagging and face recognition from social networks (as **Facebook**): wear a TagMeNot to state clearly you don't allow tagging
3. Avoid personal pictorial information online: display a TagMeNot to state that any picture of you has to be blurred prior to publishing

NAVIGATION

- [Home](#)
- [FAQ](#)
- [Tweets & feeds](#)
- [Open Letter to EU privacy institutions](#)
- [Face Recognition Privacy](#)
- [License and use](#)
- [Privacy info](#)

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*

The Law

BBC

News

Sport

Weather

Travel

Future

TV

Radio

More...

Search



NEWS EDUCATION & FAMILY

Home

UK

Africa

Asia

Europe

Latin America

Mid-East

US & Canada

Business

Health

Sci/Environment

Tech

Entertainment

Video

England

Northern Ireland

Scotland

Wales

UK Politics

Education

Queen's Diamond Jubilee

15 May 2012 Last updated at 13:02 GMT



Biometric data: Schools will need parents' approval

Schools in England will be banned from taking pupils' fingerprints and using face-recognition technology unless they get permission from parents.

New government guidance says written parental permission must be obtained to use students' biometric data.

Pupils themselves will also be allowed to refuse to participate.

Schools can use fingerprinting or face scanning for recording attendance, checking out library books, paying for lunch or accessing school buildings.

Last year the Association of School and College Leaders (ASCL) estimated that about 30% of secondaries in England were using biometric data.

Sensitive

The new advice, which is now being consulted on, will come into effect from September 2013.

Schools Minister Nick Gibb said the use of biometrics in schools was a sensitive issue and schools should be in no doubt of their responsibilities.



GETTY IMAGES

It is believed that about a third of secondary schools in England use biometrics

Related Stories

[Warning over pupil fingerprinting](#)

Top Stories



[Call for Breivik insanity verdict](#)

[Syria jet pilot defects to Jordan](#)

[EU rules on workers' annual leave](#)

[Bali bomb-maker given 20 years](#)

[Suu Kyi addresses UK's Parliament](#)

Features & Analysis



Changed by Bali

How the 2002 bombings made one angry survivor 'more humane'



Critical condition

The joint demise of Hosni Mubarak and the system he helped create



In pictures

The life LeRoy Neiman, official painter of five Olympiads



Land of opportunity?

Can surfing, bicycles and street cleaning make money in Liberia?

Art 29 Working Party

ARTICLE 29 DATA PROTECTION WORKING PARTY

00727/12/EN

WP 192

Opinion 02/2012 on facial recognition in online and mobile services

Adopted on 22 March 2012

Data Protection Directive (95/46/EC)

9 Recommendations:

1-5: Unlawful processing for the purposes of facial recognition: esp. valid consent and use for the specified purpose,

6: Security breach during transit

7: Data Minimization

8: Security breach during data storage

9: Subject access

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)

Alberto, Cammazzo “Face Recognition and Privacy enhancing techniques”

In The Social Impact of Social Computing, edited by Andy Bissett, Terry Ward Bynum, Ann Light, Angela Lauener, and Simon Rogerson, 101--109. Sheffield Hallam University, Sheffield, UK: Sheffield University, 2011.

Thank you

Alberto @ cammozzo.com

Taxonomy of FR matching in SNs

store and match activities	matching scope	face signature generation initiative	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>