A Conversation on Biometric Privacy

Paresh Trivedi

Wai L. Choy

MCCA Global TEC Forum

June 20, 2017

Proskauer

What Is Biometric Information?

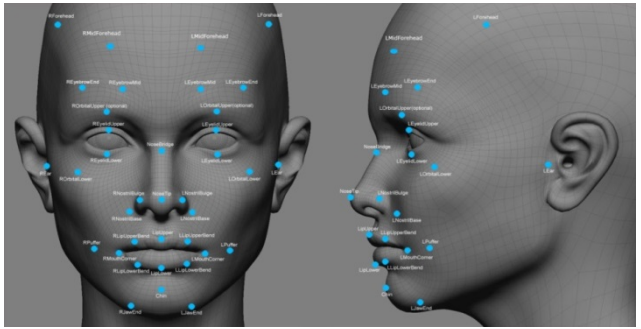
Proskauer

“Biometrics”?

Biometry: the measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns) especially as a means of verifying personal identity.

Types of Biometric Information

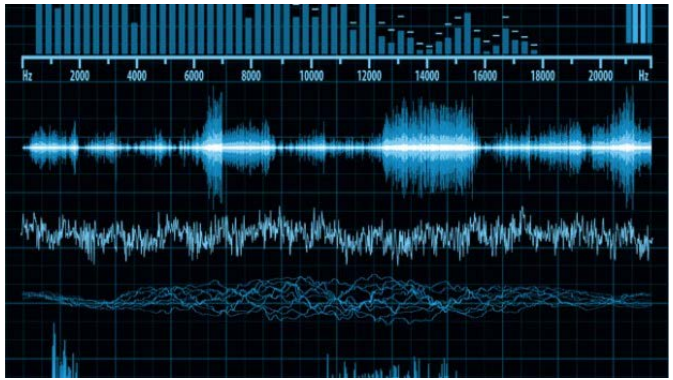
- **Physiological**
  - Fingerprints
  - Iris scans
  - Retinal scans
  - Facial recognition
  - Palm veins/palm prints
  - DNA

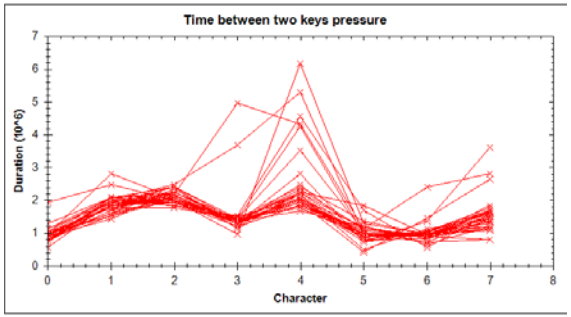


Proskauer

Types of Biometric Information

- **Behavioral**
  - Voice recognition
  - Gait analysis
  - Keystroke dynamics
  - Signature recognition





Proskauer

Biometrics in the Movies

2001: A Space Odyssey (1968)
Voice recognition

Blade Runner (1982)
Biometric scan for empathy

Star Trek II: The Wrath of Khan (1982)
Iris recognition

Judge Dredd (1995)
Biometric-authenticated weapon

Gattaca (1997)
DNA typing

Enemy of the State (1998)
Facial recognition; mass surveillance

Bourne Identity (2002)
Palm reader

Minority Report (2002)
Eye replacement for iris recognition

X-Men: Days of Future Past (2014)
Fingerprint scan spoofed


PROBABILITY .87
SCAN FOR ALTERNATIVE
LEVEL 563
VISUAL:
MALE HT 0601
WT 0215
MESOMORPH
Lite Beer
SCAN MOD 3894
SIZE ASSE MENT
NALYSIS:
34654 453 30 356878 544
54334 450 16 664217 985
665 26 254346 956
453665 766 46 35

Fingerprint Scanning

Proskauer

Facial Recognition Is Not a “New” Technology

The Boston Globe

5. RECOGNIZED BY COMPUTER

WIKIPEDIA COMMONS, 2014

THE FIRST EXPERIMENTS with semi-automated computer-based facial recognition were made during the mid-1960s by Woodrow Wilson Bledsoe, a pioneer of artificial intelligence, who devised a system for noting key facial landmarks on each picture (for example, the width of the mouth or between eyes). In the 1980s and 1990s, research by mathematicians Michael Kirby and Lawrence Sirovich at Brown University and computer scientists Matthew Turk and Alex Pentland at MIT led to a linear algebra-based system called Eigenfaces, which can plot a human face efficiently by focusing on the ways it deviates from the average. This screenshot shows some of the faces that can be created through adjusting those variables.

Proskauer

How is biometric information collected and used?

Proskauer

iPhone 5S: A Biometrics Turning Point?

Device Could Boost Interest in Advanced Authentication

Fahmida Y. Rashid (ITsecuritytech) · September 16, 2013 2 Comments

Apple's decision to include a fingerprint scanner in its new iPhone 5S is an important step toward bringing biometrics-based **authentication** into the mainstream. But there's still a long way to go before **biometrics** supplant usernames and passwords at the enterprise level.

See Also: How to Manage Vulnerabilities Associated with Third Party Systems

Owners of the new phone can use a fingerprint to physically unlock their devices instead of using a numeric passcode. Apple will also let users confirm purchases from the iTunes store by swiping a finger on the sensor.

Apple executives have not yet revealed whether they will allow third-party developers to take advantage of the new TouchID fingerprint technology to build biometrics-based

Biometrics to authenticate 2 billion payment transactions in 2017

By Fintech Innovation editors | 2017-05-08

Caption: photo courtesy of iStockphoto

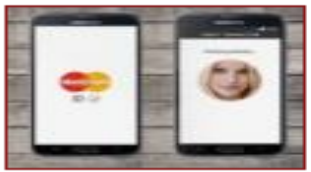
A new study by Juniper Research has found that the number of mobile payments authenticated by biometrics will rise to nearly 2 billion this year, up from just over 600 million in 2016.

The new research, Mobile Payment Security: Biometric Authentication & Tokenization 2017-2021, found that while Apple Pay had provided the catalyst for initial growth, other leading wallets including Android Pay and Samsung Pay were increasingly offering biometric solutions for authentication.

Furthermore, the size of the opportunity has been boosted by the greater availability of fingerprint sensors. Juniper estimates around 60% of smartphone models are expected to ship with such sensors this year, with many Chinese vendors incorporating them into mid-range models.

Selfie Pay

The research emphasized the increasing momentum behind alternative biometric solutions. It recognized Mastercard as an early leader in this space through its Identity Check Mobile capability, due to go live in the latter part of 2017. Informally known as "selfie pay", this allows users to scan their fingerprints and/or take selfies to validate their identities and thereby make payments.



Facebook Moments Uses Facial Recognition To Send Friends Your Photos They're In

Posted Jun 15, 2015 by ***Josh Constine*** *(@joshconstine)*

Frustrated with friends who take photos of you, say they'll pass them on, but never do? Facebook's newest companion app Moments could retrieve your memories trapped on other people's phones through facial recognition.

Moments scans your Camera Roll for the all the photos featuring a friend's face, and bundles them up for one-tap private sharing with that friend. They can contribute to the collaborative private album too, so all your pals from the party or vacation can get each

ALPHABET ARTIFICIAL INTELLIGENCE NEST LABS

Nest's new camera uses the same facial recognition tech as Google Photos

And it costs $100 more than its predecessor.

BY TESS TOWNSEND | MAY 31, 2017, 3:01AM EDT

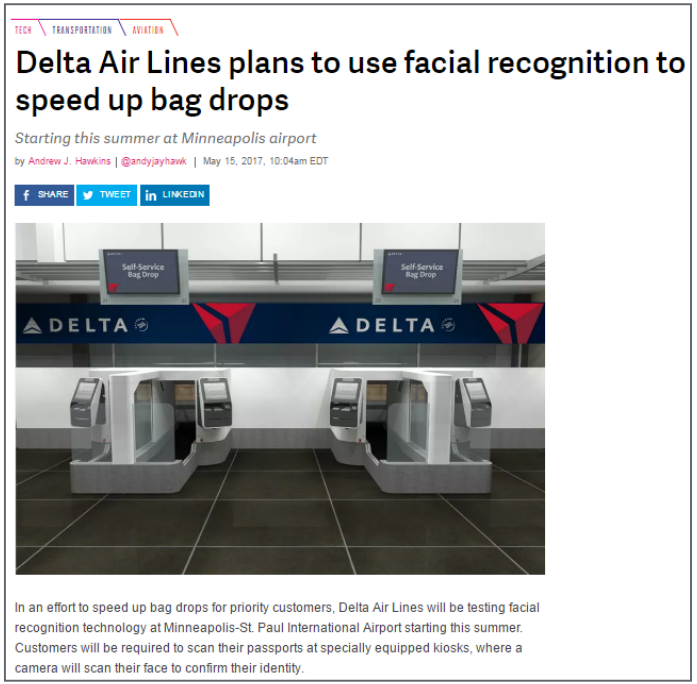
Nest

Nest is releasing a new $299 indoor camera that can recognize faces using Google's artificial intelligence software.

The Nest Cam IQ uses the same facial recognition technology as Google Photos to recognize faces and allow users to label who they are, so the user can know who was in a room when, according to

Facial Recognition

- Facial recognition technologies have been adopted in a variety of contexts, ranging from online social networks and mobile apps to retailer's analytics.
  - Potential non-security uses include:
    - Determining an individual's age range and gender to deliver targeted advertising
    - Assessing viewers' emotions to monitor engagement in video game or movie or interest in a retail store display
    - Matching faces and identifying anonymous individuals in images
    - Photo tagging



TECH \ TRANSPORTATION \ AVIATION

Delta Air Lines plans to use facial recognition to speed up bag drops

Starting this summer at Minneapolis airport

by Andrew J. Hawkins | @andyjayhawk | May 15, 2017, 10:04am EDT

SHARE TWEET LINKEDIN

In an effort to speed up bag drops for priority customers, Delta Air Lines will be testing facial recognition technology at Minneapolis-St. Paul International Airport starting this summer. Customers will be required to scan their passports at specially equipped kiosks, where a camera will scan their face to confirm their identity.

Proskauer

Facial Recognition –
Social Media

Google: Our new system for recognizing faces is the best one ever

FORTUNE

by Derrick Harris @derrickharris MARCH 17, 2015, 5:05 PM EDT

New advances in facial recognition are a step forward for an artificial intelligence technique called deep learning.

"I never forget a face," some people like to boast. It's a claim that looks quainter by the day as artificial intelligence research continues to advance. Some computers, it turns out, never forget 260 million faces.

Last week, a trio of Google (GOOG -1.93%) researchers published a paper on a new artificial intelligence system dubbed FaceNet that it claims represents the most-accurate approach yet to recognizing human faces. FaceNet achieved nearly 100-percent accuracy on a popular facial-recognition dataset called Labeled Faces in the Wild, which includes more than 13,000 pictures of faces from across the web. Trained on a massive 260-million-image dataset, FaceNet performed with better than 86 percent accuracy.

Facebook's scarily accurate facial-recognition tech can now recognize you even if it can't see your face

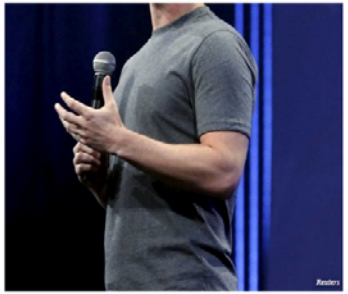
Rob Price Jun. 23, 2015, 5:07 AM 3,358 2

BUSINESS INSIDER

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

Facebook's extremely accurate facial-recognition technology, which enables the program to automatically tag faces in pictures uploaded to the website, could be getting an upgrade. The social-networking giant has developed experimental technology that can work out who you are even if it can't see your face, according to New Scientist.

The tech looks for other possible identifiers — regularly worn clothing, a distinctive posture, or a



Guess who?

Snapchat has figured out a way to use facial recognition tech to protect people's privacy

Rob Price Jul. 19, 2016, 7:25 AM 5,149

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

Snapchat is exploring how facial recognition technology could be used to protect the privacy of its users.

A new patent from the smartphone messaging company, issued by the United States Patent and Trademark Office on July 19, is entitled: "Apparatus and method for automated privacy protection in distributed images."

It discusses how sophisticated face-recognising technology could be used to scan new photos, and

The feature described in Snapchat's patent could automatically blur faces – or replace them with emoji. Ellen DeGeneres/BI

Proskauer

RETAIL

Your Favorite Stores Are Watching You While You're Shopping (and Collecting Your Biometric Data)

Some analytics companies are encouraging retailers to go all-in on facial recognition, while others are pursuing a more privacy-conscious path. How can small businesses choose?

By Cameron Albert-Deitch *Assistant editor, Inc.com* @c_albertdeitch

WRITE A COMMENT

CREDIT: Getty Images

Imagine owning a store and knowing everything about your customers from the moment they walk in: ages, genders, moods, information from their social media profiles. It seems like something out of *Minority Report*.

Except, it's nearly reality. Stores regularly track demographic and biometric data like age, gender, and mood just from reading faces of customers on video cameras. The only

EyeSee Mannequin

Craftsmanship, sustainability and innovation come together to revolutionize the fashion marketing with Almax.

Thanks to Eye See Mannequin by Almax, mannequins have become smart: this product do not only display clothes and encourage the consumer to enter the store, but it also makes it possible to "observe" who is attracted by store windows and reveal important details about customers: age range, gender, ethnicity, dwell time.

How does it work? Thanks to a complex biometrical facial analysis system, designed and manufactured in collaboration with a spin-off of Politecnico University in Milan, this special camera installed inside the mannequin's head analyses the facial features of people passing through the front and provides statistical and contextual information useful to the development of targeted marketing strategies.

All this in total respect of privacy, protected by a sophisticated mix of hardware and software technology which processes the data without the aid of a computer and without having to record and transmit sensitive information (images or biometric data), and so without leaving any trace of the face analysed.

to watch. read their minds.

Forget Fingerprints: You Could Soon Use Your Gait To Secure Your Phone

Rae Johnston
May 24, 2017, 10:15am- Filed to: Australian Stories

Share

Image: iStock

CSIRO's Data61 researchers have developed new technology which uses the way a person walks to not only power wearable devices, but also be used as a new authentication method.

Replacing passwords, pins or fingerprints with your gait could very well be a thing in the near future.

Finovate Debuts: SayPay Combines Voice Recognition and Biometric Authentication

By Julie Muhn (@julieschicktanz) Posted on May 26, 2015

Share:

SayPay Technologies uses biometric authentication to give users an easy way to pay bills, check out online, and log into their online banking website.

NOVEMBER 4, 2015 | BY DAVE MAASS

California Cops Are Using These Biometric Gadgets in the Field

This report was co-written by MuckRock Editor JPat Brown. MuckRock Co-founder Michael Morisy, MuckRock Intern Lukas Knight, and EFF Activism Intern Annelyse Gelman also contributed to this report. Another version appears at MuckRock.com.

Law enforcement agencies around the country are increasingly embracing biometric technology, which uses intrinsic physical or behavioral characteristics—such as fingerprints, facial features, irises, tattoos, or DNA—to identify people, sometimes even instantly. Just as the technology that powers your cell phone has shrunk both in size and cost, mobile biometric technologies are now being deployed more widely and cheaply than ever before—and with less oversight.

EFF and MuckRock News teamed up in August to reveal how state and local law enforcement agencies are using mobile biometric technology in the field by filing public records requests around the country. With the help of members of the public who nominated jurisdictions for investigation, we have now obtained thousands of pages of documents from more than 30 agencies.

REPORT \ US & WORLD \ POLITICS

Airport face recognition could extend to US citizens, says Customs

A 'biometric pathway' through the airport, unlocked by your face

by Russell Brandom | @russellbrandom | May 9, 2017, 10:11am EDT

Wikimedia Commons

The US government has rolled out a plan to reshape airport security around facial recognition, playing off a wealth of passport photos and visa applications.

government technology
Solutions for state and local government.

Facial Recognition for Pets Could Help Cities Save Furry Lives

Facial recognition is an emerging technology typically fraught with controversy, but most seem to agree that for animals, there's nothing but potential.

Finding Rover

Home Blog Spots Partners Login Regist

1 Take a front-facing photo

A good picture is easy to take with our bark button.

2 Mark the e and nose

Simply drag onto the pho

3 We verify t

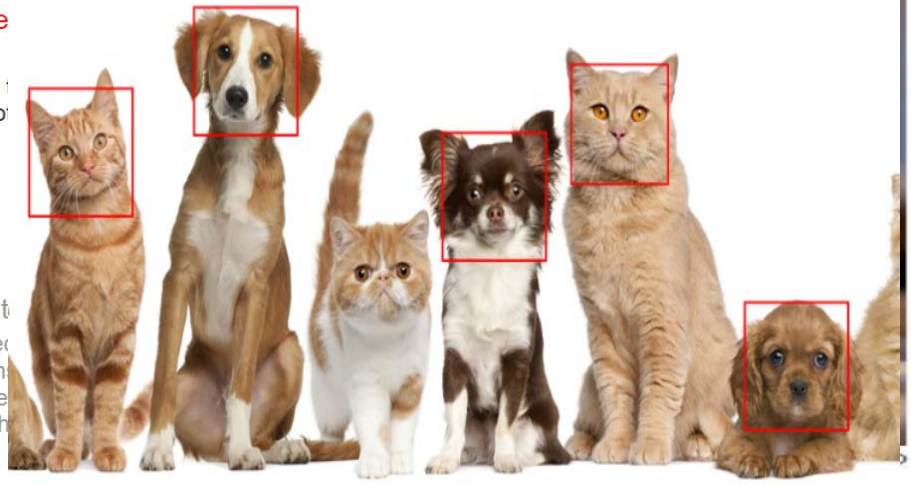
Our facial re system scan dog's unique and keeps th just in case.

ArcSoft

Technology
our core

Product
software & apps

Corporate
who we are



Wide, Wide Range of Biometrics

Amazon Developing 'Voice ID' Technology for Alexa Assistant

Tuesday February 28, 2017 1:28 AM PST by Tim Hardwick

Amazon is building upon the Alexa voice recognition technology found in its Echo range of speakers so that the virtual assistant can distinguish between individual users based on the sound of their voices.

According to anonymous sources who spoke to TIME, Amazon's feature would work by matching the person speaking to a pre-recorded voice sample, or "voice print", to verify the speaker's identity.

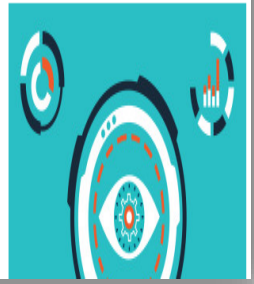
Qatar National Bank Deploys Iris Scanning ATMs

Posted on December 14, 2016

Tweet Like Plus Pin It Share

Customers of Qatar National Bank (QNB) can now access ATMs via iris scan.

The technology comes by way of Iris ID. To enroll, customers simply need to register their iris biometrics at a branch, which entails a digital photo of the iris. That information is converted into a biometric template against which the customer's irises are matched whenever they approach a QNB ATM equipped with iris scanning technology.



Michaela Rehle / Reuters

TECHNOLOGY

Machines That Can See Depression on a Person's Face

Facial-recognition technologies can discern muscle-by-muscle differences in how men and women emote when they're depressed.

Proskauer

Deploying Biometrics

Proskauer

Business Wire
A Berkshire Hathaway Company

FaceFirst™ Makes Shopping Safer With National Facial Recognition Deployment

Retail

Reduce the high costs of shoplifting and lawsuits while boosting customer loyalty.

Your retail locations all have security systems. What they don't have is an affordable way to reduce the high cost of shoplifting, customer lawsuits and employee theft -- until FaceFirst®.

An advanced facial recognition system, FaceFirst® spots known perpetrators entering your locations so you can stop them before they cost you money.

Spot and stop the bad guys.

- Receive descriptive alerts when pre-identified shoplifters walk through any door at any store.
- Get alerts when known litigious individuals enter any of your locations.

Recognize the good guys and treat them better.

- Build a database of good customers, recognize them when they come through the door, and make them feel more welcome.
- Keep repeat customers coming back and spending more.

o Decrease Shoplifting Incidences

oplifting criminal activity and these circumstances threaten
software system, recently partnered with a nationally renowned
s across the nation in order to curb shoplifting incidences and

Business Wire
A Berkshire Hathaway Company

FaceFirst™ Makes Shopping Safer With National Facial Recognition Deployment

Retail

Reduce the high costs of shoplifting and law while boosting customer loyalty.

Your retail locations all have security systems. What they don't shoplifting, customer lawsuits and employee theft -- until Facel

An advanced facial recognition system, FaceFirst® spots known stop them before they cost you money.

Spot and stop the bad guys.

- Receive descriptive alerts when pre-identified shoplifter
- Get alerts when known litigious individuals enter any of

Recognize the good guys and treat them better.

- Build a database of good customers, recognize them wh

more welcome.

- Keep repeat customers coming back and spending mor

Gaming

Spot the good guys and the bad guys entering your casinos.

Maximizing your bottom line at your casinos means keeping out the compulsive gamblers, the con artists and troublemakers while providing royal treatment to the big spenders. FaceFirst® makes it all possible -- and makes it easy.

An advanced facial recognition system, FaceFirst® identifies individuals at the door, then sends alerts to authorized personnel -- instantly.

Spot and stop the bad guys.

- Receive descriptive alerts when anyone walks into your casino who is not wanted there.
- Experience better risk management by spotting litigious individuals at the door.
- Cooperate with law enforcement. Load their criminal data into your FaceFirst® database so you can notify them if one enters your casino.
- Monitor the movement of employees and others in your facility to ensure that no one is in an area in which they are not authorized to be.

Recognize the whales and make their stay more memorable.

- Make sure your hospitality department never misses spotting a visiting VIP again.
- Provide the best experience to increase customer loyalty and return visits.
- Help prevent confrontations that disturb your other guests.

ces threaten
ationally renowned
incidences and

Business Wire
A Berkshire Hathaway Company

FaceFirst™ Makes Shopping Safer With National Facial Recognition Deployment

Retail

**Reduce the high costs of shoplifting and law
while boosting customer loyalty.**

Your retail locations all have security systems. What they don't
shoplifting, customer lawsuits and employee theft -- until FaceF

An advanced facial recognition system, FaceFirst® spots known
stop them before they cost you money.

Spot and stop the bad guys.

- Receive descriptive alerts when pre-identified shoplifter
- Get alerts when known litigious individuals enter any of

Recognize the good guys and treat them better.

- Build a database of good customers, recognize them wh
more welcome.
- Keep repeat customers coming back and spending more

Gaming

**Spot the good guys and the
casinos.**

Maximizing your bottom line at your c
troublemakers while providing royal t
easy.

An advanced facial recognition system
personnel -- instantly.

Spot and stop the bad guys.

- Receive descriptive alerts whe
- Experience better risk manage
- Cooperate with law enforceme

them if one enters your casino.

- Monitor the movement of emp

they are not authorized to be.

Recognize the whales and ma

- Make sure your hospitality dep
- Provide the best experience to
- Help prevent confrontations th

Commercial Security

Protect your property, your tenants and your bottom line.

FaceFirst®, an advanced facial recognition system, is the key to more fully protecting your property and your tenants.

Create a blacklist of persons you don't want in your buildings.

- Receive descriptive alerts when anyone walks into your building who is not wanted there.
- Flag individuals who have caused problems in the past.
- Be alerted when known litigious individuals enter any of your properties.
- Cooperate with law enforcement. Load their criminal data into your FaceFirst® database so you can notify them if one enters your building.
- Better protect your tenants.
- Monitor the movement of people in your facility to ensure that no one is in an area in which they are not authorized to be.

Biometrics Risks & Concerns

Proskauer

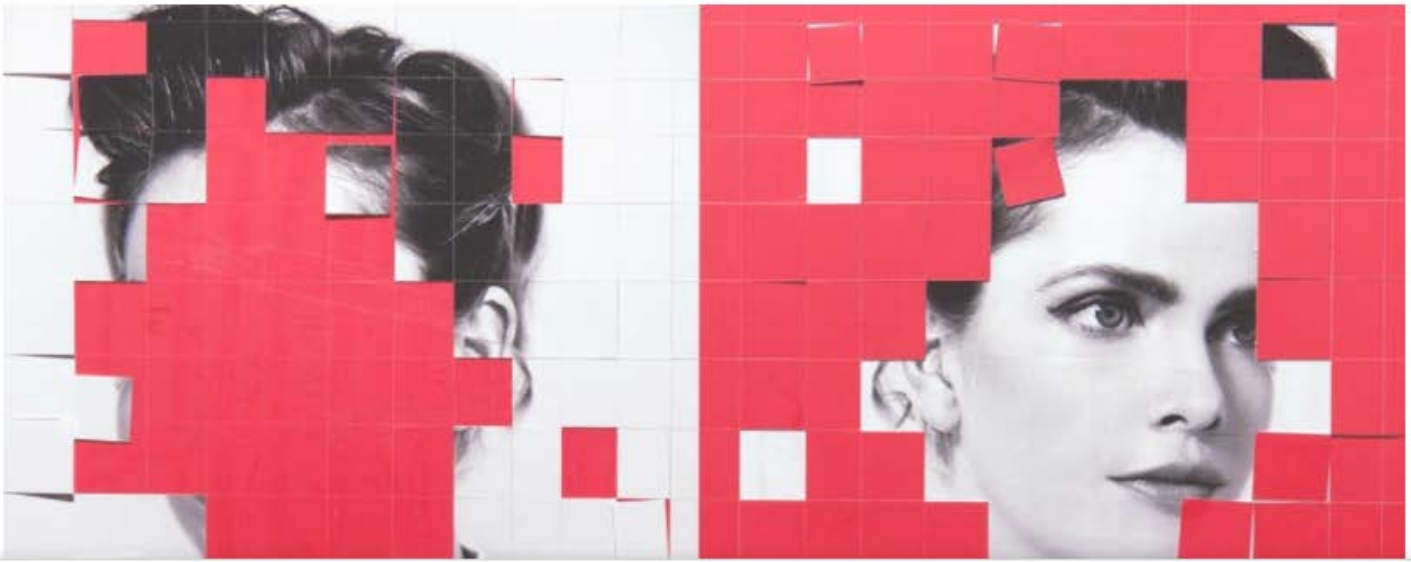
Harvard Business Review

SECURITY & PRIVACY

Passwords Are Terrible, but Will Biometrics Be Any Better?

by Anthony Rjeily and Charlie Jacco

MAY 11, 2017

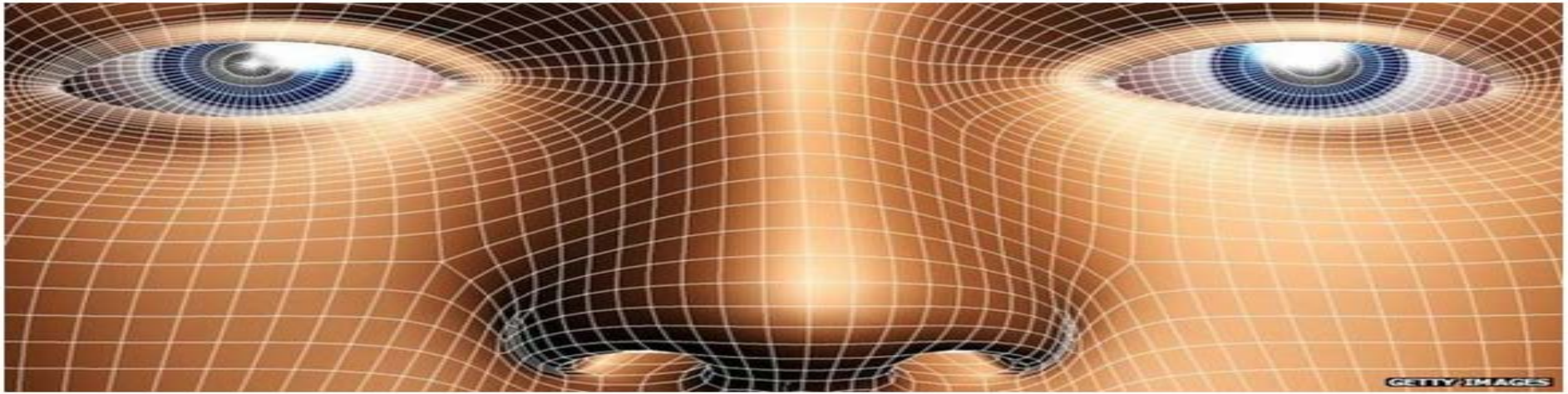


Technology

Is facial recognition tech really a threat to privacy?

By Matthew Wall
Technology reporter, BBC News

19 June 2015 | Technology



Facebook has decided not to offer its photo-sharing app Moments in Europe because of regulator concerns over its facial recognition technology.

And earlier this week, talks between US tech firms and privacy campaigners broke down over fears about how the industry is planning to use the tech.

So why is there so much concern over facial recognition tech, and is it justified? We unpick some of the issues.

Potential for Hacking and Spoofing

It's Alarmingly Easy to Hack the Samsung Galaxy S8's Iris Scanner

Adam Clark Estes
5/23/17 11:40am · Filed to: SECURITY

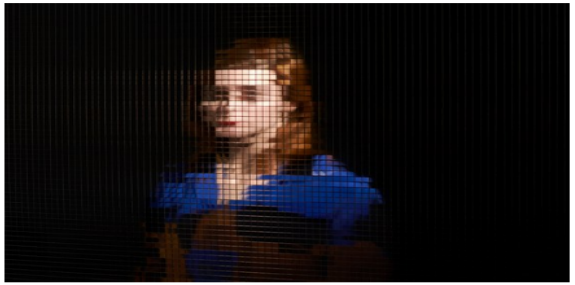
30.2K 44 8

Image: CCC

Samsung wants you to think that the iris scan technology on its new flagship phone, the Galaxy S8, is unbeatable. But it should surprise no one who pays attention to the security world that this is not the case. In fact, Samsung's new iris scanner is very easy to trick.

LILY HAY NEWMAN SECURITY 08.19.16 8:00 AM

HACKERS TRICK FACIAL-RECOGNITION LOGINS WITH PHOTOS FROM FACEBOOK (WHAT ELSE?)



GETTY IMAGES

FACIAL RECOGNITION MAKES sense as a method for your computer to recognize you. After all, humans already use a powerful version of it to tell each other apart. But people can be fooled (disguises! twins!), so it's no surprise that even as computer vision evolves, new attacks will trick facial recognition systems, too. Now researchers have demonstrated a particularly disturbing new method of stealing a face: one that's based on 3-D rendering and some

Proskauer

ANDY GREENBERG SECURITY 09.23.15 11:30 AM

WIRED

OPM NOW ADMITS 5.6M FEDS' FINGERPRINTS WERE STOLEN BY HACKERS

GETTY IMAGES/WIRED

TECHNOLOGY

Who Owns Your Face?

In June, government talks about how best to regulate facial-recognition algorithms fell apart. But should a company need your permission before scanning your face? And does the technology really work?

522

ROBINSON MEYER | JUL 2, 2015

The Switch

Facial recognition technology is everywhere. It may not be legal.

A The Washington Post

By Ben Sobel June 11

Co-administrator of the facial recognition program for the Pinellas County (Fla.) Sheriff's Office, Scott McCallum, displays a method of facial mapping used to set criteria for facial image searches. The sheriff's office uses one of the most advanced facial recognition programs for law enforcement in the country. (By Edward Linsmier for The Washington Post, 2013 file)

Ben Sobel is a researcher and incoming Google Policy Fellow at the Center on Privacy & Technology at Georgetown Law.

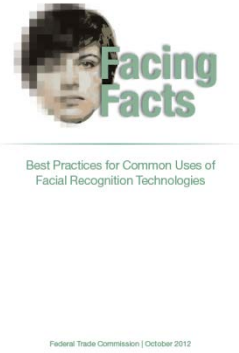
Being anonymous in public might be a thing of the past. Facial recognition technology is already being deployed to let brick-and-mortar stores scan the face of every shopper, identify returning customers and offer them

Biometric Legislation & Regulation

Proskauer

Biometrics – Federal Response

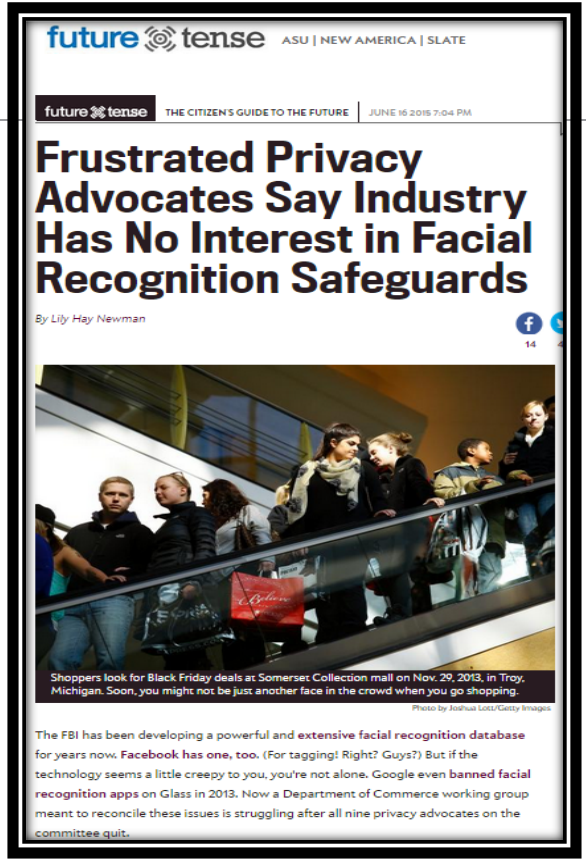
- Oct. 2012: FTC report, “Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies.”



- Synthesized the discussions and comments from FTC’s December 2011 “Face Facts Forum.”
- Among other things, the FTC report recommended that social networks using facial recognition features should provide consumers with clear notice about how the feature works, what data it collects, and how that data will be used, and should provide consumers with an easy opt-out option and the ability to turn the feature off at any time and have the biometric data previously collected from their photos permanently deleted.
- Report also noted that even if a company does not itself intend to implement facial recognition technologies, it should consider putting protections in place that would prevent unauthorized scraping of publicly available images it stores in its online database.

NTIA Initiative

- Major self-regulatory initiative intended to address privacy concerns associated with facial recognition technology.
  - Advocates and industry groups were attempting to develop a voluntary, enforceable code of conduct for the use of facial recognition technology and generally define the contours of transparency and informed consent.
- Stumbling block: nine consumer advocacy groups withdrew due to a lack of consensus on a minimum standard of consent re: commercial use of facial recognition technology.
- Self-regulatory guidelines were issued, but without any significant privacy requirements.



future tense ASU | NEW AMERICA | SLATE

future tense THE CITIZEN'S GUIDE TO THE FUTURE | JUNE 16 2015 7:04 PM

Frustrated Privacy Advocates Say Industry Has No Interest in Facial Recognition Safeguards

By Lily Hay Newman

14

Shoppers look for Black Friday deals at Somerset Collection mall on Nov. 29, 2013, in Troy, Michigan. Soon, you might not be just another face in the crowd when you go shopping.

Photo by Joshua Lott/Getty Images

The FBI has been developing a powerful and **extensive facial recognition database** for years now. **Facebook has one, too.** (For tagging! Right? Guys?) But if the technology seems a little creepy to you, you're not alone. Google even **banned facial recognition apps** on Glass in 2013. Now a Department of Commerce working group meant to reconcile these issues is struggling after all nine privacy advocates on the committee quit.

Proskauer

Facial Recognition – GAO Report

July 2015: GAO report, “Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law”

- Legal landscape specifically addressing facial recognition is spare.
- Federal law does not expressly address when commercial entities can use facial recognition technology to identify or track individuals, when prior consent should be required for the technology’s use, or how personal data gleaned from the technology may be used or shared.

Proskauer

Facial Recognition – GAO Report

GAO report noted the key issues that have been raised regarding facial recognition technology:

- **Consumer control over personal information**: Concerns about faceprints being sold or shared, especially since marketers might be interested in the fact that faceprints can link a person's online and offline presence.
- **Data Security**: Heightened concerns when biometric data is subject to a data breach.
- **Misidentification**: Technology does generate errors and captured image wrongly identified could propagate throughout different commercial systems without the individual's knowledge.
- **Disparate Treatment**: Concern about disparate treatment based upon information derived from facial recognition – denial of access to products/services if consumer denies consent; potential for "marketing surveillance" and price discrimination.

Facial Recognition – Federal Laws?

- **Wiretap Laws:** Intended to address surreptitious eavesdropping of communications, but not a square fit for biometrics.
- **HIPAA**: Rules implementing the Act list full-face images and biometric identifiers among the personal identifiers that must be removed before protected health information is no longer considered individually identifiable health information.
- **GLB**: GLB could potentially restrict the ability of financial institutions to share data collected with facial recognition technology if such data fell within the laws' definitions of protected information.
- **COPPA**: 2013 COPPA amendments classified a photograph of a child under 13 as "personal information"
- **Driver's Privacy Protection Act**: The Act addresses the use and disclosure of personal information contained in state DMV records (driver's license photos are defined as personal information).
- **FERPA**: Department of Education's regulations implementing FERPA include biometric records (and facial characteristics) within the definition of "personally identifiable information."
- **Video Voyeurism Prevention Act of 2004**: Prohibits capture of images of an individual's "private area" without consent, or to knowingly do so under circumstances in which that individual has a reasonable expectation of privacy. However, "Private area" does not include faces.

Children's Online Privacy Protection Act (COPPA)

- The COPPA Rule defines "personal information" to include individually identifiable information that is collected online, and expressly includes "a photograph, video or audio file that contains a child's image or voice." (16 C.F.R. §312.2(8))
- Applies to operators of commercial website or online services with actual knowledge of the collection of information from children under 13, or if website or online service is targeted to children under 13
- The COPPA Rule broadly defines website or online service to include any service that connects to the internet or any other wide-area network (e.g., websites, mobile apps, network-connected games, voice over IP services, location based services, social networking services).
- Clearly applies to social media apps, sites and services.
- Could COPPA apply to network connected security cameras that capture children entering a stadium, where photographs and faceprints are stored in the cloud?

Biometric Privacy –State Legislative Activity

- Some examples of related state laws:
  - Three states have passed specific biometric privacy laws
  - Several states deem biometric information as “personal information” in breach notification laws
  - Some states regulate school use of biometrics
- There are also a number of pending state bills that touch on biometric privacy for commercial uses (including drones), governmental collection and use of biometric data, and the collection and use of biometric data of students.

Biometric Privacy – State Statutes

Texas: Tex. Bus. & Com. Code Ann. §503.001(c) (2007)

- "Biometric identifier": retina or iris scan, fingerprint, voiceprint, hand or face geometry.
- A person may not capture a biometric identifier of an individual for a **commercial purpose** unless the person:
  - (1) **informs the individual** before capturing the biometric identifier; and
  - (2) **receives the individual's consent** to capture the biometric identifier.
- A person who possesses a biometric identifier of an individual:
  - (1) **may not sell, lease, or otherwise disclose** the biometric identifier to another person unless:
  - (A) the individual **consents** to the disclosure;
  - (B) the disclosure **completes a financial transaction that the individual requested or authorized**;
  - (C) disclosure permitted by law (other than FOIA) or made for law enforcement purpose
- **No private right of action**: State attorney general may bring an action ($25K/violation)

Private Right of Action

Proskauer

Biometric Privacy – State Statutes

Illinois: Biometric Information Privacy Act, ("BIPA") 740 ILCS 14/1 (2008):

- Preamble to statute mentions legislative findings suggesting growing use of biometrics in security screenings and financial transactions and that the public may be wary of the use of biometrics in such settings, justifying some regulation in this area.
- "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. **Biometric identifiers do not include** writing samples, written signatures, **photographs**, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions…."
- "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. **Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers**.

Biometric Privacy – State Statutes

Illinois: Biometric Information Privacy Act, ("BIPA") 740 ILCS 14/1 (2008):

- A company cannot collect, capture, purchase, receive through trade, or otherwise obtain a person's biometric identifier or biometric information, unless it first:
  - (1) **informs the subject in writing** that a biometric identifier is being collected
  - (2) **informs the subject in writing** of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
  - (3) **receives a written release executed by the subject**
- Statute also provides that entities in possession of such information post a written policy establishing a retention schedule and guidelines for deleting data when the initial purpose for collection has been satisfied or within 3 years of the user's last interaction with the entity.
- **Right of Action**: Provides for a private cause of action: $1,000 in statutory damages for each negligent violation, and $5,000 for intentional or reckless violation; injunctive relief; and costs and attorney's fees.
  - BIPA has been the vehicle for biometric privacy class actions lawsuits.

Biometric Privacy – State Statutes

Washington: HB1493 (passed May 16, 2017; effective July 23, 2017)

- Similar to BIPA, the bill's stated purpose is to require a business that collects and can attribute biometric data to a specific individual to disclose how it uses that biometric data and provide notice to and obtain consent from an individual before enrolling or changing the use of that individual's biometric identifiers in a database.
  - Also places limits on sale or disclosure to third parties – allows it with consent or other narrow conditions of use (e.g., complete a financial transaction, provide a requested service, required by law)
  - **No private right of action**: enforced by the state attorney general
  - *Exceptions*: Does not cover biometric identifiers that have been "unenrolled" (i.e., not able to matched to a specific person, perhaps meaning de-identified biometric data) or biometric identifiers collected and stored "in furtherance of a security purpose."
  - Holder of biometric data enrolled for commercial purposes must "guard against unauthorized access" and may retain the data no longer than is reasonable necessary to provide services

	Definition of Biometric Identifier	Private Right of Action	Basic Requirements	Relevant Exceptions
Illinois: Biometric Information Privacy Act, ("BIPA") 740 ILCS 14/1 (2008):	"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.	Yes. Statutory damages available, injunctive relief, and award of attorney's fees.	Notice and written consent; biometric policy and retention schedule; no sale or lease of biometric information. Data security (storage, transmission) as per reasonable industry standards for sensitive data.	Disclosure and dissemination with consent, if it completes an authorized financial transaction; or otherwise required by law.
Texas: Tex. Bus. & Com. Code Ann. §503.001(c)	"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.	No. Enforced by attorney general.	Notice and consent; no sale or disclosure; data destruction requirements. Data security on par with confidential information.	Sale or disclosure only with consent, to complete a financial transaction, or as required by law.
Washington HB1493	"Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual.	No. Enforced by attorney general..	Notice and consent for "enrolled" data; retention limitations; no use inconsistent with purpose at collection. Reasonable data security	Sale or disclosure with consent, complete a requested service or financial txn, 3P disclosure with contractual protections. - "Unenrolled" biometric data. - For "security purpose"

Selected Pending Biometric Privacy Bills

- **Alaska (HB 72)**: Similar to BIPA, would prohibit the collection of biometric data without proper notice and consent; requires timely data disposal. Provides a private right of action. **Status: In committee.**
- **Arizona (SB 1373)**: Limitations on collection of biometric identifiers by school or school service providers without consent and retention schedule. **Status: In committee.**
- **California** (**SB 327)**: Would require manufacturers of smart devices to, among other things, indicate when it they are collecting audio, video, location, health or biometric data beyond the stated functionality of the device and obtain consent before collecting or transmitting such information. **Status: In committee; on inactive file.**
- **Connecticut (Proposed HB 5522)**: This proposed bill would aim to prohibit retailers from using facial recognition software for marketing purposes. **Status: Referred to committee.**
- **Illinois (HB 2411)**: This bill would amend BIPA and provide that except to the extent necessary for an employer to conduct background checks or implement security protocols, a private entity could not require a person or customer to provide a biometric identifier or biometric information as a condition for the provision of goods or services. **Status: Assigned to committee**.
- **Massachusetts (SB 95):** Would add “biometric indicator” to the definition of PI under the state’s data security law (includes laws re: safeguarding of consumer PI and breach notification. **Status: In committee**.
- **New Hampshire (HB 523)**: Bill would regulate the collection, retention, and use of biometric information. Includes a private right of action. **Status: In committee.**
- **Texas (HB 3491)**: Limits collection of biometric identifiers by gov't bodies. **Status: In committee; placed on general state calendar.**

Additional State Laws to Consider? Right of Publicity

- Use of an individual's identity or likeness for commercial exploitation.
- Cal. Civil Code § 3344: "Any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent, or, in the case of a minor, the prior consent of his parent or legal guardian, shall be liable for any damages sustained by the person or persons injured as a result thereof."
- New York Civil Rights Law § 51: "Any person whose name, portrait, picture or voice is used within this state for advertising purposes or for the purposes of trade without the written consent… may maintain an equitable action…to prevent and restrain the use thereof; and may also sue and recover damages for any injuries sustained…."
- Could such laws apply to facial or other biometric scans that are then used for commercial purposes?
- What are the First Amendment considerations, particularly while recording people in public?

Biometrics Privacy Advocacy

- International Biometrics & Identification Association (IBIA) released “Privacy Best Practice Recommendations for Commercial Biometric Use” (Aug. 2014), which was submitted during NTIA process. Basic principles recommending notice and cybersecurity.
- American Civil Liberties Union: “An Ethical Framework for Facial Recognition” (May 2014). Advocated for stricter standards for use, notice, and consent than those recommended by the IBIA. Also submitted during NTIA process.
- Digital Signage Federation issued privacy standards for its members in 2011. Under standards, companies should post privacy policies, obtain consent before affirmatively identifying an individual, notice at site if collecting general demographic data.
- EFF: In Senate testimony in 2012, the EFF stated that because of the risk that faceprints will be collected without individuals’ knowledge, rules should define clear notice requirements to alert people that a faceprint has been collected and include information on how to request that data collected on them be removed.

Biometric Privacy Litigation

Proskauer

Illinois Facial Recognition Law Leads To Wave Of Class Actions Against Facebook, Others

Legal Newsline, CONTRIBUTOR

We cover issues that affect businesses in state and federal courts FULL BIO

Opinions expressed by Forbes Contributors are their own.

POST WRITTEN BY

Stephanie Grimoldby

I am a freelance reporter who has written for numerous publications, on legal issues and business trends. Valparaiso grad.

A Facebook employee holds a laptop with a 'like' sticker on it during an event at Facebook headquarters on April 4, 2013, in Menlo Park, California. (Photo by Justin Sullivan/Getty Images) [+]

At the opening of this millennium, the idea of computer programs using facial recognition software to target ads to people was the stuff of such science fiction stories as the 2002 film "Minority Report."

Biometric Privacy Lawsuits

THE DAILY ONLINE EXAMINER

Google Accused Of Violating Illinois Privacy Law By Compiling 'Faceprints'

by Wendy Davis @wendyndavis, Yesterday, 4:08 PM

Comment ★ Recommend (1)

Google has been hit with a potential class-action lawsuit in Illinois for allegedly violating a state privacy law by collecting people's "faceprints" without their consent.

55 SHARES

"Google has created, collected and stored, in conjunction with its cloud-based 'Google Photos' service, millions of 'face templates' (or 'face prints') -- highly detailed geometric maps of the face -- from millions of Illinois residents, many thousands of whom are not even enrolled in the Google Photos service," Illinois resident Lindabeth Rivera alleges in a lawsuit filed Tuesday in federal court in Illinois.

Lawsuit challenging Facebook's facial recognition system moves forward

Judge says the company is bound by Illinois's biometric privacy law

by Russell Brandom | @russellbrandom | May 5, 2016, 8:05pm EDT

SHARE TWEET LINKEDIN

A lawsuit alleging that Facebook photo tagging violates user privacy has cleared a crucial early hurdle. A judge in Northern California District Court today ruled against a motion by Facebook to dismiss. That leaves the larger questions around biometric privacy

L.A. TAN™
THE TANNING AND SKIN CARE PROFESSIONALS

Company to pay $1.5 million in suit filed under Illinois Biometric Privacy Act

Tanning salon used fingerprint access control, did no harm, but failed to obtain written consent

26 December, 2016 By: Chris Corum CATEGORY: BIOMETRICS, CORPORATE

SHUTTERFLY

Shutterfly hit with privacy suit over "faceprints," use of photos

Jeff John Roberts
Jun 18, 2015

A Chicago man claims the popular photo-book service Shutterfly is violating a law that restricts how companies collect biometric data, and is seeking at least $5 million on behalf of others whose faces have been added to the Shutterfly (SFLY, -1.23%) database without permission.

THE DAILY ONLINE EXAMINER

Take-Two Fights 'Gotcha' Privacy Suit

by **Wendy Davis** **@wendyndavis**, May 30, 2017

Take-Two Interactive Software is asking an appellate court to refuse to revive a class-action lawsuit accusing the company of violating an Illinois privacy law by collecting faceprints of video game players.

The company argues that the alleged violations didn't result in any injury to Vanessa and Ricardo Vigil -- the brought and sister who brought the case.

Proskauer

NBA 2K15

You'll Be Able To Scan Your Face Into NBA 2K15

preview

17

by Mike Futter on September 17, 2014 at 02:26 PM / 18,635 Views / PS4 / ★★★★★

This year, 2K Sports will be fulfilling the wishes of many NBA hopefuls (and couch coaches). You'll be able to use first-party camera technology like the PlayStation camera on PS4 to create a 3D model of your face in the game.

A new video shows off the process, which involves a short amount of time and a straightforward process. The resultant scan can be tweaked before you take control of your hoops star.

Biometric Privacy Litigation –

Santana v. Take-Two Interactive Software, Inc., No.15-08211 (S.D.N.Y. filed Oct. 19, 2015)

- Plaintiffs' putative class action claims violation of BIPA over collection, storage, use and dissemination of users' face templates via the gaming platform camera for the creation of a virtual avatar that resembles the user.
- Image is also allegedly disseminated to others during multiplayer games.
- Claims:
  - Lack of adequate consent before collection (specifically, claims lack of notice of "indefinite storage of face template on Take-Two's servers")
  - Complaint cites company's alleged contravention of FTC 2012 privacy principles on facial recognition
  - Lack of written notice of purpose and posted retention schedule for faceprints
  - Lack of posted biometric privacy policy
  - Sought damages for intentional violation of BIPA ($5K per violation), or alternatively, negligent violation ($1K/violation); and injunctive relief

Judge rules in favor of video game maker using biometrics

NBA 2K15 uses face biometrics for player avatars, company sued under Illinois Biometric Information Privacy Act

01 February, 2017 By: **Chris Corum** CATEGORY: BIOMETRICS, CORPORATE

An important court decision impacting the biometric industry was reached as an Illinois judge found that a video game publisher would not be penalized for storing player face likenesses for in-game display.

It's an big win for the use of biometrics as the uncertainty caused by a 2008 Illinois state law has had many concerned about launching consumer-facing implementations.

Late last year, SecureIDNews reported that another Illinois judge found that a tanning studio had violated the state's Biometric Information Privacy Act and was ordered to pay $1.25 million.

Biometric Privacy Litigation – Videogames

Vigil v. Take-Two Interactive Software, Inc., No. 15-8211 (S.D.N.Y. Jan. 27, 2017) (on appeal to Second Circuit)

- Court dismissed BIPA claims over Take-Two's NBA 2K videogame series
  - If a user wants to use the MyPlayer function, he or she must agree to the following terms:
    - Your face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay. By proceeding you agree and consent to such uses and other uses pursuant to the End User License Agreement. www.take2games.com/eula
  - The plaintiffs made no allegations that their faceprints were disseminated or used for any other purpose outside of the game (for which they gave consent).
- Court ruled that procedural violations of the notice and consent provisions of BIPA are not in-of-themselves sufficient to confer standing under *Spokeo*.
  - Court: "The alleged failure to give the plaintiffs more extensive notice and consent is not a material risk to a concrete BIPA interest where no material risk of biometric data misuse ever materialized."

Biometric Privacy Litigation – Fingerprints

Sekura v. L.A. Tan Enterprises, Inc., No. 2015-CH-16694 (Ill. Cir. Ct. Cook Cty. First Amended Class Complaint filed Apr. 8, 2016)

- Illinois court approved a $1.5M settlement in a class action against L.A. Tan.
- Settlement resolved allegations that L.A. Tan violated BIPA by collecting Illinois members' fingerprints for verification during check-in without proper notice and consent requirements (note: no allegations of misuse or disclosure)
  - Unlike other facilities that issue membership cards or fobs to present at check-in, L.A. Tan salons reportedly collected members' fingerprints and stored them in a company-wide database to enable check-in at any national location.
  - Beyond alleged violations for such fingerprint collection without proper consent, the complaint asserted that L.A. Tan salons violated BIPA by disclosing member fingerprints to an out-of-state vendor without first obtaining member consent. Complaint also claims that L.A. Tan failed to provide members with a written data retention policy that disclosed guidelines for permanently destroying its customers' fingerprints as required by BIPA.
  - As fingerprints are expressly included in definition of "biometric identifier," the salient legal issues in the dispute appeared to be whether or not L.A. Tan complied with the statute, to what extent L.A. Tan could be liable for alleged BIPA violations of its franchisees (interestingly, the Settlement's definition of "Released Parties" expressly excludes all L.A. Tan franchisees), and any potential class certification issues.

Biometric Privacy Litigation – Fingerprints The Latest Dispute

Baron v. Roundy's Supermarkets Inc., No. 17-03588 (N.D. Ill. Ill. filed May 11, 2017)

- Claims alleging violations of BIPA against supermarket chain for collecting employees' fingerprints for clocking in and out – no written consent for storage; no retention policy.
- Standing/*Spokeo* issues?

Lawsuit alleges supermarket chain violated Illinois' biometrics info privacy law

BIOMETRIC UPDATE.COM

By Justin Lee Tweet

May 31, 2017 - Employees at Roundy's Supermarkets, Inc. have filed a class action suit alleging that the supermarket chain violated Illinois' Biometric Information Privacy Act (BIPA), according to a report by HRDive.

The lawsuit claims the company's practice of obtaining and storing employees' fingerprints for timekeeping purposes does not meet adhere to the state's BIPA requirements.

Proskauer

Biometric Privacy Litigation – Fingerprints

McCollough v. Smarte Carte, Inc., No. 16-03777 (N.D. Ill. Aug. 1, 2016)

- An Illinois federal court dismissed, for lack of standing, a putative class action alleging BIPA violations against Smarte Carte, a train locker concession, for allegedly retaining plaintiff's fingerprint data without proper consent.
  - The lockers at issue in Chicago's Union Station used the renter's fingerprint as a "key."
- Plaintiff alleges that Smarte Carte violated BIPA by failing to obtain advance consent and inform her that it would retain her fingerprint data and for what period of time, if any, beyond the rental period.
  - Citing *Spokeo*, the court granted the motion, finding plaintiff only alleged a "bare procedural violation."
  - Court: "How can there be an injury from the lack of advance consent to retain the fingerprint data beyond the rental period if there is no allegation that the information was disclosed or at risk of disclosure? It was simply retained."

Biometric Privacy Litigation – Photo Tagging

- In the set of photo tagging lawsuits against social media providers, plaintiffs have generally brought claims against tech companies for allegedly collecting and storing biometric data without adequate notice and consent and failing to provide a retention schedule and guidelines for permanent deletion, or otherwise comply with Illinois statute (BIPA) with respect to Illinois users.
  - Non-user issue: In one suit, plaintiff claimed that Shutterfly creates a template for each face in an uploaded photo, regardless of whether a face belongs to a Shutterfly user or unwitting nonuser.
- Complaints seek injunction relief and statutory damages for each violation.
- While BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," it also specifically excludes photographs from that definition. Facebook and others have attempted to dismiss suits over photo tagging by using this apparent ambiguity within the statute.
  - Facebook: ""The across-the-board exclusion of photographs and information derived from them would be rendered meaningless if the statute were interpreted to cover data derived from the scan of a photograph."
  - Defendants have argued that the statutory text "scan of hand or face geometry" means an in-person scan of a person's actual hand or face (as for verification or security purposes).

Biometric Privacy Litigation – Photo Tagging

- In three instances, a district court refused, at an early stage of a litigation, to dismiss BIPA claims relating to the online collection of facial templates for photo-tagging purposes.
  - ***Norberg v. Shutterfly, Inc.,* No. 15-05351 (N.D. Ill. filed June 17, 2015):** Court allowed BIPA claim to go forward; matter was settled in April 2016.
  - ***In re Facebook Biometric Information Privacy Litig.,* No. 15-03747 (N.D. Cal. May 5, 2016):** Court found Facebook's terms of use to be enforceable, but declined to enforce the California choice of law provision and held that the plaintiffs stated a claim under BIPA.
  - ***Rivera v. Google, Inc.*, No. 16-02714 (N.D. Ill. Feb. 27, 2017):** An Illinois district court refused to dismiss a putative class action alleging that the cloud-based Google Photos service violated BIPA by automatically uploading plaintiffs' mobile photos and allegedly scanning them to create unique face templates (or "faceprints") for subsequent photo-tagging without consent.

Final Takeaways and Practical Tips

Proskauer

Business and Economic Issues to Consider

- **Vendor Lock In:** How do you avoid “vendor lock-in” to biometric solutions?
- **Insurance:** Evaluate your cybersecurity insurance policies to see if they cover biometric-related issues.
- **Technology Failure**: What are the implications of technology failure for your organization? While the frequency of failure varies based on what form of biometrics one uses (e.g. voice, faceprint, iris scan, fingerprint), systems are subject to authentication failure or other incidents. In many cases, these technologies are still evolving.
- **ROI**: Is this a worthwhile investment for your organization? It may involve a significant information technology investment (e.g., software and hardware, legacy system upgrades, maintenance, consulting, etc.) as well as employee training and user education. This must be balanced many expected benefits -- new products, services or features; reduced fraud or unauthorized access; cost efficiencies; enhanced customer service; and risk avoidance.
- **PR:** How will your customers feel? Many people find biometrics to be creepy, so customer relations should remain an important consideration.

Data Security Issues to Consider

- As seen in the OPM breach of 5.6 million fingerprints, biometrics data could be subject to a security breach that results in sensitive data accessed by unauthorized entities.
  - Government re: the OPM breach: "Federal experts believe that, as of now, the ability to misuse fingerprint data is limited. However, this probability could change over time as technology evolves."
  - Biometric data breach may have an even greater impact than the breaches of financial and personal data because passwords or payment card data can be changed or reissued, while a faceprint cannot.
  - Organizations that collect and store biometric data must be prepared to house such data with appropriate levels of security, access restrictions and safeguards, including using encryption and restricting third-party access to biometric data unless necessary for the purpose of collection.
- Should evaluate whether cybersecurity insurance policies would cover this data.

Privacy Issues to Consider

- How should the concepts of transparency and consent apply to the collection and use of biometric data?
- What level of control should individuals have over when and how biometric data is stored and used?
- What limitations should be placed on the sale of biometric data to third parties? What contractual protections should be considered when allowing a third party access to biometric data to provide services?
- Should companies obtain prior affirmative consent before collecting such data?
- How should a company's policy regarding biometric data deal with non-members of a service or anonymous members of the public captured in a photo?
- What level of transparency is appropriate when a company combines biometric data with third-party data for analytics or secondary uses?
- How should a company address retention periods for biometric data?
- Data disposal: What should happen to the biometric data of a user who unsubscribes from a service?
- Should biometric data be the subject of heightened data security (e.g. encryption)?
- Should additional restrictions be placed on the use of commercial technology re: teens' biometric data?
- Would a standard electronic contracting process, whereby a user consents to a service's terms of service and privacy policy via a clickwrap agreement, constitute appropriate notice and consent for the use of biometric data? Or must there be a distinct, written notice and consent process for facial recognition data collection practices as well as a formal, posted facial recognition policy?

Thank You!

Any Questions?

Paresh Trivedi
ptrivedi@proskauer.com

Proskauer