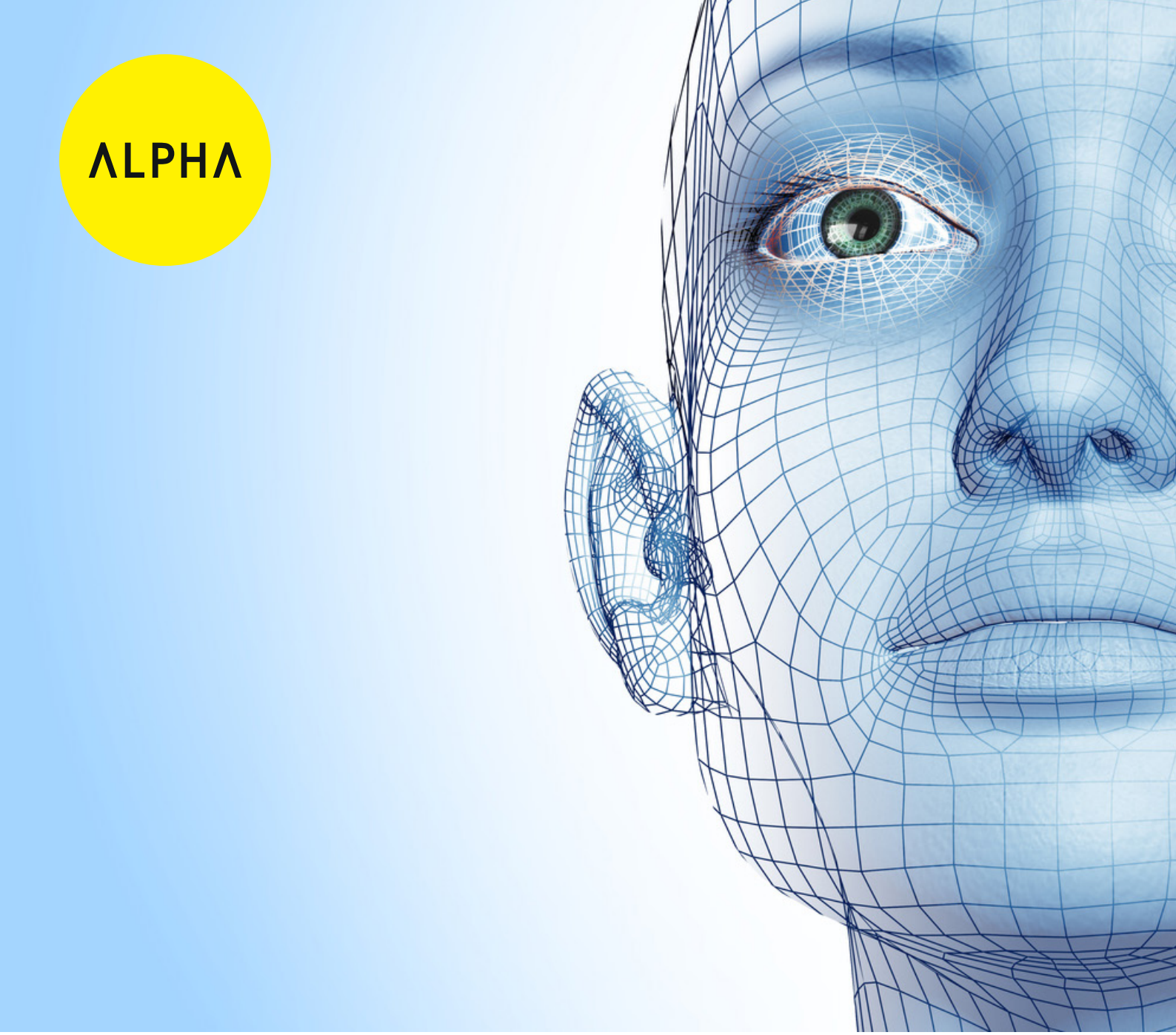


Thought piece

The end of anonymity?

Unmasking the ethics of face recognition

Whether you're having a bad hair-day, or just popping to the 7/11 in your sweats, sometimes it's nice to go unnoticed. But from social networks to street corners, biometric facial recognition technology could soon render the phrase "just a face in the crowd" obsolete – raising huge questions over privacy, consent and data profiling.

ALPHA LTD
St Andrew's House
St Andrew's Road
Cambridge CB4 1DL
United Kingdom

@thisisalphalive

thisisalpha.com

Facing the future

A world where your face is immediately recognised has huge opportunities; largely for money-makers.

We've seen it in fiction. In the film *Minority Report*, Tom Cruise's character is bombarded by personalised ads from billboards as he makes his way through the mall – "John Anderton! You could use a Guinness right now" suggests one. Inside Gap, he overhears a hologram greeting another retina-scanned customer: "Welcome back Miss Balfour. Did you come back for another pair of those chamois lace-ups?"

Instant recognition can give access to a history of consumer choices and demographics, followed up by a targeted on-brand customer interaction. Which is every marketer's dream, right? In *Minority Report*, however, the commercial opportunities have some deeply sinister undertones. The State, for example, uses the same retina-scanning technology to detect and arrest those "predicted" to commit crimes at some future date. When Anderton falls under suspicion for a "future" crime, he visits a black market doctor for an eye transplant in an attempt to avoid capture. The film suggests that, in a world where our personal identity is always accessible via our physical features, the line between empowered consumer choices and coercive state surveillance is a fine one.

The future of happy meals

Back in 2002, when Steven Spielberg directed *Minority Report*, this kind of technology may have appeared wildly futuristic – the film itself is set in 2054. Yet, a decade-and-a-half later, many aspects of *Minority Report* are already with us. Advertising technology that profiles consumers by their facial characteristics? Check. Stores using facial recognition systems to recognise repeat customers? Check. Security services employing "real-time" facial surveillance in public spaces to identify suspects? Check. It's not yet quite as slick as the Hollywood version, but the everyday application of facial recognition technology has most definitely arrived.

In Beijing, for example, KFC recently installed facial recognition technology in one of its restaurants to offer customers personalised menu recommendations based on their age, sex and, apparently, mood[1]. The system is designed to remember the faces of repeat customers and their preferences, so that they can quickly order the menu combinations they like best. We are not, as yet, clear whether the system can detect the facial signals which clarify the difference between the office worker feeling a little peckish (those tell-tale salad eyes) or dangerously ravenous (the feed-me-now look).

[1] https://www.theguardian.com/technology/2017/jan/11/china-beijing-first-smart-restaurant-kfc-facial-recognition

Back in 2013, supermarket giant Tesco unveiled plans to install facial recognition technology in its petrol stations, aiming to target adverts at customers according to their age and gender[2]. There are some important differences to note in these two approaches. At the KFC restaurant in Beijing, customers can choose whether to use facial-recognition technology or not. The reported lack of queues at the automated counters suggest that the new approach to customer service hasn't yet caught the imagination of the chicken-loving Chinese public, who still prefer to order their meals at the human-staffed counters.

There was no such "opt-in" choice in the Tesco model – customers were to be scanned indiscriminately and without their knowledge. This divergence of models, and the issue of consent, brings us to heart of the ethical debate on facial recognition. In public spaces, what rights do we as individuals have over the biometric scanning of our faces? How is such biometric data stored? Who has access to it and for what purposes? Ultimately, of course, perhaps the most urgent question in this fast-moving technology sector is: can and should legislation try to protect our rights to privacy in the light of increased exposure to it? And, if so, how?

The absence of consent

According to some, current privacy legislation is woefully inadequate to deal with this new set of 21st-century challenges. US Senator Al Franken, as Chairman of the US Subcommittee on Privacy and the Law, wrote: "Unlike other biometric identifiers such as iris scans and finger prints, facial recognition is designed to operate at a distance, without the knowledge or consent of the person being identified... Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere – on a lamp post, attached to an unmanned aerial vehicle or, now, integrated into the eyewear of a stranger"[3].

His comments were made in response to the controversy generated by *NameTag*, the first facial recognition app to be developed for Google Glass. In 2014, the app sparked a rash of often hostile media reaction[4] as a result of its purported ability to match the faces of strangers with their online profiles, providing users with instant access to personal details potentially gained from dating sites such as Match.com.

[2] http://www.bbc.co.uk/news/technology-24803378

[3] https://www.theguardian.com/technology/2014/may/04/facial-recognition-technology-identity-tesco-ethical-issues

[4] http://www.cbc.ca/newsblogs/yourcommunity/2014/01/nametag-facial-recognition-app-criticized-as-creepy-and-invasive.html

Familiar strangers

NameTag obviously viewed their offering as a legitimate and logical extension of our shared online experience. But to many others, this is a serious breach of their rights. Certainly Senator Franken found the whole concept deeply concerning, writing to the app's owners to say: "This [process] is apparently done without that person's knowledge or consent, which crosses a bright line for privacy and personal safety. I urge you to delay this app's launch until best practices for facial recognition technology are established..."[5].

Of course, being targeted by an overbearing retail outlet or a potential pick-up artist is only one of many concerns generated by the apparently unstoppable spread of facial recognition technology. Top of many lists is its unregulated use by law enforcement and other security agencies, in which George Orwell's vision of a state where "Big Brother is watching you" is quickly becoming a disturbing reality.

Pooling the evidence

According to a report by The Center on Privacy & Technology, 16 US states currently allow the FBI to use facial recognition technology to compare the faces of suspected criminals with driver licenses and ID photos, accessing images for nearly 64 million Americans[6]. Unlike databases for fingerprints or DNA, this biometric network is primarily made up of law-abiding citizens rather than those who have been investigated in relation to or convicted of a criminal offence.

In particular, the report highlights the potential threat from real-time streaming systems. "If deployed pervasively on surveillance video or police-worn body cameras," it says, "real-time face recognition will redefine the nature of public spaces. At the moment, it is also inaccurate. Communities should carefully weigh whether to allow real-time face recognition. If they do, it should be used as a last resort to intervene in only life-threatening emergencies. Orders allowing it should require probable cause, specify where continuous scanning will occur, and cap the length of time it may be used."[7]

[5] https://www.franken.senate.gov/?p=press_release&id=2699
[6] https://www.perpetuallineup.org/
[7] https://www.perpetuallineup.org/

A different angle: the security specialist

For others, however, the security benefits of facial recognition technology are already evident and compelling. Roger Rodriguez is one such advocate. Now part of a company specialising in facial and licence plate recognition technology, this former police officer served over 20 years with the NYPD and led its first dedicated facial recognition unit.

He is at pains to make the important distinction that we are discussing the use of a "biometric tool" rather than a "biometric science". "Facial recognition is not 100% accurate," he wrote in a post in February 2017. "But here's what I do know: After working on countless cases using facial recognition, I am certain it works when properly used in the investigative process to develop leads and help solve cases."[8]

He is also very clear in addressing one commonly voiced concern. "Facial recognition technology provides leads; it is NOT the basis for arrest. The onus always falls on the agency to establish probable cause. Agencies should follow best investigative practices and establish policies for facial recognition investigations including: documenting what you have done, creating an audit trail, and demonstrating a disciplined approach to facial recognition investigations."[9]

As with any truly disruptive technology, facial recognition presents us with ethical challenges and dilemmas that are new, complex and sometimes divisive. Could and should a regulatory framework help to safeguard our privacy in an era when our facial features can be scanned almost as accurately as a barcode? It is an important question that demands some urgent attention from lawmakers and enforcers, technology companies, marketers and, of course, citizens and consumers. Attempting to play legislative catch-up once the technology has become even more embedded is rarely a model for good regulatory practice.

How to be invisible

Finally, for those who may be feeling a little uncomfortable at the apparent proliferation of electronic eyes keeping tabs on you 24/7, all is not yet lost. Because, if you want to pick up some milk in your pyjamas at 5am without being recognised, there is one solution that doesn't involve sending your identical twin.

Berlin-based artist and technologist Adam Harvey has created a range of "anti-surveillance" patterns printed on clothing or textiles[10]. The project, known as Hyperface, is designed to confuse facial recognition technology systems by overloading them with images that are erroneously interpreted as facial features. No need, just yet, for a balaclava or face surgery. In the right outfit, it seems, hiding in plain sight is a perfectly viable option.

[8] https://www.vigilantsolutions.com/facing-the-facts-about-biometric-facial-recognition-technology/
[9] https://www.vigilantsolutions.com/facing-the-facts-about-biometric-facial-recognition-technology/
[10] https://www.theguardian.com/technology/2017/jan/04/anti-surveillance-clothing-facial-recognition-hyperface

Facial recognition technology in numbers

97.35% accuracy of Facebook's DeepFace facial recognition technology[11]
97.53% accuracy of human facial recognition[12]
0.33 seconds time taken for DeepFace to process one image[13]
350 million photos uploaded per day onto Facebook[14]
75% of survey respondents would not stop at a store that used facial recognition technology for marketing purposes.[15]

[11] https://www.cs.toronto.edu/~ranzato/publications/taigman_cvpr14.pdf

[12] https://www.technologyreview.com/s/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/

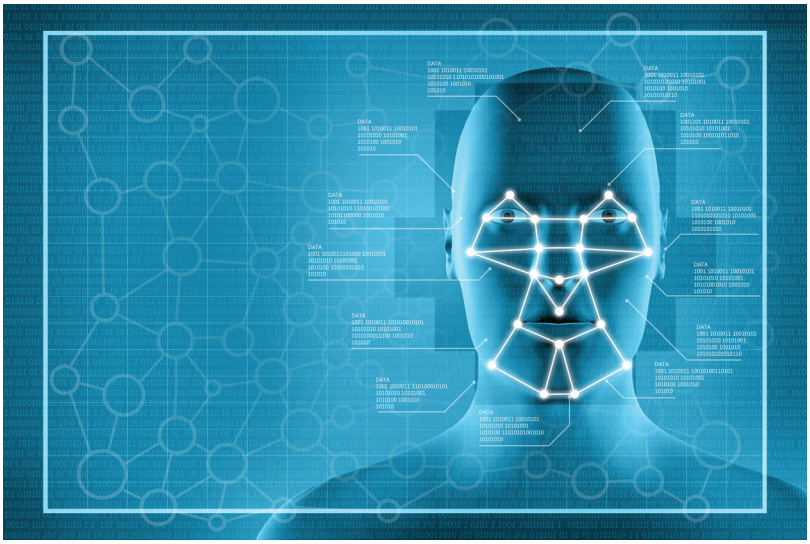
[13] https://www.cs.toronto.edu/~ranzato/publications/taigman_cvpr14.pdf

[14] http://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9?IR=T

[15] http://www.firstinsight.com/press-releases/true-detective-first-insight-finds-what-consumers-really-want-from-retailers

How does Facebook's DeepFace work?

Facebook's DeepFace 3D facial recognition technology has achieved 97.35% accuracy in matching different photos of the same person (or identifying non-matches). But how does it work? Unlike previous 2D technology, DeepFace builds up a 3D picture of the face based on measurements of features such as the curves of the eye socket, chin or nose.



Because the 3D image can be tilted or rotated in different directions, DeepFace can compare photos of subjects in different poses and lighting conditions. And as areas of rigid tissue or bone such as the eye socket, chin or nose are less prone to change over time, it's also easier compare younger and older photos of the same person.

Machine learning is the other key innovation driving DeepFace's high accuracy score. Each time the system correctly identifies a match or non-match, it stores and "learns" the steps it took to make the identification – making future matches both quicker and more accurate. Put simply, the more DeepFace is used, the better it becomes. Super smart or slightly worrying? Perhaps a bit of both.

Pull-quotes

> It's not yet quite as slick as the Hollywood version, but the everyday application of facial recognition technology has most definitely arrived.

> Ultimately, of course, perhaps the most urgent question in this fast-moving technology sector is: can and should legislation try to protect our rights to privacy in the light of increased exposure to it?

Found that interesting?

If you're not already signed up to our newsletter, email **marketing@thisisalpha.com** to receive lots more great articles that will help you on your journey to going global.