INFO 350

Surveillance

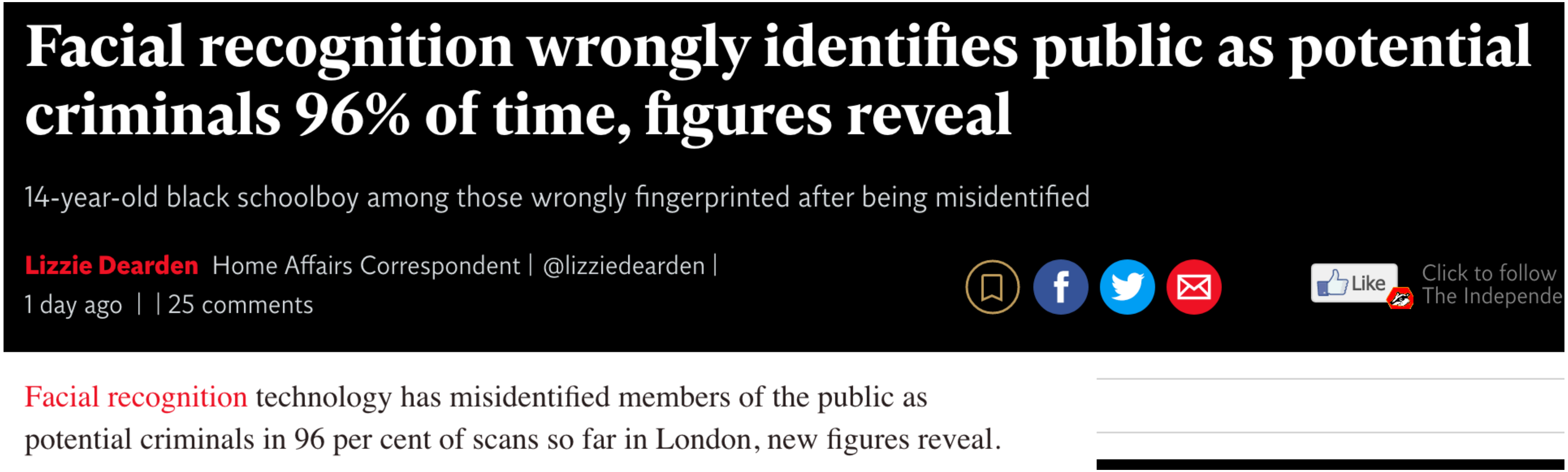
Facial Recognition

Facial Recognition

- What is it?
- Biometrics
  - Faces
  - Fingerprints
  - Gait analysis (?)
  - Haptic sensing (?)

What are the concerns?

- We are adopting this technology *fast*
  - Almost no regulations
  - Washington attempted a facial recognition law, but it failed
- Accuracy
  - Dark skin, feminine features lower recognition accuracy
  - What are the risks of “false positives?”
- Where and who gets targeted
  - Existing problems/questions about surveillance are not resolved
  - Biometrics more likely to be used on the low wage workers and communitites historically targeted by police, government, etc.



Facial recognition wrongly identifies public as potential criminals 96% of time, figures reveal

14-year-old black schoolboy among those wrongly fingerprinted after being misidentified

Lizzie Dearden Home Affairs Correspondent | @lizziedearden |
1 day ago | | 25 comments

Facial recognition technology has misidentified members of the public as potential criminals in 96 per cent of scans so far in London, new figures reveal.

Risk (law enforcement context)

- “What happens if a system like this gets it wrong? A mistake by a video-based surveillance system may mean an innocent person is followed, investigated, and maybe even arrested and charged for a crime he or she didn’t commit. A mistake by a face-scanning surveillance system on a body camera could be lethal. An officer alerted to a potential threat to public safety or to himself, must, in an instant, decide whether to draw his weapon. A false alert places an innocent person in those crosshairs.”
- *-Clare Garvie*

Authors’ main arguments

- Surveillance conducted with facial recognition systems is intrinsically oppressive.
- Facial recognition is often invisible, so you never know when it is happening.
- People will act differently if they suspect they’re being surveilled.
    - Aka “the chilling effect” personal expression and behavior.

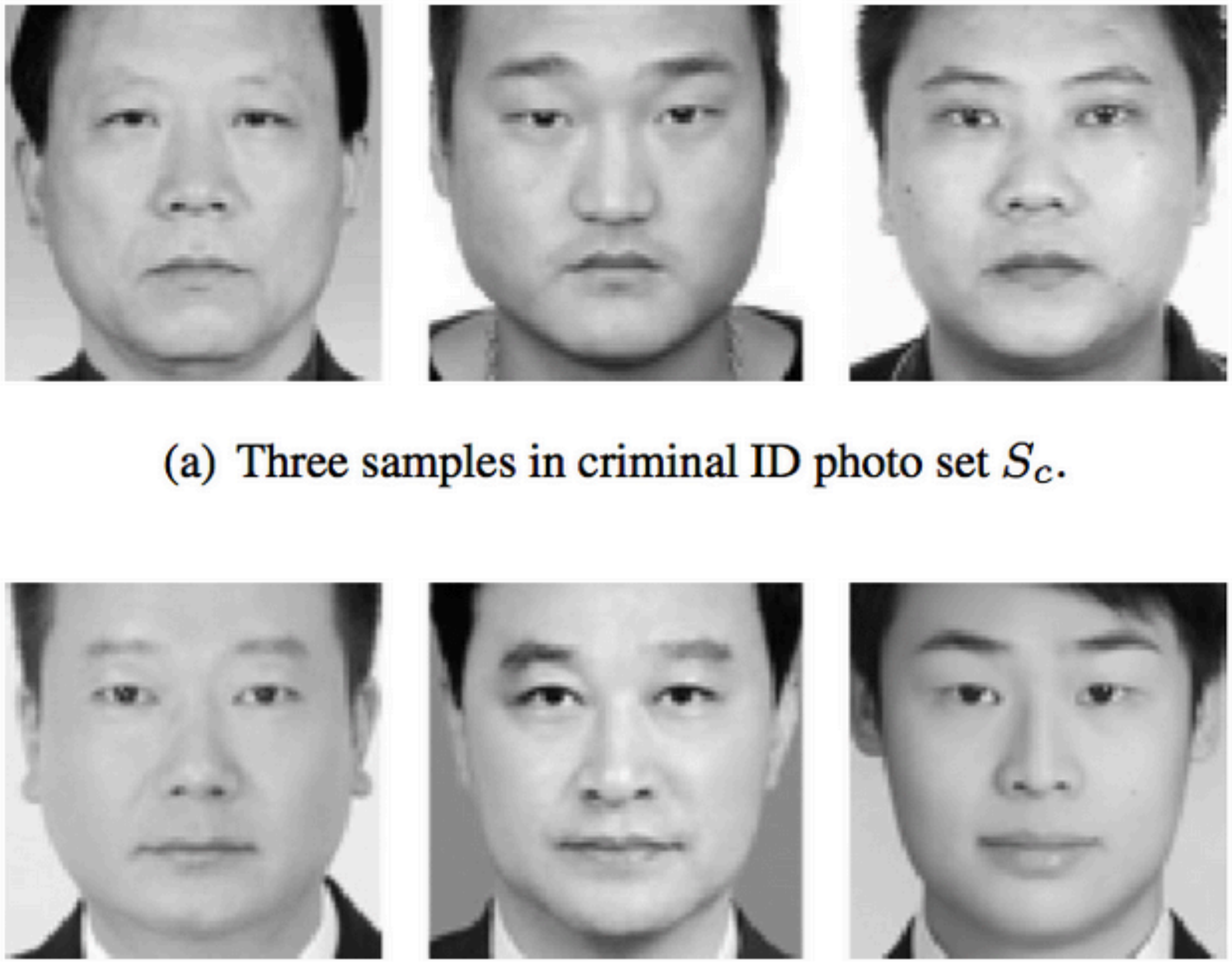
Facial recognition…

- Disproportionately impacts people of color and other minority and vulnerable populations.
  - Disproportionate policing of non-white communities and people
- Shifting the ideal from “presumed innocent” to “people who have not been found guilty of a crime, yet.”
  - Suspicionless inclusion in surveillance data
- Facilitation of harassment and violence.
  - It’s not only the “good guys” who can use it
- Risk of arbitrary government tracking of one’s movements, habits, relationships, interests, and thoughts.
  - If you have surveillance data, there is a temptation to use it.
- The suffocating restraint of the relentless, perfect enforcement of law.

Other issues

- Who will use it and why?
- What are people (like you) willing to give up to feel safer or more in control?
- Yes, there is a slippery slope (first they came for the terrorists…)

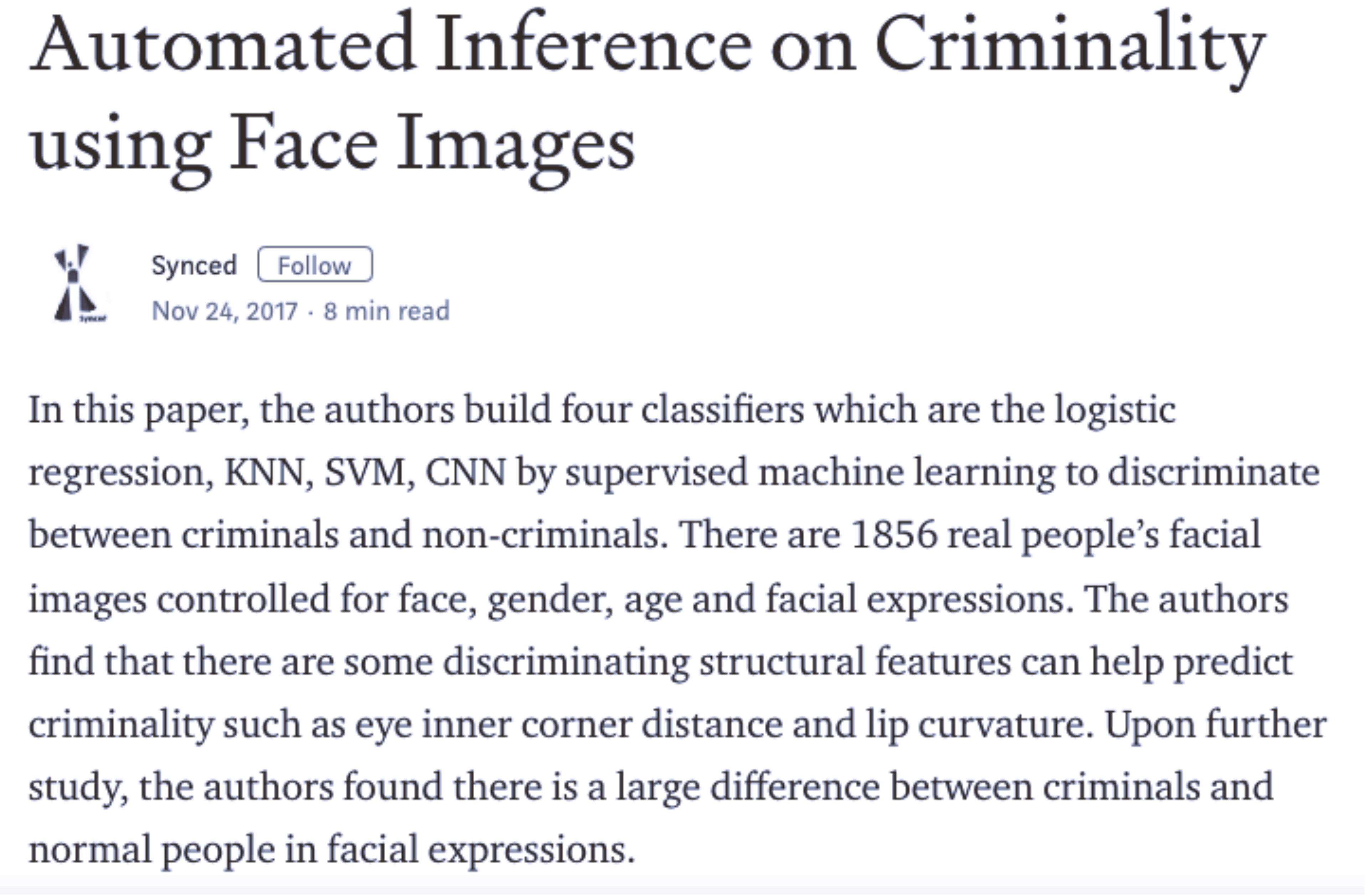
Facial recognition in practice



(a) Three samples in criminal ID photo set S_c.

(b) Three samples in non-criminal ID photo set S_n

Figure 1. Sample ID photos in our data set.

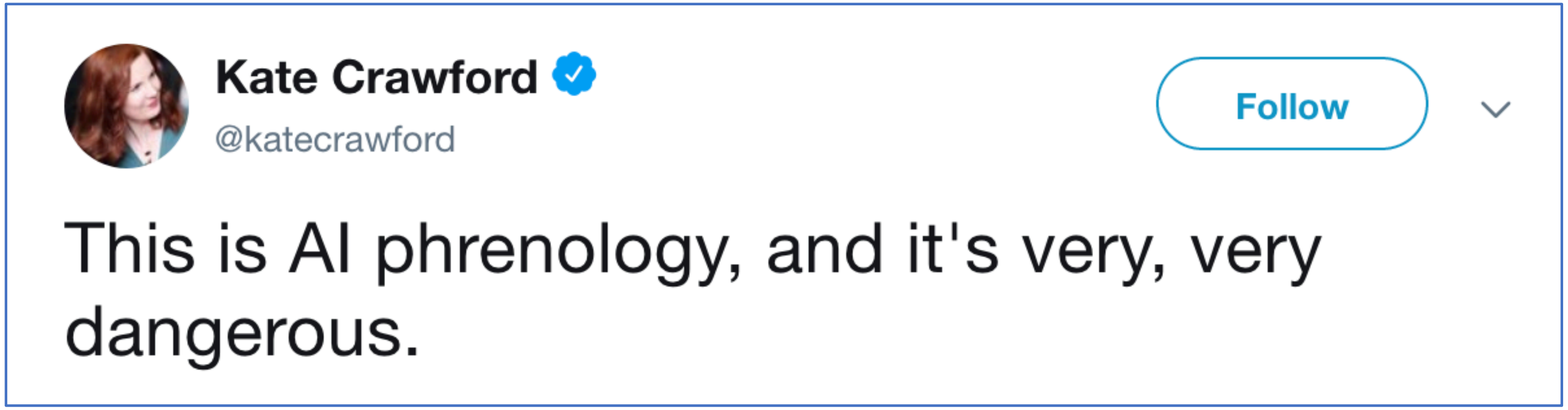


Automated Inference on Criminality using Face Images

Synced Follow

Nov 24, 2017 · 8 min read

In this paper, the authors build four classifiers which are the logistic regression, KNN, SVM, CNN by supervised machine learning to discriminate between criminals and non-criminals. There are 1856 real people's facial images controlled for face, gender, age and facial expressions. The authors find that there are some discriminating structural features can help predict criminality such as eye inner corner distance and lip curvature. Upon further study, the authors found there is a large difference between criminals and normal people in facial expressions.

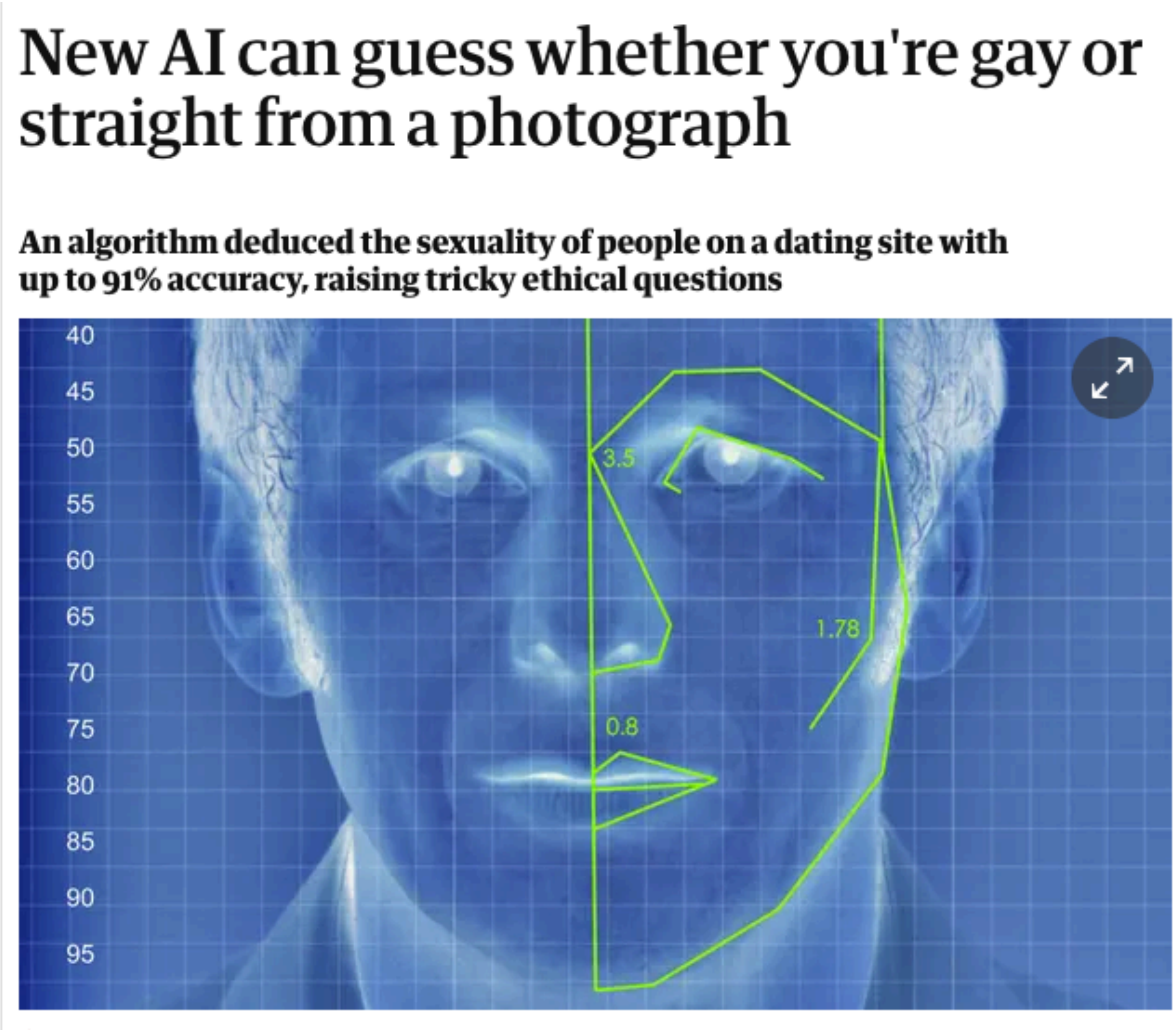


Kate Crawford ✓

@katecrawford

This is AI phrenology, and it's very, very dangerous.

- What are the risks? (what is phrenology?)
- What kinds of safety or insights are we trying to achieve?
- What if someone develops algorithms to detect other facets of a person using FR?



New AI can guess whether you're gay or straight from a photograph

An algorithm deduced the sexuality of people on a dating site with up to 91% accuracy, raising tricky ethical questions

More of the author’s arguments

- Faces are hard to hide or change. They can’t be encrypted, unlike a hard drive, email, or text message. A hacked database of faces…
- Existing name and face databases, such as for driver’s licenses, mugshots, and social media profiles. Further exploitation is easy to do when the data is already there.
- The infrastructure is already pervasive. Just add software. The data inputs (cameras) for facial recognition are widespread and in the field right now, namely with CCTV and officer-worn body cams.

- Tipping point creep. Not just “suspects” but all of us.
  - Any database of faces created to identify individuals arrested or caught on camera requires creating matching databases that, with a few lines of code, can be applied to analyze body cam or CCTV feeds in real time.
- Faces are central to our identity.
  - It’s easy to think people don’t have a strong privacy interest in faces because many of us routinely show them in public. Indeed, outside of areas where burkas are common, hiding our faces often prompts suspicion.

Regulation?

- Is going to be hard.
- Financial rewards will encourage entrepreneurialism that pushes facial recognition technology to its limits, and corporate lobbying will tilt heavily in this direction.
- Self regulation seems unlikely to be effective.
- Using “consent” seems a little lightweight.
    - If you consent to using faceid on your iPhone, it seems pretty minor, right?
    - Like with other privacy and surveillance tech, consent will typically be “take it or leave it”

INFO Policy, Law, and Ethics

A poster representing facial recognition at a security conference in Beijing, China, where authorities have aggressively invested in the controversial technology. // Thomas Peter/Reuters

The Tenants Fighting Back Against Facial Recognition Technology

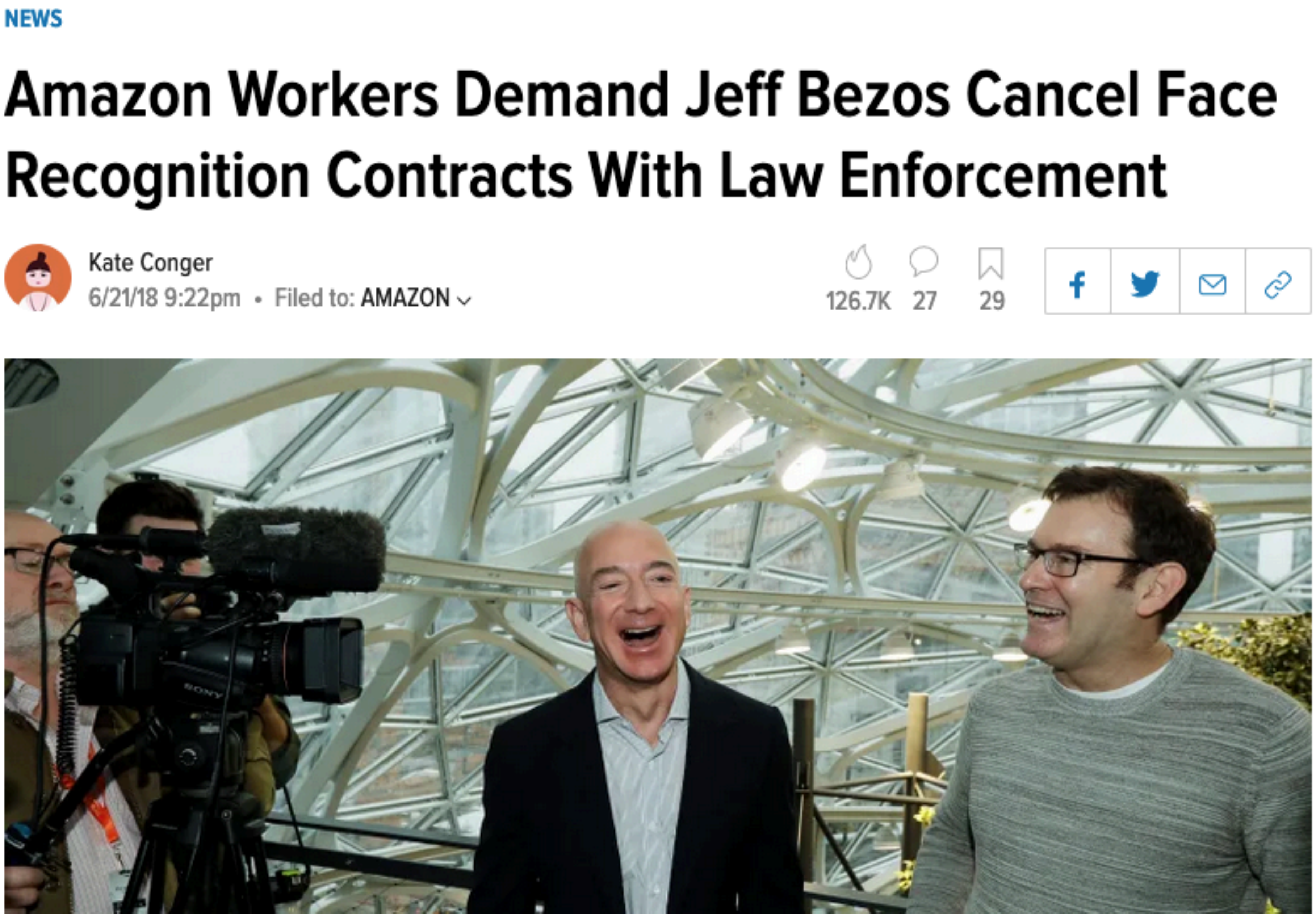
TANVI MISRA MAY 7, 2019

- Last year, residents of Atlantic Plaza Towers, **a rent-stabilized** apartment building in Brooklyn, found out that their landlord was planning to replace the key fob entry system with facial recognition technology. The goal, ostensibly, was to modernize the building’s security system.
- But some residents were immediately alarmed by the prospect: They felt the landlord’s promise of added security was murky at best, and didn’t outweigh their concerns about having to surrender sensitive biometric information to enter their own homes.
- Last week, lawyers representing 134 concerned residents of the building filed an objection with the state housing regulator. It is the first visible opposition in New York City to the deployment of such technology in the residential realm.

Washington State

- This year, the American Civil Liberties Union advocated for a bill in the Washington legislature to regulate facial recognition.
  - Opposed by industry (Amazon, Microsoft).
  - Ultimately died in committee.

- A *different* facial recognition bill was introduced and heavily lobbied by Microsoft.
  - ACLU said: “the bill sets up a permissive regime that will encourage face surveillance to be acquired by law enforcement without any meaningful discussion of the proper place for this technology in our democracy. This provision allows use of face surveillance by law enforcement with a warrant, and allows warrantless use under some circumstances as well.”

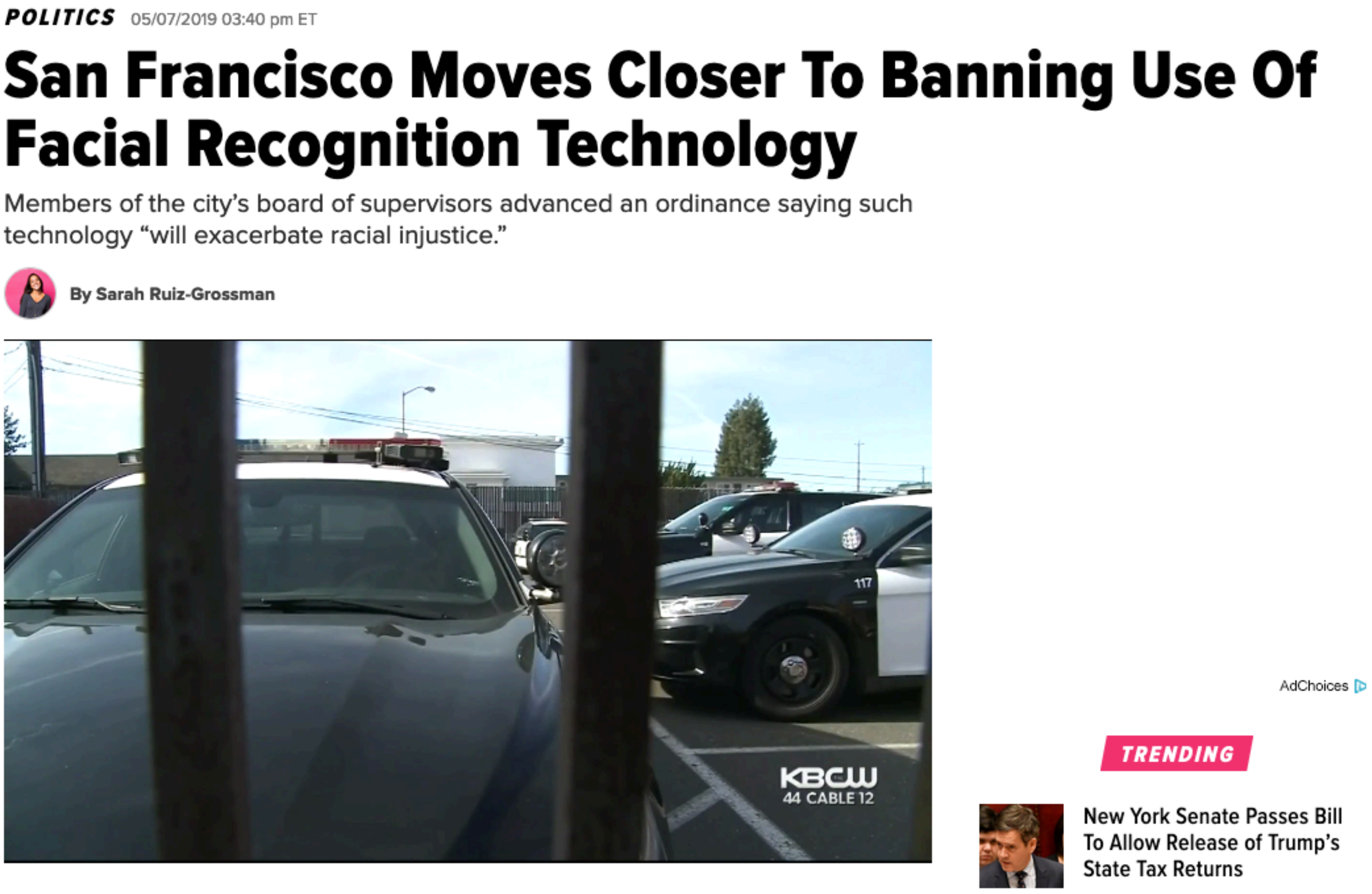


NEWS

Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts With Law Enforcement

Kate Conger

6/21/18 9:22pm • Filed to: AMAZON



POLITICS 05/07/2019 03:40 pm ET

San Francisco Moves Closer To Banning Use Of Facial Recognition Technology

Members of the city’s board of supervisors advanced an ordinance saying such technology “will exacerbate racial injustice.”

By Sarah Ruiz-Grossman

TRENDING

New York Senate Passes Bill To Allow Release of Trump’s State Tax Returns

https://www.huffpost.com/entry/san-francisco-ban-facial-recognition_n_5cd1d01ce4b0e4d757395587?guccounter=1