



FG2020

# Is FG Enabling a Surveillance Dystopia?



**Matthew Turk**

Toyota Technological Institute at Chicago

<http://www.ttic.edu/mturk>

# Informal survey questions

---

## 1. Is facial recognition technology biased?

- Yes
- No
- Unsure

## 2. What permissions should researchers secure in order to use images with people's faces for research, training, and testing?

- Freely use any publicly available images
- Freely use any images permitted by their terms or licenses
- Informed consent from all people in images
- Other or unsure

## 3. Is it ethical to undertake facial recognition research that may be later used to enable FR systems that are used unethically?

- Yes
- No
- Unsure

## 4. Do you consider a CNN-based deep network for face recognition from a single photo to perform a “scan of face geometry”?

- Yes
- No
- Unsure

## 4. Are you generally comfortable with FR systems, if they are highly accurate and unbiased, used in these ways? (Check all for which your answer is "yes.")

- Criminal law enforcement
- Airport and/or border security
- Tracking employee and visitor identities at places of employment
- Tracking customer identities at retail stores
- Tracking student, employee, and visitor identities at public schools

# Report from The Brookings Institution's Artificial Intelligence and Emerging Technology (AIET) Initiative

August 20, 2020

**BROOKINGS** AI · TRANSITION 2021 · CITIES & REGIONS · GLOBAL DEV · INTL AFFAIRS · U.S. ECONOMY · U.S. POLITICS & GOVT · MORE

SERIES: AI Governance

**REPORT**  
**Who thought it was a good idea to have facial recognition software?**  
Mark MacCarthy · Thursday, August 20, 2020

f t in v ...

For media inquiries, contact:  
Governance Studies  
Main Line  
202.797.6090

*Editor's Note: This report from The Brookings Institution's Artificial Intelligence and Emerging Technology (AIET) Initiative is part of "AI Governance," a series that identifies key governance and norm issues related to AI and proposes policy remedies to address the complex challenges associated with emerging technologies.*

**R**ecounting her experiences working with Barak Obama as a candidate and as president, [Alyssa Mastromonaco](#) says he would often challenge his staff with the question, "Uh, who thought this was a good idea?" It was an attempt to ensure his advisers took personal responsibility for the recommendations they made, especially when things went wrong.

It's about time someone asked that question about facial recognition software. It would oblige the developers and users of the technology to explain exactly why they think it's a good idea to create something with that level of power.

 **Mark MacCarthy**  
Adjunct Faculty - Communication, Culture, and Technology - Georgetown University  
[Mark\\_MacCarthy](#)

# Why automatic facial recognition?

---

- Increased safety at airports, public venues and spaces, private buildings
- Counter terrorism
- Reduction of theft and fraud
- Convictions of criminals
- Acquit wrongly accused persons
- Locating missing people
- Healthcare applications – diagnostic, monitoring, compliance
- Non-touch, frictionless access and login
- Photo indexing and tagging
- Aid for visually impaired people
- Etc., etc.
- New York City Police Department
  - Adopted in 2011
  - Led to 1000 arrests in 2018
  - Arrests in murders, robberies, assaults, etc.
  - Aided in identifying victims
  - Has cleared many suspects

# Why automatic facial recognition?

## Early days of FR research

- Canonical example of computer vision and object recognition
- Understanding human perception
- Visual neuroscience
  - Face-selective cells
  - Prosopagnosia
- AI challenge
  - “Computers can’t recognize a face”
- Curiosity!

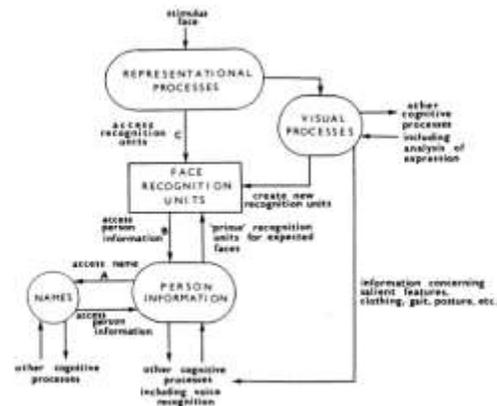
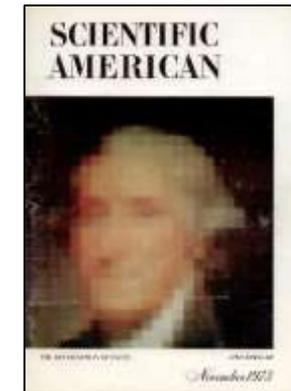
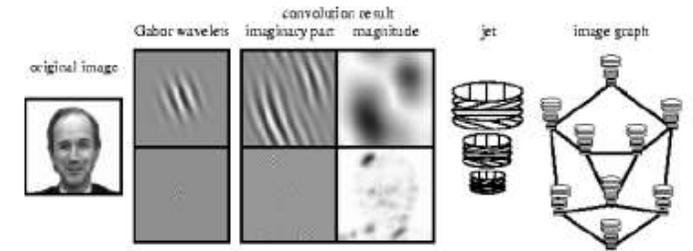
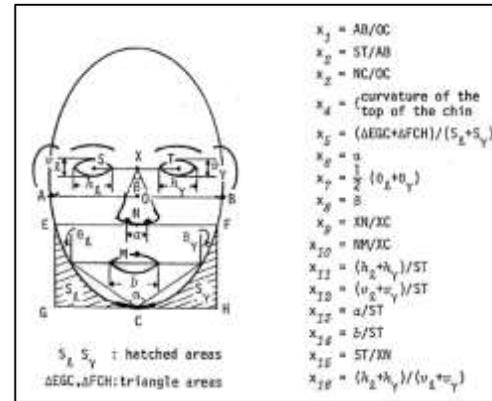
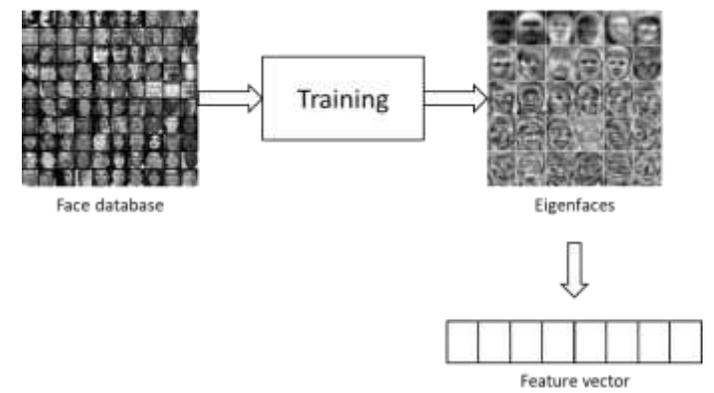
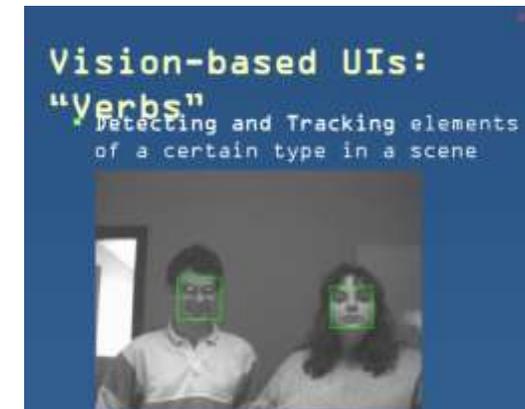


Figure 1. Hay & Young's (1982) model of the functional components involved in face recognition. (reproduced with permission).



# Why automatic facial recognition?

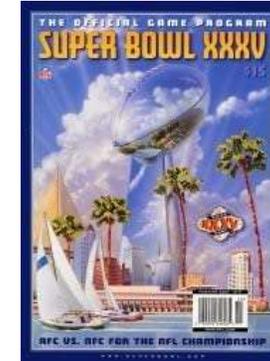
- Early days of FR products (1990s)
  - Viisage
  - Visionics
  - Identix
  - Miros
  - Etc.
- Hoping for markets to emerge for FRT products



# Why automatic facial recognition?

---

- January 2001 Snooper Bowl
  - Super Bowl XXXV in Tampa, FL
  - Large FRT experiment *without public knowledge*
    - Viisage & partners – based on Eigenfaces
  - Out of ~70,000 people entering the stadium, the system identified 19 people thought to be subjects of outstanding warrants
    - All petty criminals – none were arrested
  - Prompted a backlash
- Viisage CEO Thomas Colatosti: “The great advantage of face recognition is that it's impartial.”



# Why automatic facial recognition?

---

- After the 9/11 terrorist attacks, the U.S. government began significant investments into biometrics technologies – especially facial recognition.
- Focus on FBI-level surveillance and security
  - Soon police departments...
  - ...casinos
  - ...check cashing machines
  - ...retail surveillance
  - ...etc.



Surveillance video showing Mohammad Atta at an airport in Maine on the morning of 9/11

# Why automatic facial recognition?

- April 2013 Boston Marathon Bombings
  - Killed 3 people, wounded 264
- The FBI released images and videos of the two suspects to the public
  - Subsequently killed an MIT police officer
- Use of FR failed even though both suspects had photos in official government databases.
- Widely viewed by the media as a failure for automated facial recognition; but people also clearly saw the possibilities.

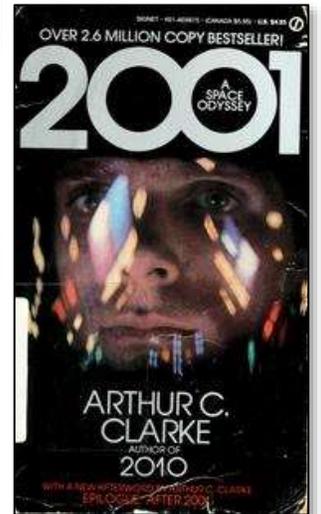
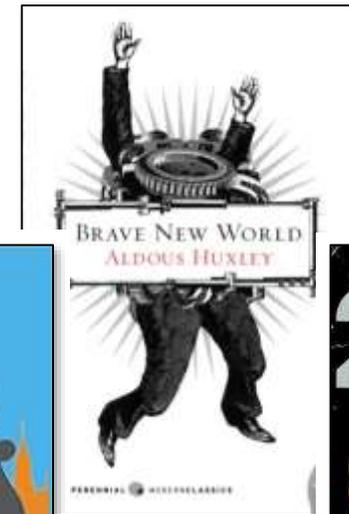
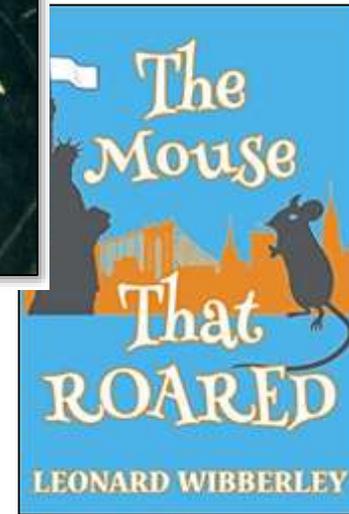
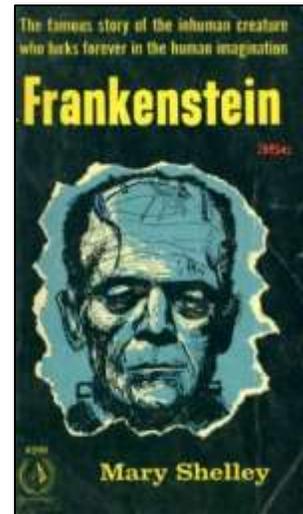




# Science policy, humanities, and ethics perspectives

- There has long been robust discussion in academia among scholars in public policy, humanities, and ethics about the role of science and technology in society, in areas such as:

- Nuclear weapons
- Chemical weapons
- Biological weapons
- Cloning
- Stem cells
- Eugenics
- Bias in medical research and practice
- Etc.



- What are the responsibilities of individuals, companies, governments, society?

# General environment of mistrust about computing technology

---

- Many recent well-known ethical issues and debates related to computing:
  - Major data breaches over the past 15 years – security and privacy
  - Unemployment due to technology (e.g., self-driving trucks)
  - Inequality – how is the wealth distributed that is created by IT?
  - Hazardous online behavior (bullying, etc.)
  - Biased search results, mortgage lending, recruiting tools, criminal prediction systems
  - Cambridge Analytica scandal
  - Self-driving car fatalities
  - Voting machine allegations
  - Etc., etc....
- Many studies find **declining trust** around the world and across technology sectors
  - Also declining trust in government, police, news media, and other institutions





# Error and bias in facial recognition systems

---

- July 2015 – Google apologizes for a flaw in Google Photos that led the new application to mistakenly label photos of some black people as “gorillas.”
- May 2016 – Israeli company Faception claims to accurately score facial images using personality types like “academic researcher,” “brand promoter,” “terrorist” and “pedophile.”
- Oct 2017 – “Gaydar” article: Stanford researchers Chen and Kosinski, “Deep neural networks are more accurate than humans at detecting sexual orientation from facial images.”
- Feb 2018 – Gender Shades paper showed disparate performance in commercial FRT systems across classes of gender and skin color in the task of gender classification – “intersectional accuracy disparities.”
- May 2020 – Harrisburg University researchers claim their FRT is able to predict if someone is a likely to be a criminal with 80% accuracy and with no racial bias.

## Gender Shades audit, 2018

Accuracy in gender classification

	Darker Male	Darker Female	Lighter Male	Lighter Female	Largest Gap
IBM	88.0%	65.3%	99.7%	92.9%	34.4%
Megvii	99.3%	65.5%	99.2%	94.0%	33.8%
Face++					
Microsoft	94.0%	79.2%	100.0%	98.3%	20.8%

## Actionable Auditing audit, 2019

Accuracy in gender classification

	Darker Male	Darker Female	Lighter Male	Lighter Female	Largest Gap
Amazon	98.7%	68.6%	100.0%	92.9%	31.4%
Kairos	98.7%	77.5%	100.0%	93.6%	22.5%
IBM	99.4%	83.0%	99.7%	97.6%	16.7%
Face++	98.7%	95.9%	99.5%	99.0%	3.6%
Megvii					
Microsoft	99.7%	98.5%	100.0%	99.7%	1.5%

# Error and bias in facial recognition systems (cont.)

---

- Jul 2018 – The ACLU used Amazon Rekognition to compare photos of U.S. lawmakers to a database of 25,000 mug shots. 28 member of Congress were incorrectly matched with people who had been arrested (5% error rate).
- NIST FRVT Part 3: Demographic Effects – analysis of demographic effects (sex, age, race) showing bias in FR systems.
  - “Reporting of demographic effects often has been incomplete in academic papers and in media coverage.”
- Jun 2020 – The first known account of an American being wrongfully arrested based on a flawed match from a facial recognition algorithm (Robert Julian-Borchak Williams, Detroit area).
- July 2020 – Second case of a man (in Detroit) wrongfully arrested after being misidentified by FR technology (Michael Oliver).



Robert Julian-Borchak Williams

Accused of shoplifting and arrested on the basis of flawed police work that relied on faulty facial recognition technology.

Blamed on flawed technology and poor police work.



Michael Oliver

Wrongfully arrested after being misidentified by FR technology.

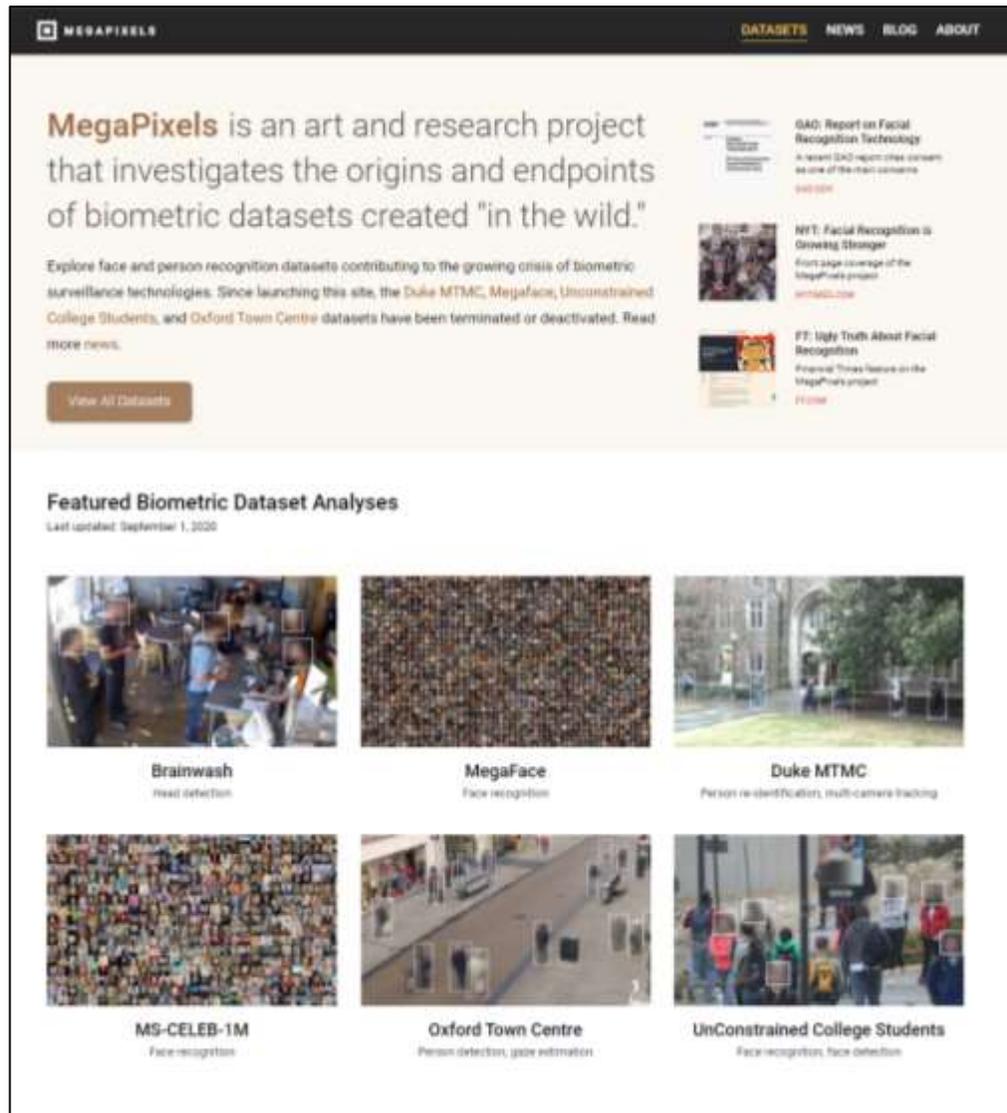
Police chief James Craig blamed poor investigative work

# Datasets and FR systems decommissioned

---

- Jun 2020 – Amazon, Microsoft, and IBM announce pauses or halts on their development or marketing of FRT
- Jul 2020 – New York lawmakers passed a moratorium on the use of Aegis, a facial recognition system, in schools until 2022.
- Aug 2020 – UK Court of Appeal temporarily halts the use of a FRT used by South Wales Police.
- Past year or two – Various face-related databases taken out of commission
  - MS-Celeb
  - Brainwash
  - Megaface
  - Unconstrained College Students
  - Diversity in Faces

<https://megapixels.cc/>



**MegaPixels** is an art and research project that investigates the origins and endpoints of biometric datasets created "in the wild."

Explore face and person recognition datasets contributing to the growing crisis of biometric surveillance technologies. Since launching this site, the [Duke MTMC](#), [MegaFace](#), [Unconstrained College Students](#), and [Oxford Town Centre](#) datasets have been terminated or deactivated. [Read more news.](#)

[View All Datasets](#)

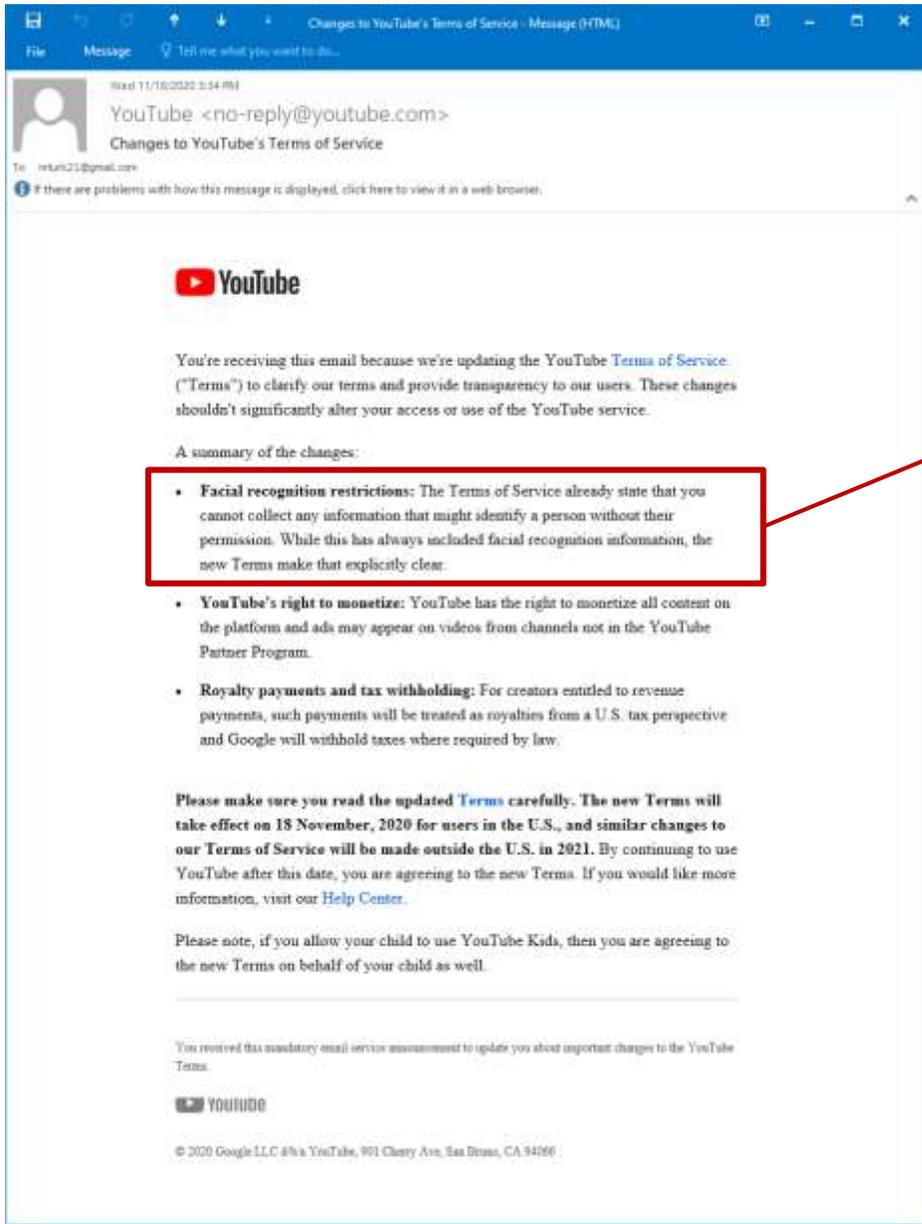
### Featured Biometric Dataset Analyses

Last updated: September 1, 2020

- Brainwash**  
Head detection
- MegaFace**  
Face recognition
- Duke MTMC**  
Person re-identification, multi-camera tracking
- MS-CELEB-1M**  
Face recognition
- Oxford Town Centre**  
Person detector, gaze estimator
- UnConstrained College Students**  
Face recognition, face detection

MegaPixels is an art and research project of Berlin artist Adam Harvey that investigates the origins and endpoints of biometric datasets created “in the wild.”

- Brainwash
- Clifton
- Duke MTMC
- MegaFace
- MrSub
- MS-CELEB-1M
- Oxford Town Centre
- QMUL GRID
- UnConstrained College Students
- WILDTRACK



## Email from YouTube yesterday

- **Facial recognition restrictions:** The Terms of Service already state that you cannot collect any information that might identify a person without their permission. While this has always included facial recognition information, the new Terms make that explicitly clear.

# Recent company actions

---

- In early 2019, Google said they would not sell a face recognition product until the technology's potential for abuse is addressed
  - Recently suggested a temporary ban might be welcome
- In June 2020, IBM, Microsoft, and Amazon announced pauses or halts on their development or marketing of FRT
  - IBM “no longer offers general purpose IBM facial recognition or analysis software.” Will no longer provide facial recognition technology to police departments or for mass surveillance, racial profiling, violations of basic human rights and freedoms, etc. (Still working on it?)
  - Amazon – one-year moratorium on police use of Rekognition
  - Microsoft will not sell FRT to police departments in the U.S., at least until there is a federal law to regulate it.

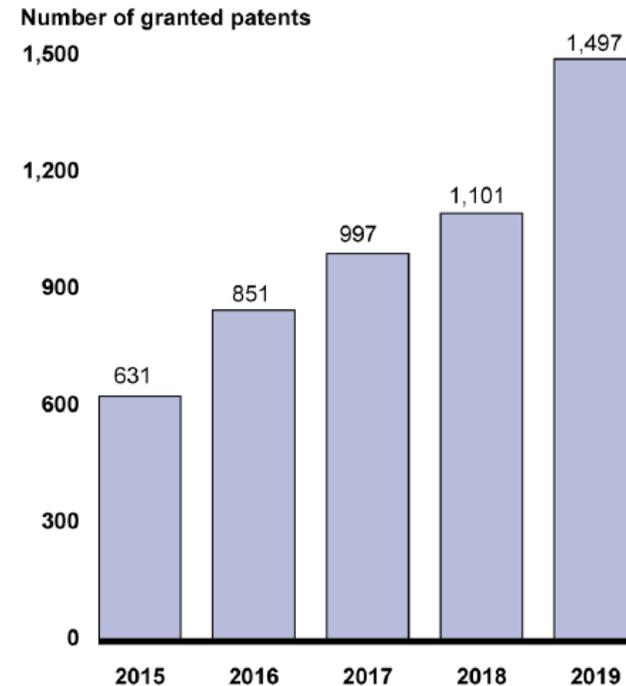
# Facial recognition technology companies

---

These are largely symbolic gestures, however!

- NEC
- Atos
- ImageWare Systems
- FaceFirst
- Securix
- Kairos
- Cognitec
- Megvii
- Cloudwalk
- SenseTime
- DERMALOG
- Clearview AI

Global facial recognition market size was **\$3.54B** in 2019, and it is expected to reach **\$10B** by 2025, at a CAGR of 18.84%.



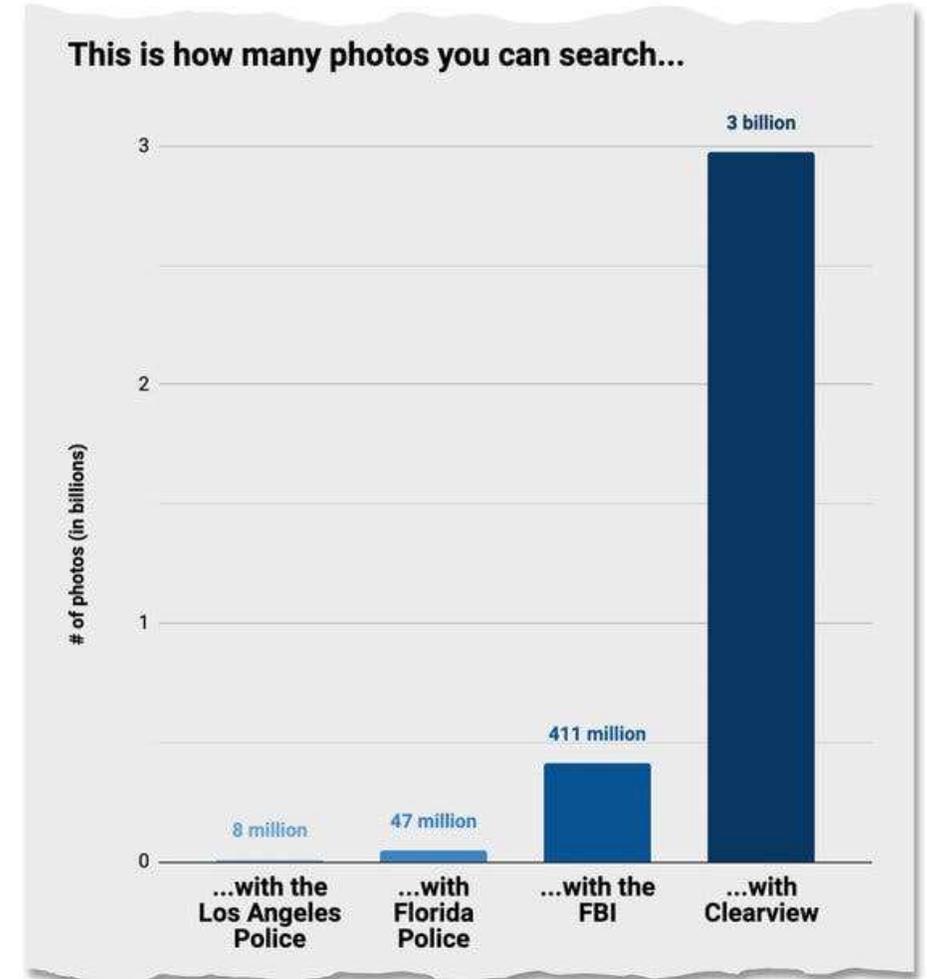
# Clearview AI

---

- In early 2020, reports began to surface about Clearview AI, a semi-stealth startup providing “search by face image” on huge amounts of public face data (~3B images scraped from many sources) – and concerns about weaponization.
  - NYT article: “The Secretive Company That Might End Privacy as We Know It”
- Jan – New Jersey Barred Police From Using Clearview Facial Recognition App
- Jan/Feb – Twitter, LinkedIn, YouTube send Clearview AI cease-and-desist letters
- Feb – Clearview AI’s entire client list was stolen in a data breach.
- Mar – Article about how investors and clients of Clearview AI used their system as a “secret plaything of the rich” - employing it personally on dates, at parties, to spy on the public.
- Apr – Clearview AI announces they will stop selling FRT to private companies

# Clearview AI

- Startup providing “search by face image”
- Database: ~3 billion images scraped from public sources
- David Scalzo (early investor):  
“I’ve come to the conclusion that because information constantly increases, there’s never going to be privacy. Laws have to determine what’s legal, but you can’t ban technology. Sure, that might lead to a dystopian future or something, but you can’t ban it.”
- *People can be identified and correlated with their data at a speed and scale previously unseen.*



# Reports on China's growing surveillance state

---

- For the last couple years, there have been many reports on China's use of facial recognition technologies to track and control citizens.
  - Especially ethnic minority groups like the 11M largely Muslim Uighurs on China's western frontier.
- And the increase in video surveillance in Chinese cities, claims of building a high-tech authoritarian surveillance state to identify and track 1.4B people.
- China has become the world's biggest market for security and surveillance technology.
- It already has the world's largest surveillance network; China deploys over half of all surveillance cameras in use around the world. [Forbes 11/2020]



# Reports on China's growing surveillance state

---

- China has a national database of individuals it has flagged for watching – suspected terrorists, criminals, drug traffickers, political activists and others – includes 20-30 million people.
- While many people in China are concerned about this, many seem to be happy about the physical security promised by the surveillance network.
- China has begun exporting this technology to nations that seek closer surveillance of their citizens, including Ecuador, Zimbabwe, Uzbekistan, Pakistan and the United Arab Emirates.



# Reports on China's growing surveillance state

---

There's some recent interesting pushback:

- On Oct 26, the eastern city of Hangzhou (near Shanghai) prohibited property owners from the mandatory use of biometrics in residential properties.
- First (known) regulations of this kind in China.
- Earlier this year, Baidu CEO Robin Li proposed a personal privacy protection bill to the annual plenary session of the People's Congress.



# Growing surveillance in India

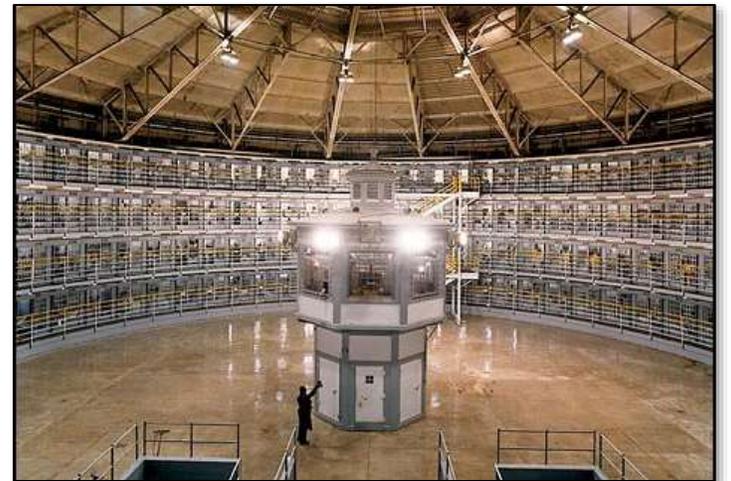
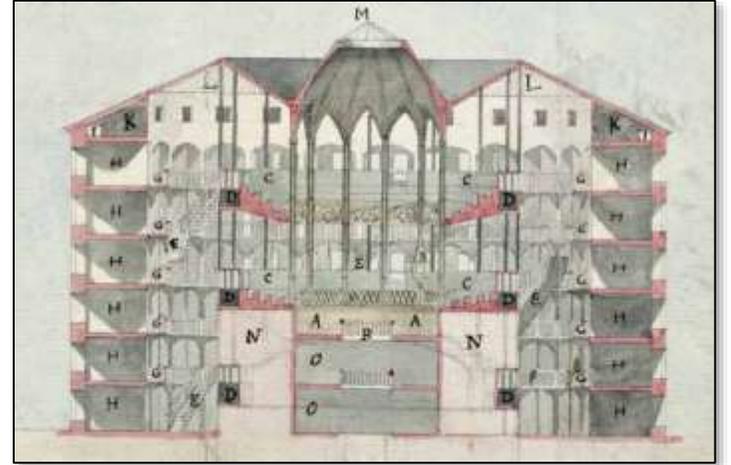
---

- India's surveillance state is on the rise as well
- Planning for the world's largest automatic facial recognition system in 2021.
- The Indian National Crime Records Bureau (NCRB) is preparing to install a nationwide facial recognition system, the Automated Facial Recognition System (AFRS)
- Desire to help remedy current "under-policed" situation in the country.



# Panopticon

- Introduced ~1785 by English philosopher Jeremy Bentham, from the Greek *panoptes* (“all seeing”)
- An design for an institutional building and system of control, allowing all prisoners of an institution to be observed by a single security guard in a central tower, without the inmates being able to tell if they are being watched.
  - The guard was to be observed by the general public and public officials.
- Bentham also thought that the prison design could be used for factories, asylums, hospitals, and schools.
- Many have considered this mechanism of surveillance as a tool of oppression and social control.



# Panopticon

---

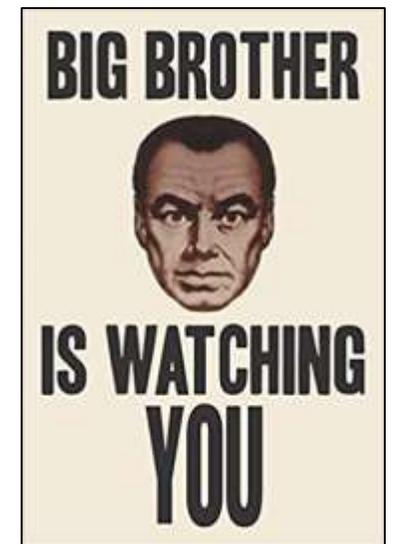
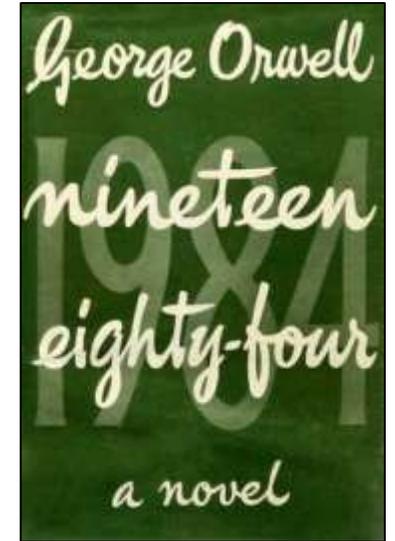
- London – a city with a history of terrorist attacks – has for a long time been considered the #1 surveillance city in the world
  - CCTV cameras on lampposts, buildings, train stations, and on main roads throughout the city.
  - According to civil rights group Liberty, on average a Londoner is captured on camera about 300 times daily. \*
- “As a modern police force, I believe that we have a duty to use new technologies to keep people safe in London.” Nick Ephgrave, Asst. Police Commissioner
- But for many years, London surveillance was more about the threat than the reality.



# 1984 (George Orwell)

---

- Centers on the consequences of totalitarianism, mass surveillance, and repressive regimentation of persons and behaviors within society
- In Oceania, the upper and middle classes have very little true privacy. All of their houses and apartments are equipped with telescreens so that they may be watched or listened to at any time. Similar telescreens are found at workstations and in public places, along with hidden microphones.
- *“There was of course no way of knowing whether you were being watched at any given moment.... You had to live ... in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.”*



# Key concerns and fears about FRT

---

- FRT is biased and “racist”
  - Race, gender, age, etc., and intersectionalities
- Data privacy violations and consent issues
  - Loss of anonymity; lack of consent; ownership of your own data
- Deployed systems lack transparency
- Function creep; can be used in unauthorized, inappropriate, and nefarious ways
- Permanence: can’t be reset or undone
- Can be weaponized against particular people and communities
- Can enable a dangerous, repressive surveillance state
  - Psychological impacts of being watched
- Can have a chilling effect on free speech and expression
- It feels creepy

# nature

18 November 2020

nature Search Login

[Explore our content](#) [Journal information](#) [Subscribe](#)

---

EDITORIAL · 18 NOVEMBER 2020

## Facial-recognition research needs an ethical reckoning

The fields of computer science and artificial intelligence are struggling with the ethical challenges of biometrics. Researchers, funders and institutions must respond.

[Twitter](#) [Facebook](#) [Email](#)



Over the past 18 months, a number of universities and companies have been removing online data sets containing thousands – or even millions – of photographs of faces used to improve facial-recognition algorithms.

In most cases, researchers scraped these images from the Internet. The pictures are classified as public data, and their collection didn't seem to alarm institutional review boards (IRBs) and other research-ethics bodies. But none of the people in the photos had been asked for permission, and some were unhappy about the way their faces had been used.

## Features

News Feature | 18 November 2020

### Is facial recognition too biased to be let loose?

The technology is improving — but the bigger issue is how it's used.

Davide Castelvecchi

News Feature | 18 November 2020

### Resisting the rise of facial recognition

Growing use of surveillance technology has prompted calls for bans and stricter regulation.

Antoaneta Roussi

News Feature | 18 November 2020

### The ethical questions that haunt facial-recognition research

Journals and researchers are under fire for controversial studies using this technology. And a *Nature* survey reveals that many researchers in this field think there is a problem.

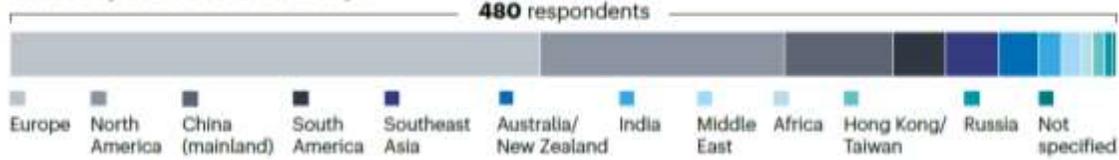
Richard Van Noorden

*Nature* asked 480 researchers around the world who work in facial recognition, computer vision, and AI for their views on thorny ethical questions about facial-recognition research.

# FACIAL RECOGNITION: A SURVEY ON ETHICS

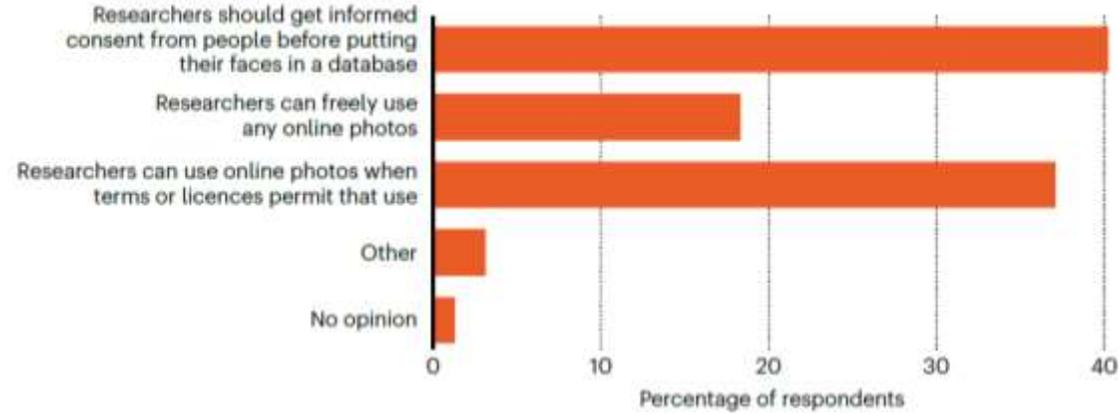
Nature surveyed\* nearly 500 researchers who work in facial recognition, computer vision and artificial intelligence about ethical issues relating to facial-recognition research. They are split on whether certain types of this research are ethically problematic and what should be done about concerns.

## Who responded to the survey?



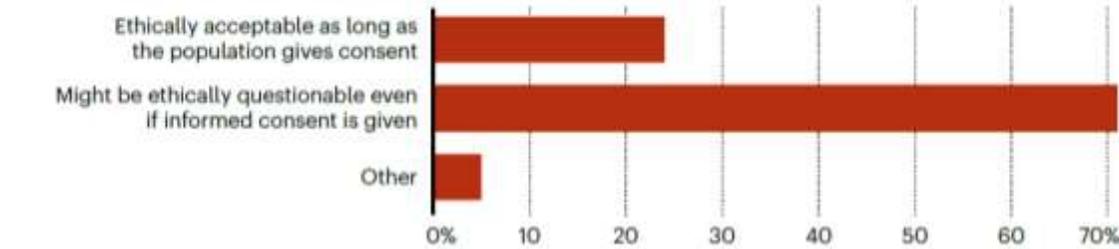
## Restrictions on image use

**Question:** Researchers use large data sets of images of people's faces — often scraped from the Internet — to train and test facial-recognition algorithms. What kind of permissions do researchers need to use such images?



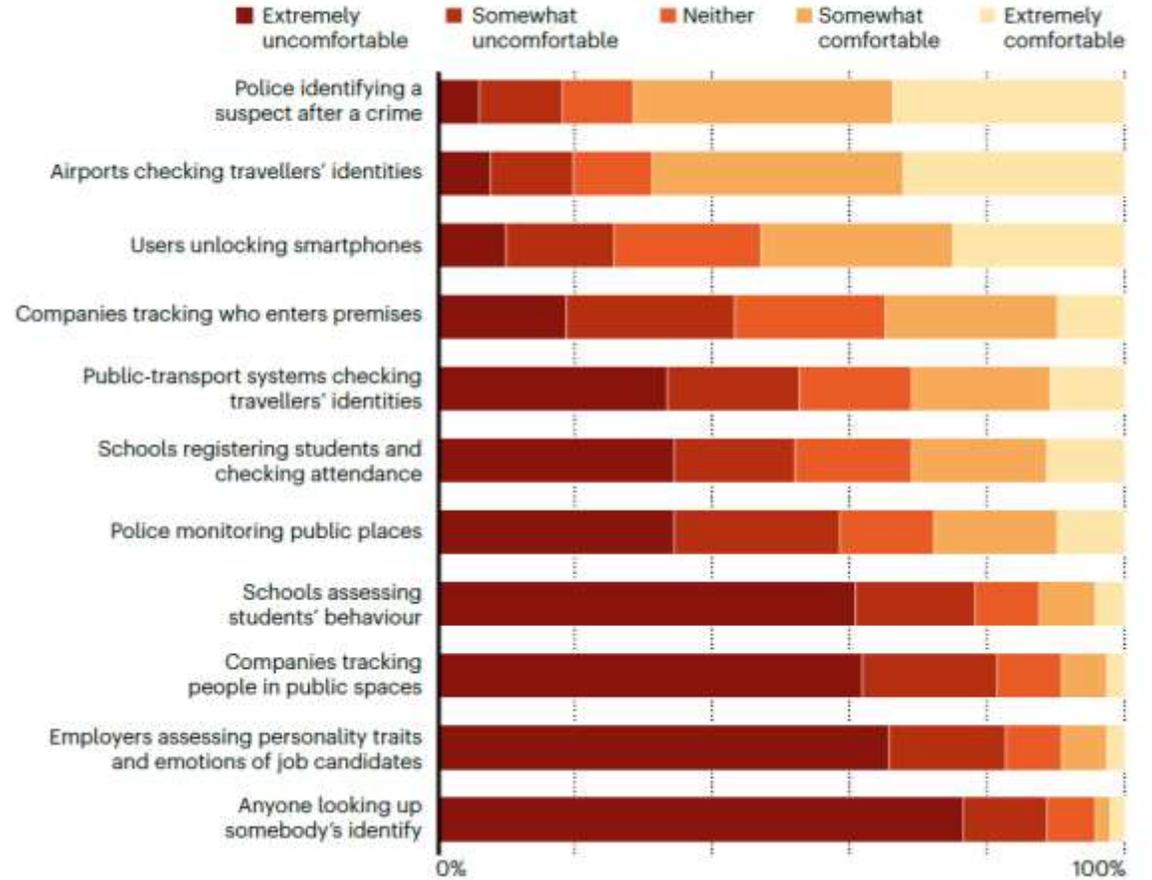
## Restrictions related to vulnerable populations

**Question:** Is it ethical to do facial-recognition research on vulnerable populations that might not be able to freely give informed consent, such as the Muslim population in western China?



## Attitudes on different uses

**Question:** How comfortable are you with facial-recognition technology being used in the following ways?



# Legal perspectives

 **NCSL** NATIONAL CONFERENCE OF STATE LEGISLATURES



**Spotlight | Facial Recognition Gaining Measured Acceptance**

By Pam Greenberg | Sept. 18, 2020 | [State Legislatures Magazine](#)

Authority to legislate?

Local, regional, national, international?

**Facial Recognition Is Here But We Have No Laws**



By SAM BUPONT / JULY 6, 2020

Without legal safeguards, this technology will undermine democratic values and fundamental rights.

**Nextgov**

**WIRED**

**Facial Recognition Laws Are (Literally) All Over the Map**

From Portland to Plano, local governments are placing different limits on the use of biometric data. That's a good thing.



Government, police, companies, individuals, use cases, public/private spaces?

Regulate, ban, moratorium, penalties?

# Broader data privacy legislation

---

- EU – General Data Protection Regulation (2016)
  - To give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
- U.S. – No comprehensive information privacy law
- California Consumer Privacy Act (2018)
  - Gives consumers more control over the personal information that businesses collect about them. Right to know, to delete, to opt-out, to non-discrimination.
- Various U.S. government and industry guidelines...

# FRT legislation in the U.S. – city, state

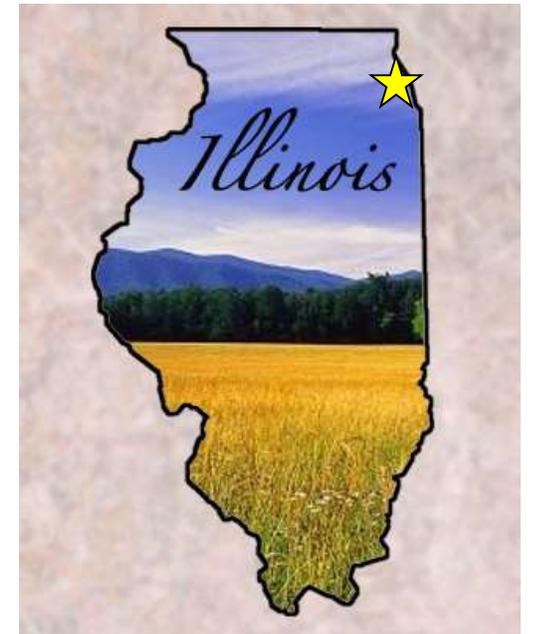
---

- City bans (mostly for police and city government)
  - San Francisco, Oakland, Berkeley, Alameda (CA)
  - Springfield, Cambridge, Northampton, Brookline, Somerville, Boston (MA)
  - Portland (OR), Portland (ME), Jackson (MI)
  - Perhaps more, certainly others in the works
  - Other legislation has passed requiring informed consent, regulating funding, etc.
- State legislation
  - Biometric data: Illinois (2008), Texas (2009), Washington (2017)
    - WA is seen by many as a model – sets forth requirements for businesses who collect and use biometric identifiers for commercial purposes
  - New Hampshire, Oregon, California, Vermont (Oct)
    - Restrictions or bans on police use of FRT
  - Several states limit the police use of databases with driver's license photos in FRT

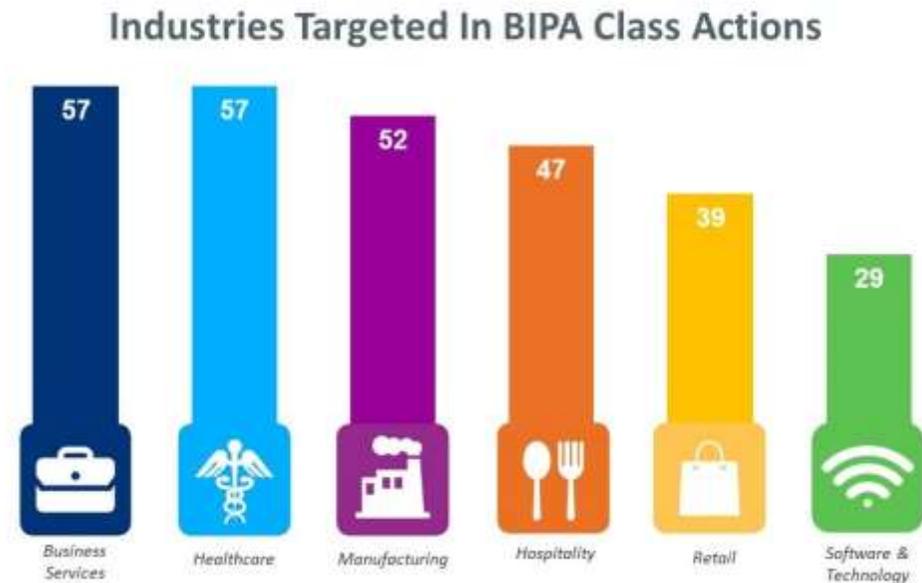
# Illinois Biometric Information Privacy Act (BIPA)

---

- Illinois was the first U.S. state to regulate the collection and storage of biometric information by businesses through its **Biometric Information Privacy Act (BIPA)**.
- The oldest and strongest biometric privacy law in the country
  - Covers biometrics of retina, iris, fingerprint, voice, hand, and face
- Requires companies doing business in Illinois to comply with several requirements, including user consent and secure storage of biometric identifiers
- Individuals do not have to demonstrate actual “harm” to establish being “aggrieved” under BIPA.



# Illinois Biometric Information Privacy Act (BIPA)



Recent BIPA cases brought against Microsoft, Amazon, Google, Clearview AI, & Apple

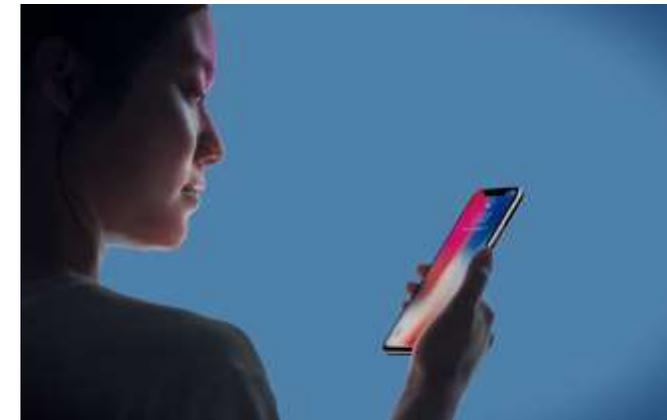
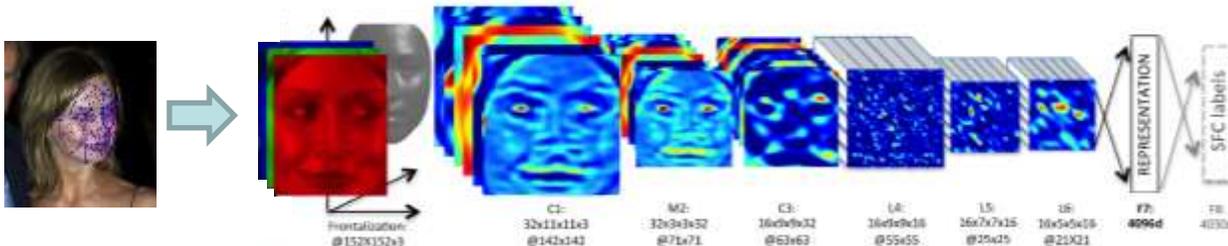
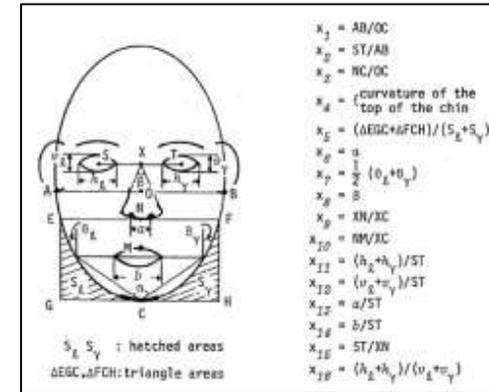
- Some related to IBM's "Diversity in Faces" database.

Not just tech companies, but users:

- Del Monte Foods, Southwest Airlines, Sky Chefs, Bimbo Bakeries, UChicago Medical Center, Jackson Park Supportive Living Facility, Six Flags Entertainment, Twin City Fire Insurance Co., Peri Formwork Systems Inc., Lathem Time Co., Trump International Hotel Chicago....

# Illinois Biometric Information Privacy Act (BIPA)

- “Biometric information” = any information based on an individual’s biometric identifier used to identify an individual
- “Biometric identifier” = “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry”
- What is a “scan of face geometry”?
- Does my product “scan face geometry”?



# Facebook BIPA case

\$650M

Facebook will pay ~~\$550~~ million to settle class action lawsuit over privacy violations

Devlin Coldewey @techcrunch · 8:24 PM CST · January 26, 2020

Comment



Image Credits: Getty Images

Facebook will pay over half a billion dollars to settle a class action lawsuit that alleged systematic violation of an Illinois consumer privacy law. The settlement amount is large indeed, but a small fraction of the \$35 billion maximum the company could have faced.

## Facebook BIPA lawsuit

- Originally by individuals (2016), later converted into a class action suit (2018)
- For FB users in Illinois who appeared in a picture uploaded after June 7, 2011
- Settled in 2020 for \$550M, then increased to \$650M
- \$400-600 payment per person expected
- The deadline to file a claim is **Nov. 23 – Monday!**

# Facebook BIPA case

\$650M

## Facebook will pay ~~\$550~~ million to settle class action lawsuit over privacy violations

Devlin Coldewey @techcrunch · 8:24 PM CST · January 26, 2020

Comment

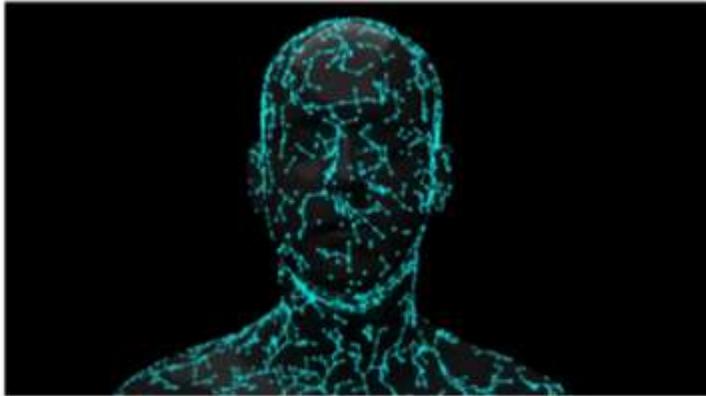


Image Credits: Getty Images

Facebook will pay over half a billion dollars to settle a class action lawsuit that alleged systematic violation of an Illinois consumer privacy law. The settlement amount is large indeed, but a small fraction of the \$35 billion maximum the company could have faced.

My email notice:

Official Notice from the United States District Court for the Northern District of California

[Español](#)

### Facebook users in Illinois may be entitled to payment if their face appeared in a picture on Facebook after June 7, 2011

Don't worry, you are not being sued. This is an official court notice, not an ad for a lawyer.

Facebook, Inc. has settled a class action that claimed Facebook violated Illinois law by collecting and storing biometric data of Facebook users in Illinois without the proper notice and consent, as part of its "Tag Suggestions" feature and other features involving facial recognition technology. Facebook denies it violated any law. You can fill out a short claim form and potentially get an estimated \$200 - \$400 by clicking below.

[Claim Now](#)

#### Am I A Class Member?

The Court decided that all people who fit this definition are included in the Class: "Facebook users located in Illinois for whom Facebook created and stored a face template after June 7, 2011." Facebook's records show that you are likely a class member.

To file a valid claim under the Settlement, you must have lived in the State of Illinois for a period of at least 183 days (6 months). Time spent traveling or taking a vacation outside of Illinois can be included in this time period and does not make you ineligible.

For more information, please visit [www.facebookbipaaction.com](http://www.facebookbipaaction.com).

#### What can I get?

If you believe you are a class member you can fill out a short claim form and potentially receive approximately \$200 to \$400 from a \$650 million Settlement Fund. The amount you receive may be less than or greater than this amount depending on the number of valid claims filed. This fund will also be used to pay the costs of notifying people about the settlement, the lawyers' fees, award payments to the users who helped bring the lawsuit, and certain taxes.

The Settlement also requires Facebook to turn "off" the Facial Recognition setting and delete face templates for most Class Members unless they turn it back "on."

# Facebook BIPA case

---

- How does facial recognition work? Neural networks? Deep learning? Viola-Jones face detection? Facial image alignment?
- Does FB's CNN-based approach rely on a 3D scan of a person's face?
- Does their face signature represent face geometry?
- Is the approach feature-based or holistic?
- Does their system rely on, or extract, facial landmarks or features (eyes, nose, mouth, chin, etc.)?
- Are "image features" directly related to "face features" (eyes, nose, mouth, etc.)?
- Could their face signature be used to reconstruct the face or steal someone's identity?

# FRT legislation in the U.S. – federal

---

Federal – some legislation has been introduced, and more is coming

- Senate

- Commercial Facial Recognition Privacy Act of 2019 (Mar 2019)
- Facial Recognition Technology Warrant Act of 2019 (Nov 2019)
- Ethical Use of Facial Recognition Act (Feb 2020)
- Facial Recognition and Biometric Technology Moratorium Act of 2020 (June 2020)
- National Biometric Information Privacy Act of 2020 (Aug 2020)

- House of Representatives

- Advancing Facial Recognition Act (May 2020)
- To prohibit Federal funding from being used for the purchase or use of facial recognition technology, and for other purposes (July 2019)
- FACE Protection Act of 2019 (July 2019)
- Stop Biometric Surveillance by Law Enforcement Act (June 2020)
- Facial Recognition and Biometric Technology Moratorium Act of 2020 (June 2020)

# Biden-Harris Administration

---

- What should we expect – for legislation and government funding?
- Biden has proposed investments that would benefit “key technologies” like 5G, artificial intelligence, advanced materials, biotechnology, and clean vehicles.
  - “Declines in federal R&D spending have contributed to a hollowing out of the American middle class.”
  - Proposed to increase the amount of federal R&D spending to \$300 billion over four years (from \$134B in 2020).
- Harris has previously called attention to potential problems using AI in the criminal justice system, concerned about misuse.



# Biden-Harris Administration

---

- Sept 2018: Sen. Harris wrote letters to the FBI, FTC, and EEOC about the biases and risks in facial recognition.
  - *“While they may offer benefits, we are concerned by the mounting evidence that these tools may perpetuate gender, racial, age, and other biases.”*
- Sept 2019: Plan to Transform the Criminal Justice System by then-candidate Harris
  - It is important to address racial disparities in technology used by law enforcement, including *“facial recognition and other surveillance.”*
- Dec 2019: Harris and two other senators called on HUD to review policies governing the use of facial recognition software in federally assisted housing.
  - *“[T]he expansion of facial recognition technology in federally assisted housing properties poses risks to marginalized communities, including by opening the door to unchecked government surveillance that could threaten civil rights.”*

# Biden-Harris Administration

---

General consensus seems to be:

- Good for science
- Good for R&D funding
- Increasing focus on regulation of AI-related technologies and firms

**What to expect from Biden-Harris on tech policy, platform regulation, and China**

Brookings Institution report:

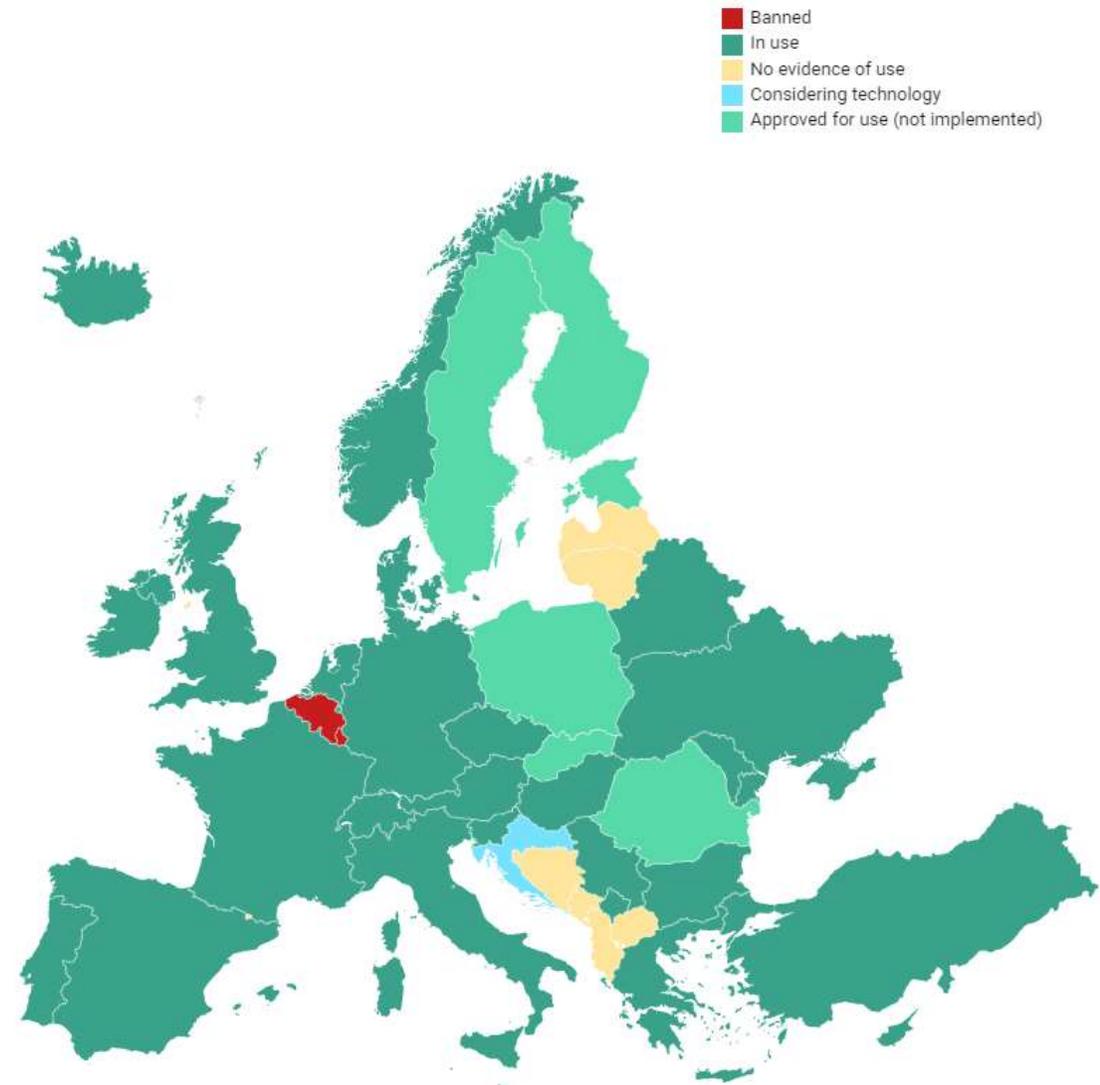
*In their efforts to address their past and current positions on criminal justice and policing, both Biden and Harris are more likely to support stronger guardrails on the use of facial recognition and other surveillance technologies, particularly among law enforcement and border security officials. Senator Harris may also address the technical flaws in the accurate identification of diverse populations in facial recognition.*

# FRT legislation in Europe

---

The EU is currently considering a 3-5 year ban on FRT in public spaces.

*(While not banned by law, Belgium found its use to be in breach of the law and Luxembourg prime minister spoke against it.)*



# FRT legislation in Europe

---



Wojciech Wiewiórowski

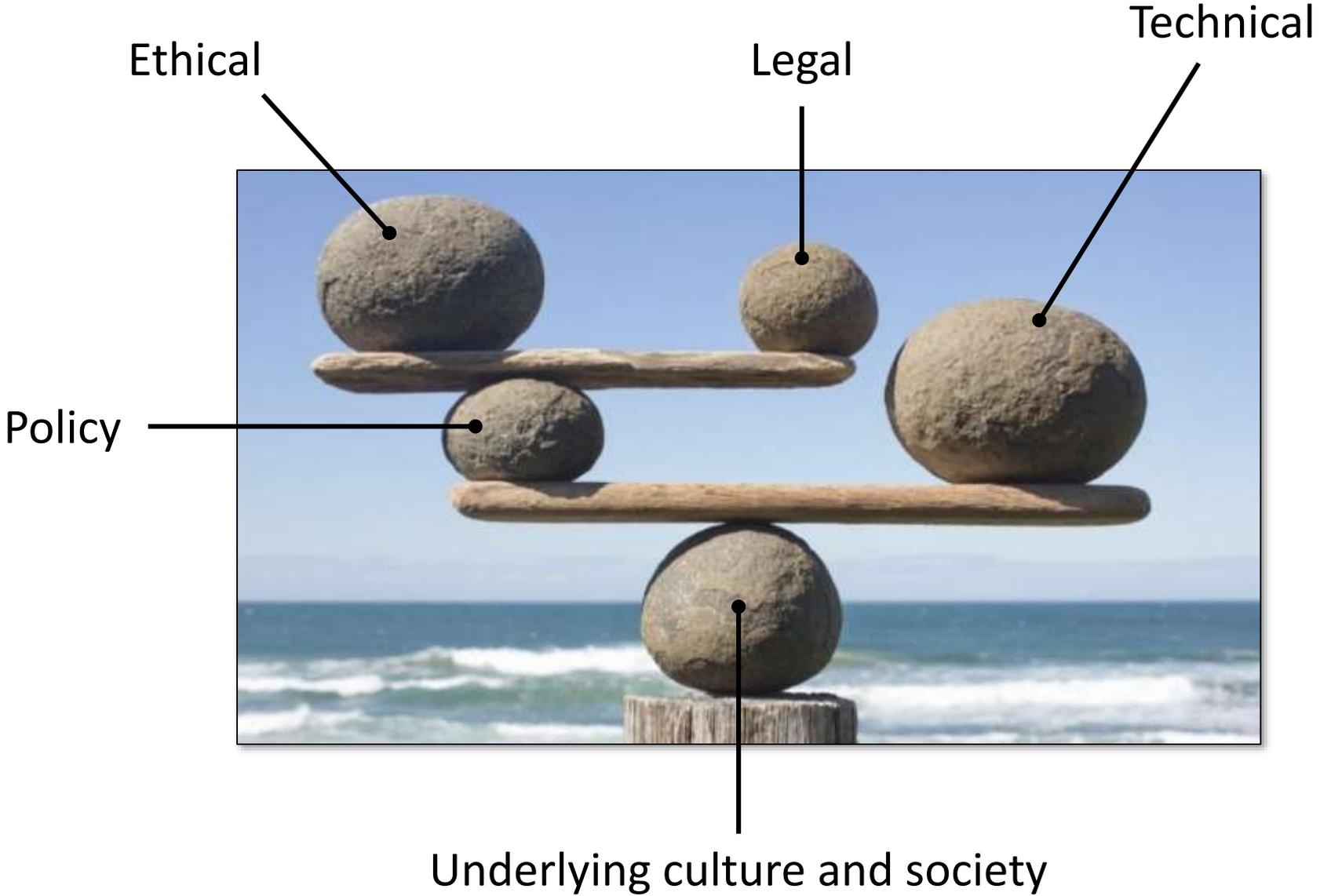
European Data Protection Supervisor

Speech to 2020 Biometrics Institute Congress, October 2020



*I fear we in our societies still lack the full picture of the individual and societal impact of automated recognition in public spaces of human features, not only of faces but also of gait, voice, and other biometric or behavioural signals. I therefore support the idea of a moratorium on their deployment, in the EU, so that an informed and democratic debate can take place.*

*For biometrics to thrive, it is vital to invest in public trust.*



# Advocacy and activism

---

***Advocacy:*** Activity by an individual or group that aims to influence policy decisions within political, economic, and social institutions.

***Activism:*** The practice of vigorous action or involvement as a means of achieving political or other goals.

Many groups have been attempting to raise awareness, build momentum, and create change with respect to facial recognition technologies

- Professional groups
- Industry groups
- Large companies
- Civil liberties groups
- Other lobbying groups

# ACM U.S. Technology Policy Committee (USTPC) Statement

---

## Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies [June 30, 2020]

- *The technology too often produces results demonstrating clear bias based on ethnic, racial, gender, and other human characteristics recognizable by computer systems.*
- *Such bias and its effects are scientifically and socially unacceptable.*
- *USTPC urges an immediate suspension of the current and future private and governmental use of FR technologies in all circumstances known or reasonably foreseeable to be prejudicial to established human and legal rights.*
- *Universal principles for the accurate and just use of FR technology, and for its principled regulation, must be developed without delay.*
- *Guiding principles regarding accuracy, transparency, governance, risk management, and accountability.*

# Companies

---

Microsoft on regulation of facial recognition:

- The law should specify that consumers consent to the use of facial recognition services when they enter premises or proceed to use online services that have this type of clear notice.
- Legislation should permit law enforcement agencies to use facial recognition to engage in ongoing surveillance of specified individuals in public spaces only when:
  - a court order has been obtained to permit the use of facial recognition services for this monitoring; or
  - where there is an emergency involving imminent danger or risk of death or serious physical injury to a person.

# Microsoft's facial recognition principles

---

- ***Fairness.*** We will work to develop and deploy facial recognition technology in a manner that strives to treat all people fairly.
- ***Transparency.*** We will document and clearly communicate the capabilities and limitations of facial recognition technology.
- ***Accountability.*** We will encourage and help our customers to deploy facial recognition technology in a manner that ensures an appropriate level of human control for uses that may affect people in consequential ways.
- ***Non-discrimination.*** We will prohibit in our terms of service the use of facial recognition technology to engage in unlawful discrimination.
- ***Notice and consent.*** We will encourage private sector customers to provide notice and secure consent for the deployment of facial recognition technology.
- ***Lawful surveillance.*** We will advocate for safeguards for people's democratic freedoms in law enforcement surveillance scenarios, and will not deploy facial recognition technology in scenarios that we believe will put these freedoms at risk.

# The Partnership on AI

---

Conducts research, organizes discussions, shares insights, provides thought leadership, consults with relevant third parties, responds to questions from the public and media, and creates educational material that advances the understanding of AI technologies including machine perception, learning, and automated reasoning.

Over 100 partners in 13 countries, including:

AAAI

ACLU

AI NOW Institute

Allen Institute for AI (AI2)

Alan Turing Institute

Amazon

Amnesty International

Apple

BBC

Berkeley Center for Law & Technology

Center for Democracy & Technology

CMU Center for Human Rights  
Science

Electronic Frontier Foundation

Facebook

Future of Privacy Forum

Google

IBM

Intel

Microsoft

The New York Times

Samsung



# Civil liberties and other advocacy groups

---

- The ACLU has engaged with FRT from the perspective of guarding individual rights and liberties
  - Advocates bans and moratoriums on facial recognition applications, in government and industry, pending a range of issues and thorough review at all levels
- Filed many FRT lawsuits, e.g.,
  - May 2020 – against Clearview AI alleging violation of Illinois residents' privacy rights under the Illinois BIPA
  - Oct 2019 – against U.S. DOJ/DEA/FBI challenging secrecy in federal law enforcement use of FRT
- Electronic Frontier Foundation (EFF)
  - Works to ensure that rights and freedoms are enhanced and protected as use of technology grows
  - FRT “poses a threat to our privacy, chills protest in public places, and disparately impacts people of color. Congress should ban government use of face surveillance.”

# Ban Facial Recognition ([www.banfacialrecognition.com](http://www.banfacialrecognition.com))

---



**BAN FACIAL RECOGNITION**

BREAKING: Congress just introduced a bill that would effectively ban law enforcement use of facial recognition. Send a message now to tell your members of Congress that facial recognition surveillance technology is unreliable, unjust, and a threat to basic rights and safety, and they should support the legislation to stop facial recognition!

**REGULATION IS NOT ENOUGH**

**IT'S BROKEN**  
**IT'S INVASIVE**  
**IT'S UNJUST**  
**IT'S VULNERABLE**

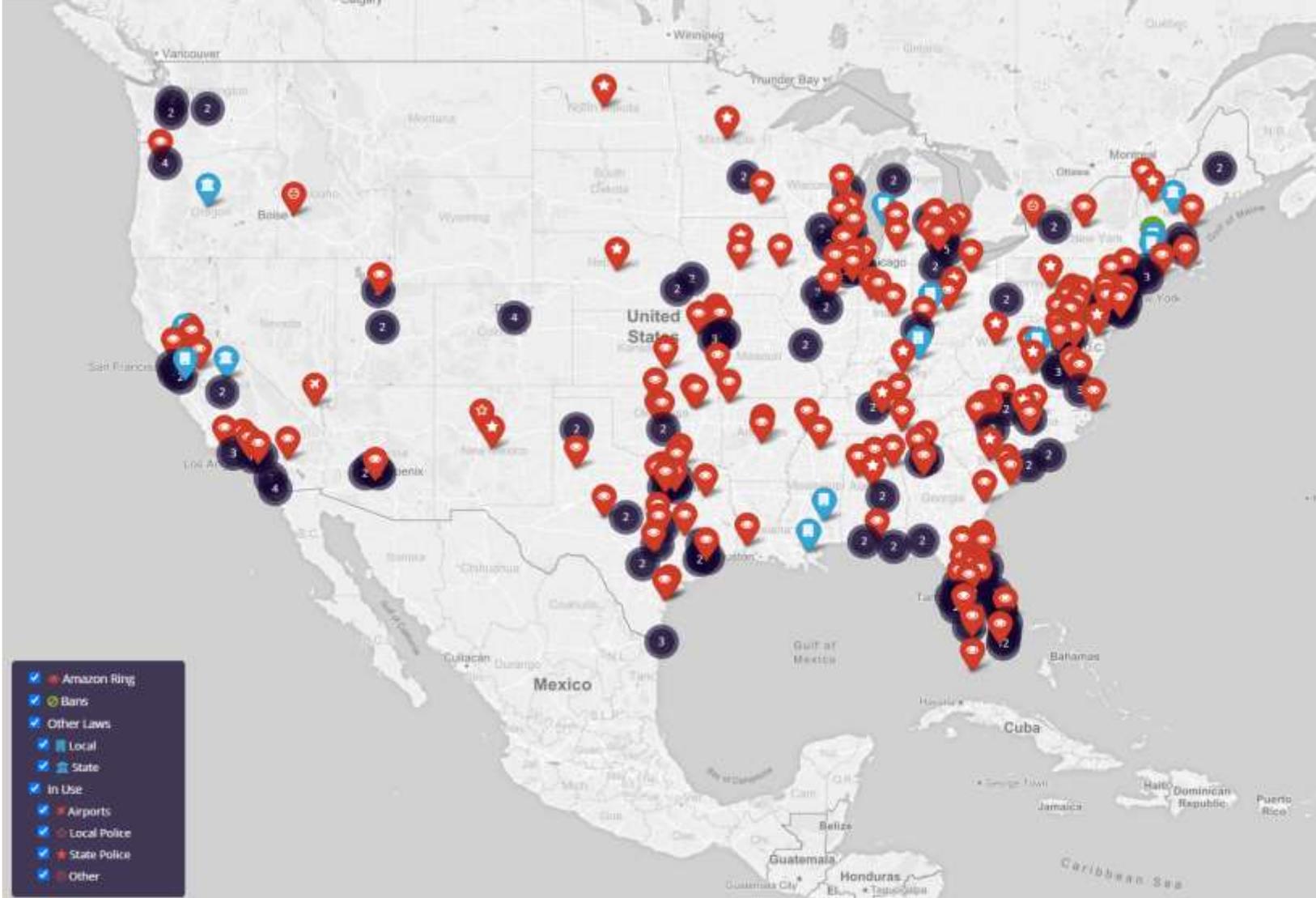
## *REGULATION IS NOT ENOUGH*

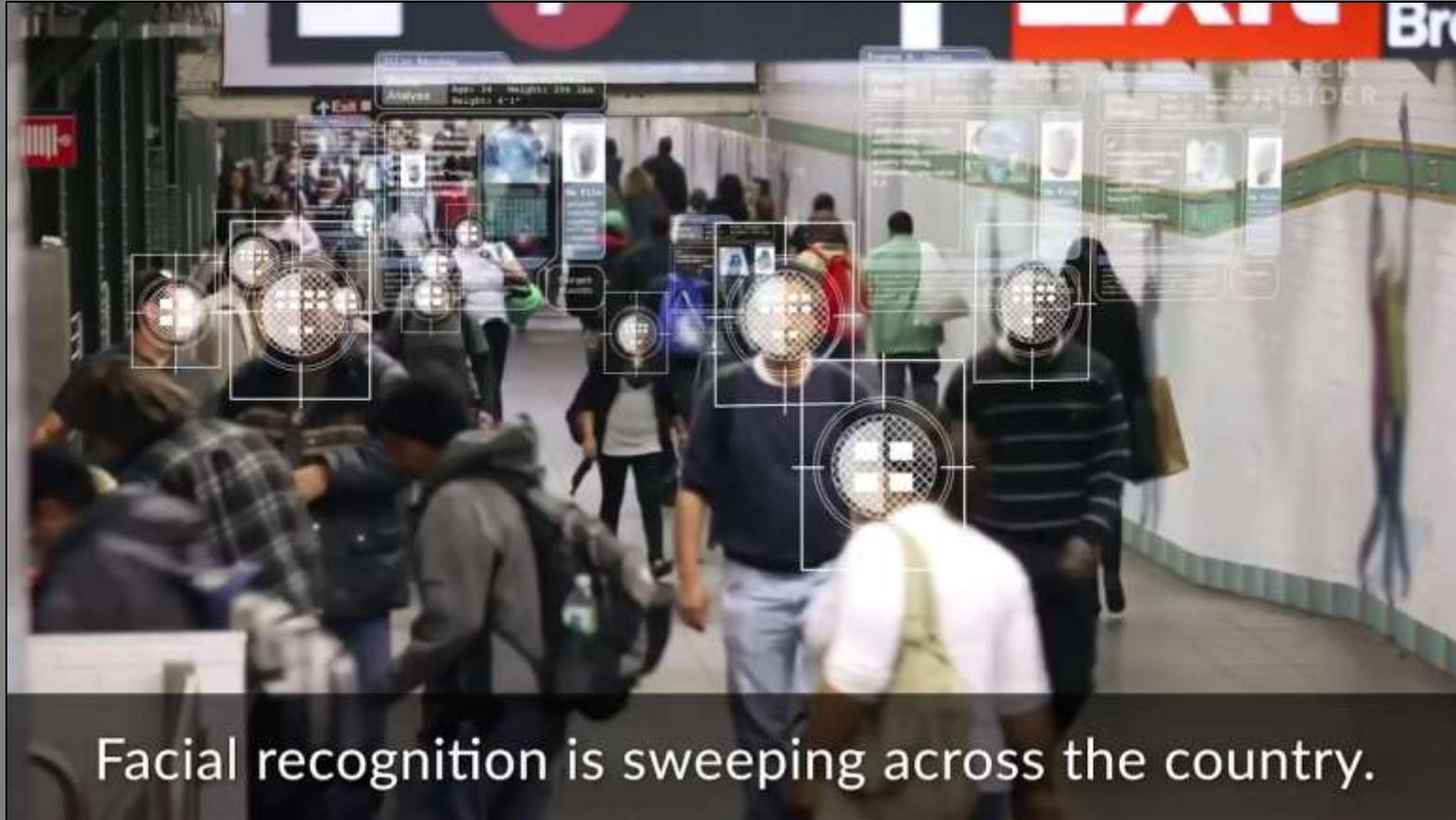
*Like nuclear or biological weapons, facial recognition poses a threat to human society and basic liberty that far outweighs any potential benefits. Silicon Valley lobbyists are disingenuously calling for light “regulation” of facial recognition so they can continue to profit by rapidly spreading this surveillance dragnet. They’re trying to avoid the real debate: whether technology this dangerous should even exist. Industry-friendly and government-friendly oversight will not fix the dangers inherent in law enforcement’s use of facial recognition: we need an all-out ban.*

Congressional Scoreboard

Who supports banning facial recognition

# Ban Facial Recognition





# So....

---

- We have this AI technology that is quite good and getting better all the time.
- Is it a wonderful technology that promises convenience, better security and privacy, and solutions to difficult problems in law enforcement and elsewhere?
- Or is it ushering in a dystopian Orwellian mass surveillance state and society?
- How should/can we balance between these?
  
- How important is “It feels creepy”? Does that mean it should be banned?
  - Electricity, automobiles, telephones, ...
- How do we know before it’s too late?
- Who decides?
  
- Should we “burn it all down”?



## ***Our Challenge: Misinformation***



Masahiro Ikeno, President & CEO, NEC Corporation of America  
Sept 2019 Speech to Japan Society of NYC

# Technical issues and challenges

---



- The components must continue to be improved
  - Algs, datasets, bias, accuracy, robustness, etc.
- But the bigger issue is the whole system
  - FRT algorithms and models
  - Data (from various sources)
  - Metadata
  - Privacy, security, access control
  - User expectations and consent
  - Humans in the loop who will make mistakes and violate guidelines and restrictions
- Systems engineering – full risk analysis, identify the weak points that require strict oversight

# There are many technical research challenges

---

- Improving data creation/collection processes
- Techniques and models for fairness-aware face recognition
- Formalizations of, and metrics for, fairness, bias, and discrimination
- Defining, measuring and mitigating biases in data sets
- Interpretability of machine learning models
- Automatic generation of explanations of system modeling, processing, and decision
- Revocable biometrics, allowing identifiers to be cancelled
- Translation of legal, social, and philosophical models of fairness into mathematical objectives
- Fairness and the relationship between prediction and intervention
- Systematic methods for auditing data and algorithms

# But also things beyond the core technical challenges

---

- Governments and companies have responsibility, but – in my opinion – researchers and practitioners have a special responsibility to understand the implications of technologies they are creating, and to communicate the potentially harmful or concerning implications as well as the technical successes and progress.
  - What are the social consequences of my work?
  - Is there potential social cost to this new approach?
  - Who can I engage with in a broader discussion of the impacts?
- The technical considerations of FR can't be divorced from its social implications. We must consider the social landscape in which the technology is embedded.
- Engage with colleagues who study (and make) public policy, have open-minded discussions.
  - Good opportunities for interdisciplinary funding!

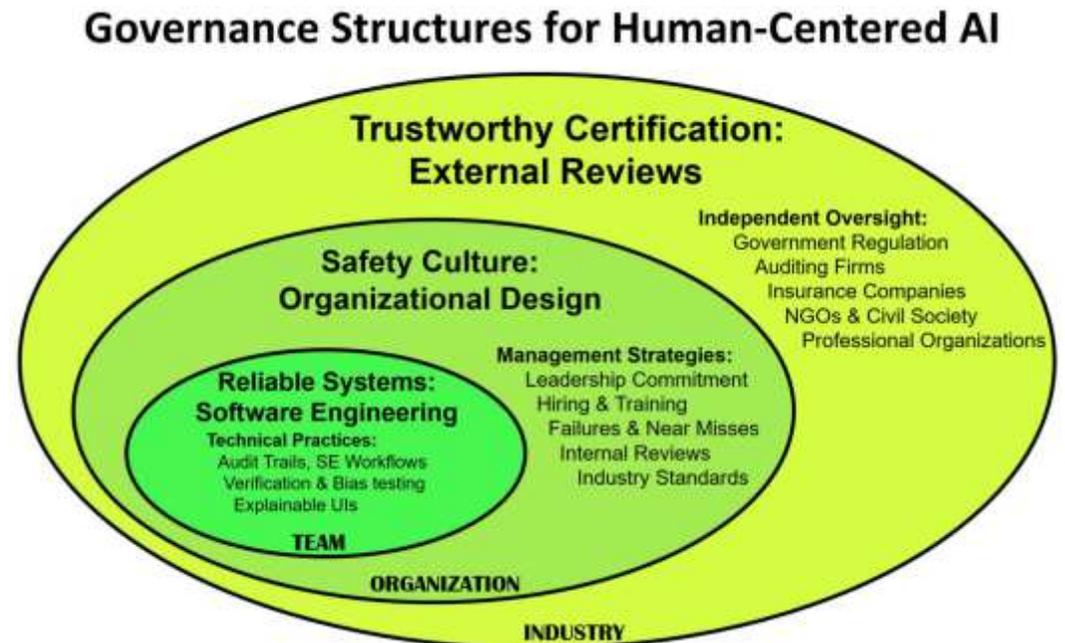
# Bridging the gap between ethics and practice

## Bridging the Gap Between Ethics and Practice: Guidelines for Reliable, Safe, and Trustworthy Human-centered AI Systems

Ben Shneiderman, University of Maryland

ACM Transactions on Interactive Intelligent Systems, Vol. 10, No. 4, October 2020

- 15 proposed recommendations at three levels of governance: team, organization, and industry
- Intended to increase the reliability, safety, and trustworthiness of HCAI systems
- Includes:
  - Sound software engineering practices for reliability
  - Business management strategies for safety culture
  - Independent oversight for trustworthy certification



# Bridging the gap between ethics and practice

---

- Sound software engineering practices for reliability
  - Audit Trails and Analysis Tools
  - Software Engineering Workflows
  - Verification and Validation Testing
  - Bias testing to Enhance Fairness
  - Explainable User Interfaces
- Business management strategies for safety culture
  - Leadership Commitment to Safety
  - Hiring and Training Oriented to Safety
  - Extensive Reporting of Failures and Near Misses
  - Internal Review Boards for Problems and Future Plans
  - Alignment with Industry Standard Practices
- Independent oversight for trustworthy certification
  - Government Interventions and Regulation
  - Accounting Firms Conduct External Audits
  - Insurance Companies Compensate for AI Failures
  - Non-governmental and Civil Society Organizations
  - Professional Organizations and Research Institutes

# What can FG do?

---

- Next month's NeurIPS conference will, for the first time, require that scientists address ethical concerns and potential negative outcomes of their work.
  - *Submissions will also be considered on ethical grounds. Regardless of scientific quality or contribution, a submission may be rejected for ethical considerations, including methods, applications, or data that create or reinforce unfair bias or that have a primary purpose of harm or injury.*
  - *In order to provide a balanced perspective, authors are required to include a statement of the potential broader impact of their work, including its ethical aspects and future societal consequences. Authors should take care to discuss both positive and negative outcomes.*
- Can/should FG do something similar?

# What can FG do?

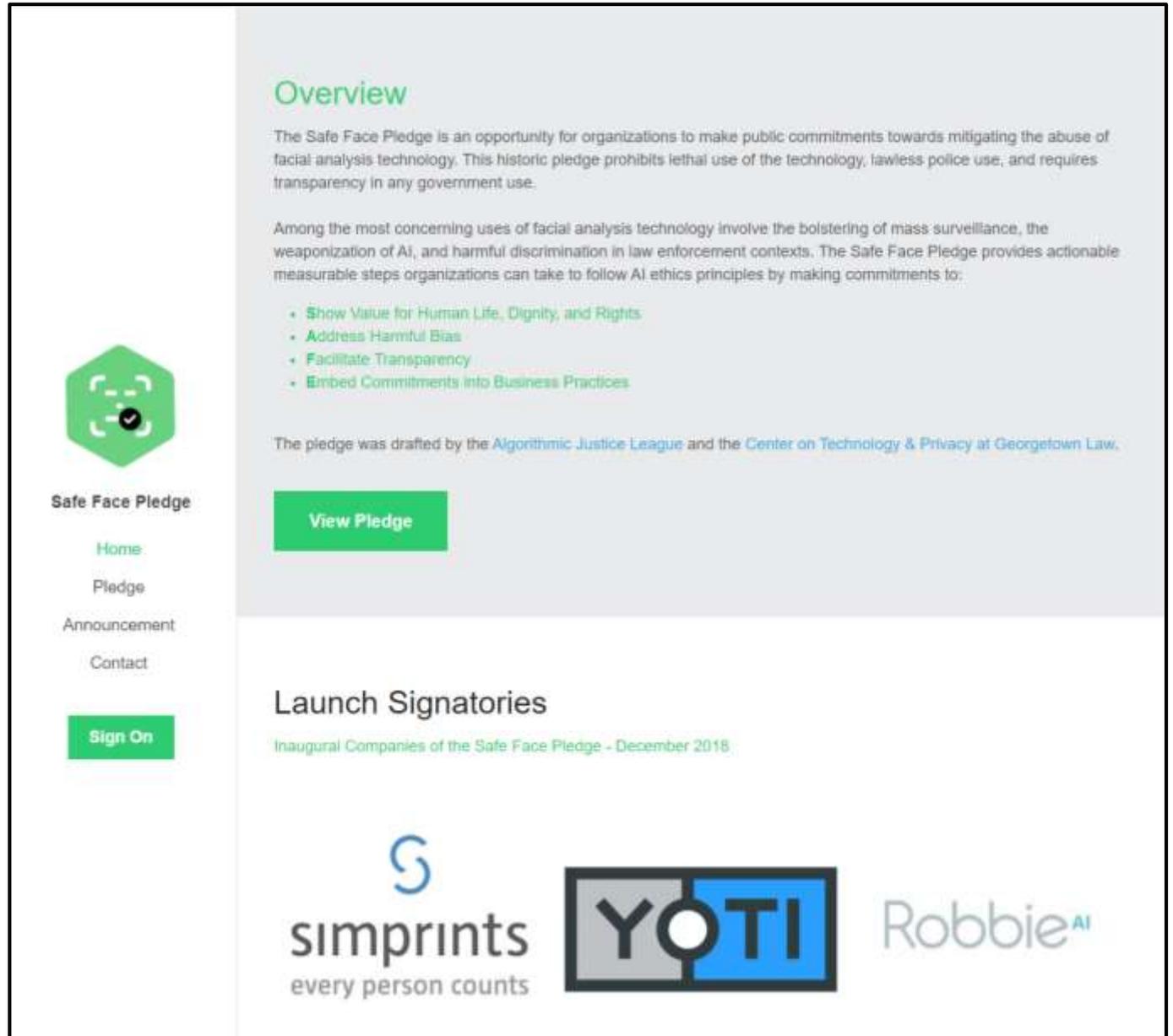
---

- Perhaps we should be introspective and ask ourselves some tough questions:
  - What might now be unacceptable for FG research – or at least raise ethical questions – that has been considered routine in the past?
  - Are there potential negative consequences of our work in general? Of specific subareas or projects?
  - Is there a clear (enough) distinction between academic research and how facial recognition is utilized?
  - There is, in fact, a long history of science being used to legitimize violence against marginalized people. Is this relevant to us?
  - Is denouncing unethical uses of FRT enough?
  - What are the community's responsibilities?
- Let's actively look for interdisciplinary opportunities with colleagues who study ethics, humanities, social science, law and policy.

<https://www.safefacepledge.org/>

### Commitments:

1. Show Value for Human Life, Dignity, and Rights
2. Address Harmful Bias
3. Facilitate Transparency
4. Embed Safe Face Pledge into Business Practices



The screenshot shows the homepage of the Safe Face Pledge website. On the left is a navigation menu with a green hexagonal logo containing a face icon with a checkmark. The menu items are: Safe Face Pledge, Home, Pledge, Announcement, Contact, and a green 'Sign On' button. The main content area has a grey header with the title 'Overview'. Below the title is a paragraph explaining the pledge's purpose. This is followed by a list of four commitments: 'Show Value for Human Life, Dignity, and Rights', 'Address Harmful Bias', 'Facilitate Transparency', and 'Embed Commitments into Business Practices'. A paragraph below states the pledge was drafted by the Algorithmic Justice League and the Center on Technology & Privacy at Georgetown Law. A green 'View Pledge' button is positioned below this text. The lower section is titled 'Launch Signatories' and includes the text 'Inaugural Companies of the Safe Face Pledge - December 2018'. At the bottom, logos for 'simprints every person counts', 'YOTI', and 'Robbie<sup>AI</sup>' are displayed.

## Overview

The Safe Face Pledge is an opportunity for organizations to make public commitments towards mitigating the abuse of facial analysis technology. This historic pledge prohibits lethal use of the technology, lawless police use, and requires transparency in any government use.

Among the most concerning uses of facial analysis technology involve the bolstering of mass surveillance, the weaponization of AI, and harmful discrimination in law enforcement contexts. The Safe Face Pledge provides actionable measurable steps organizations can take to follow AI ethics principles by making commitments to:

- [Show Value for Human Life, Dignity, and Rights](#)
- [Address Harmful Bias](#)
- [Facilitate Transparency](#)
- [Embed Commitments into Business Practices](#)

The pledge was drafted by the [Algorithmic Justice League](#) and the [Center on Technology & Privacy at Georgetown Law](#).

[View Pledge](#)

## Launch Signatories

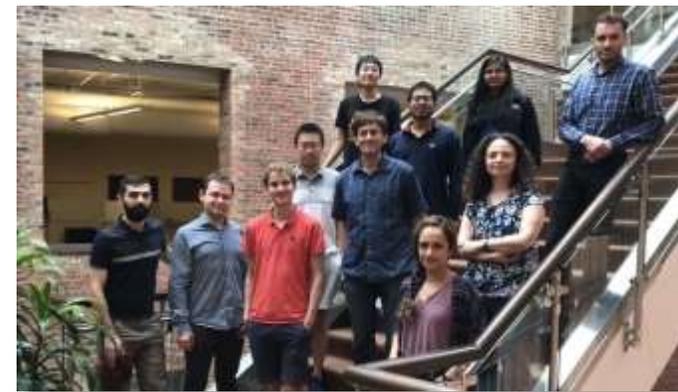
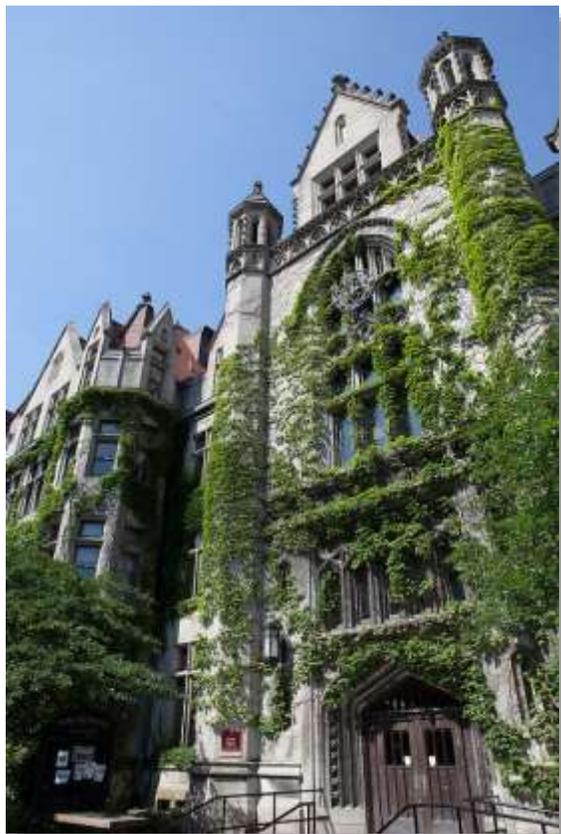
Inaugural Companies of the Safe Face Pledge - December 2018

# Summary

---

- Facial recognition is an appealing/promising technology for many good reasons.
- But concerns about the use of FRTs are growing and motivating action. This is not going away.
- “We just do research” is not a valid excuse (IMO) for not engaging with relevant questions of society and policy.
- Responsible research, development, and deployment matters
  - Personal, corporate, community, global
  - “Adding a course in ethics” is not the solution
- Neither extreme – Pollyannish or Luddite – is probably useful or appropriate.
- A combination of technical, policy, and regulatory approaches can make a huge difference
  - There’s plenty of common ground despite political preferences and differences.



Thank You!



<http://www.ttic.edu/mturk>

