**The Good, the Bad, the Ugly**

*Facial Recognition technology does not care whether you are pretty, or* ***pretty ugly****, a clear image of your countenance is all that is required*

It's 2021 fans, and now there are millions of cameras everywhere, usually for public security reasons. Additionally, many homes are now protected by camera, inside and outside homes. If you are not used to it yet, get use to it. Because of modern hi-res camera technology, our human faces are recorded constantly and almost everywhere. With the capability to capture facial images, facial recognition is a standard practice for private and government data base files. Is this good or bad?

When we can visually capture crimes in progress and there is good video, criminals cannot deny that they were not present at the crime scene. The actual criminal act is often captured. Hooray, life is tougher now, for many criminals, *especially those not wearing face masks.*

On January 6, 2021, when extremists/insurrectionists invaded our National Capital building, multiple cameras captured the faces of hundreds of participants, and now we know who many of the perpetrators are, and they are being prosecuted. Without a lot of videos covering many parts of the invasion of our capital, many suspects would never have identified or caught.

Thus, when facial recognition is used to catch criminals and insurgents, it serves a very good public purpose which no one denies. But having images of virtually everybody does introduce opportunities for abuse. But like a lot of new technology, facial recognition can be used for good purposes, or be used for negative purposes.

Now, for anyone who has the new iPhone 12, or Samsom 21, face recognition replaces passwords, which is very handy, also security is better as *duplicating ugly faces is very hard to do.* Facial recognition at ATMs would be great too. The crooks will have to be a lot smarter to fake out facial recognition.

**Interested in what China has done with facial recognition?**

**I**n China, facial recognition is used for many purposes, including the control of ethnic minorities (the Uighurs), deterring crime (recording and identifying criminals in action) and also shaming citizens who behave outside of normal standards - even some fairly innocuous behavior. The citizens photographed behaving badly are publicly shamed for low standards of behavior. China uses shame to control public human behavior. Cameras have deterred citizens from spitting and urinating in public places. Foreigners who visited China before Mao died and visit today report that China is now a very clean country.

Now that Chinese facial recognition databases are very robust, personal safety and security for her citizens is a positive feature of modern Chinese society. Add in strict gun controls, and many visitors to China are very impressed that there is a lot less crime, and streets are safe in China, even at night. Most Chinese do not object to the invasion of their privacy as they are willing to give up some of their civil rights to live in an environment almost free of crime.

China also uses this technology to track foreigners. Passport images are used to open files on foreign officials so that their movements (and contacts) can be monitored. Intelligence officers under official cover operating in China will need to leave the embassy in disguise, or hidden in the back seat, or the trunk of a vehicle, to evade surveillance by Chinese security. Many activities will take place stealthily at night and in sanitized areas (rooms), perhaps out of city limits away from millions of cameras.

**==================================**

**Sources:**

**1. "*The Promise and Peril of Facial Recognition," Floyd Abrams, Lee Wolosky, WSJ, 14 Jan 2021***

***2. https://www.cnet.com/google-amp/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/***

**How China uses facial recognition to control human behavior**

When facial recognition is everywhere, anything you do is fair game for public shaming and punishment.

[**Alfred Ng**](https://www.cnet.com/profiles/alfred.ng/) **, Aug. 11, 2020 5:00 a.m. PT**



A screen shows a demonstration of SenseTime Group's SenseVideo pedestrian and vehicle recognition system at the company's showroom in Beijing.

Gilles Sabrie/Bloomberg via Getty Images [This story is part of Generation China, CNET's series exploring the nation's technological ambition.](https://www.cnet.com/generation-china/#ftag=CAD-00-10aag7d)

Facial recognition supporters in the US often argue that the surveillance technology is reserved for the greatest risks -- to help deal with [violent crimes](https://www.npr.org/2019/08/21/752484720/how-a-tip-and-facial-recognition-technology-helped-the-fbi-catch-a-killer), [terrorist threats](https://nypost.com/2019/08/25/how-nypds-facial-recognition-software-ided-subway-rice-cooker-kook/) and [human trafficking](https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/). And while it's still often used for petty crimes like [shoplifting](https://www.cnet.com/news/with-facial-recognition-shoplifting-may-get-you-banned-in-places-youve-never-been/#ftag=CAD-00-10aag7d), [stealing $12 worth of goods](https://www.cnet.com/news/facial-recognition-overkill-how-deputies-solved-a-12-shoplifting-case/#ftag=CAD-00-10aag7d) or [selling $50 worth of drugs](https://www.jacksonville.com/public-safety/2016-11-11/how-accused-drug-dealer-revealed-jso-s-facial-recognition-network), its use in the US **still looks tame compared with how widely deployed facial recognition has been in China.**

**China's facial recognition system** [**logs nearly every single citizen in the country**](https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html)**, with a vast network of cameras across the country**. A [database leak in 2019](https://www.cnet.com/news/chinese-facial-recognition-company-left-database-of-peoples-location-exposed/#ftag=CAD-00-10aag7d) gave a glimpse of how pervasive China's surveillance tools are -- with more than 6.8 million records from a single day, taken from cameras positioned around hotels, parks, tourism spots and mosques, logging details on people [as young as 9 days old](https://twitter.com/0xDUDE/status/1098251123754962945).

Top of Form

Bottom of Form

The Chinese government is **accused of using facial recognition to commit atrocities against Uyghur Muslims, relying on the technology to carry out "**[**the largest mass incarceration of a minority population in the world today**](https://www.cbsnews.com/news/china-puts-uighurs-uyghyrs-muslim-children-in-prison-re-education-internment-camps-vice-news/)**."**

**"China uses facial recognition to profile Uyghur individuals, classify them on the basis of their ethnicity, and single them out for tracking, mistreatment, and detention**," a bipartisan group of 17 senators [said in a letter](https://www.portman.senate.gov/sites/default/files/2020-03/China%20Warren%20AI%20Letter_0.pdf) to Secretary of State Mike Pompeo on March 11. "And these technologies are deployed in service of a dystopian vision for technology governance, that harnesses the economic benefits of the internet in the absence of political freedom and sees technology companies as instruments of state power."

China's aggressive development and use of facial recognition offers a window **into how a technology that can be both benign and beneficial -**- think your iPhone's Face ID -- can also be twisted to enable a crackdown on actions that the average person may not even consider a crime. Chinese officials have used surveillance tools to [publicly shame people wearing sleepwear in public](https://www.cnet.com/news/chinese-city-uses-surveillance-tech-to-shame-citizens-for-wearing-pajamas-outside/#ftag=CAD-00-10aag7d), calling it "uncivilized behavior."

The punishing of these minor offenses is by design, surveillance experts said. **The threat of public humiliation through facial recognition helps Chinese officials direct over a billion people toward what it considers acceptable behavior,** from what you wear to how you cross the street.

"The idea is that the authorities are trying to put in place comprehensive surveillance and behavioral engineering on a mass scale," said Maya Wang, a senior researcher on China at the Human Rights Watch. "The authorities want to create a kind of society that would be very easy for them to manage."

**Behavioral engineering**

The idea that China's facial recognition would automatically [put your name and photo on a billboard for jaywalking](https://gizmodo.com/facial-recognition-flags-woman-on-bus-ad-for-jaywalking-1830654750) and [privately text you a fine](https://www.cnet.com/news/jaywalking-in-china-surveillance-system-will-sms-you-a-fine/#ftag=CAD-00-10aag7d) instills fear in people to behave a certain way, Wang said.

**Technology has often had that ability to affect behavior, even outside of China.**

Behavioral engineering is the concept of [combining technology and psychology to nudge people to act a certain way](https://venturebeat.com/2013/07/08/behavior-enigineering/), and it's something we see every day. It's evident in "[dark patterns](https://www.cnet.com/news/facebook-google-and-microsoft-trick-people-into-sharing-personal-data-report-says/#ftag=CAD-00-10aag7d)," interface designs like hidden opt-out buttons that trick people into giving up their personal data, for example.

[Generation China](https://www.cnet.com/generation-china/#ftag=CAD-00-10aag7d) is a CNET series that looks at the areas of tech where the country is seeking to take the leadership position.

But there's a key difference in how behavioral engineering is carried out in the US compared with China and its facial recognition.

"It's expressed in a commercial manner in the US, whereas in China it's a state effort," Wang said. "The dynamics are different, and the amount of power is different, but it has striking similarities."

In the US, behavioral engineering can be done through amassing data on people, and pushing or excluding content to them based on predicted personality traits.

Facebook's [2018 scandal with Cambridge Analytica](https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/#ftag=CAD-00-10aag7d) stemmed from the fact that the now-defunct UK data analytics firm used [data from millions of people to target advertising](https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie) that would sway people to vote a certain way.

Russia's 2016 US election meddling efforts involved using [Facebook to create divisive groups](https://www.cnet.com/news/this-was-the-most-viewed-facebook-ad-bought-by-russian-trolls/#ftag=CAD-00-10aag7d) and stage events where people would show up to protest. These posts would be targeted to police groups or specifically to Spanish speakers, for example.

While that type of behavioral engineering is mostly geared for selling products and profits, China's push is more about instilling fear and control over its population -- and facial recognition plays a key part in that.

"It conditions the idea of 'this is how society works,' that you're always being watched," said Jake Laperruque, a senior counsel at the Constitution Project. "It seems like trying to reinforce to people that 'we're watching all the time, if you ever do anything to piss us off, we will see and we will find a way to embarrass you.'"

**China's track record**

**In China, no one is safe from facial recognition, or the public shaming that comes with it.**

Cameras set up at crosswalks to identify and post photos of jaywalkers are commonplace, and a [report from Abacus in May 2019](https://www.scmp.com/abacus/tech/article/3029382/facial-recognition-china-shames-jaywalking-child-erupting-debate) showed photos of children jaywalking on a digital billboard. The local traffic police said "children should be treated the same as adults," according to the outlet.

A Chinese park [has also relied on facial recognition to prevent people from taking too much toilet paper](https://www.cnn.com/2017/03/20/world/china-toilet-paper-thieves-face-recognition-trnd/index.html), scanning people's faces before dispensing out the rolls.

"It's kind of an 'anything goes' system there, no matter how minor," the Constitution Project's Laperruque said.  "Any sort of offense goes for this kind of tech."

And while in the US, [facial recognition is going through a reckoning over its racial bias and human rights concerns](https://www.cnet.com/news/lawmakers-propose-indefinite-nationwide-ban-on-police-use-of-facial-recognition/#ftag=CAD-00-10aag7d), in China, the surveillance technology's providers boast its abilities to single out people of different ethnicities.

"There's no allowed space at all, both online and offline, to discuss racial bias and the persecution of minorities in China."

**Maya Wang, senior researcher on China at the Human Rights Watch**

Last November, IPVM found that Chinese surveillance company Hikvision [marketed that its cameras could automatically identify Uyghur Muslims](https://ipvm.com/reports/hikvision-uyghur) with its facial recognition.

There's pushback on facial recognition in the US because researchers are able to bring to light their concerns about the technology's racial bias, but there isn't similar scrutiny in China, researchers said.

China's facial recognition accuracy rates aren't challenged, even when it accidentally picks up a [person on a bus ad and considers them a jaywalker](https://www.cnet.com/news/facial-recognition-system-mistakes-bus-ad-for-jaywalker/#ftag=CAD-00-10aag7d).

"Americans can talk about racial inequalities without fear," the Human Rights Watch's Wang said. "These systems are not discussed or pushed back in China. There's no allowed space at all, both online and offline, to discuss racial bias and the persecution of minorities in China."

**Recognizing influence**

China's model of facial recognition, from its oppressive surveillance of Uyghur Muslims to its every day grip over a population of 1.4 billion people, also poses a concern for the international community, US lawmakers said.

Last September, the Carnegie Endowment for International Peace found that China was a major supplier of AI surveillance, [providing the technology to 63 countries](https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847).The next closest provider for AI surveillance tech was Japan's NEC Corporation, which sells facial recognition to 14 countries.

In April, [Reuters reported that Amazon](https://www.reuters.com/article/us-health-coronavirus-amazon-com-cameras/exclusive-amazon-turns-to-chinese-firm-on-u-s-blacklist-to-meet-thermal-camera-needs-idUSKBN22B1AL) bought cameras from Dahua, a Chinese surveillance company blacklisted by the US over allegations that it helps China detain and monitor Uyghur Muslims.

*The $10 million deal was for 1,500 cameras to help monitor the spread of COVID-19, according to the report.*

In the senators' letter on March 11, they raised issues about China's influence on how facial recognition should be used when it's the technology's top exporter.

Wang noted that while facial recognition is often a subsidiary for US tech giants, like Amazon's Rekognition or Microsoft, in China, there are multiple companies already dominating the industry. The country's acceptance of a surveillance state allows facial recognition providers to push forward with the technology, even for the most trivial uses.

With that level of influence, there're concerns that China's model of how to use facial recognition -- a widespread network designed for public shaming and control -- could spread to the rest of the world.

"Unfortunately, China has indicated a willingness to use standard setting bodies in perverse ways to normalize global opinions about Orwellian surveillance technology," the group of lawmakers said. "By shaping the debate about the legitimate uses of artificial intelligence and facial recognition, China can expand opportunities for countries, particularly those in the developing world, to utilize Chinese surveillance technology."