# FACIAL RECOGNITION: FROM FICTION TO REALITY
# WHAT ABOUT PRIVACY RIGHTS AROUND THE GLOBE?

## INTRODUCTION

**BLACK MIRROR** – On facial recognition and social scoring. For those who are familiar with the series, you probably recall one of the episodes called "Nosedive", which depicts a world placed under facial recognition and each individual rating one another on a five-points scale.
From Science Fiction to reality: Comparison with the book of G. Orwel "1984" and Philip K Dick's "Minority Report".

Watch **2 videos**:
https://www.youtube.com/watch?v=Fq1SEqNT-7c (Wall Street Journal): China embraces facial recognition.
https://www.youtube.com/watch?v=-yvxbi5GMnA (SKYNEWS, In England)

https://www.youtube.com/watch?v=nT_PXjLol_8
https://www.youtube.com/watch?v=eViswN602_k

**In January 2018, the world discovers the scary reality in China through the news**. China has come under particular criticism for rapidly deploying AI in surveillance for alleged security reasons. Facial-scanning cameras are part of daily life in China, where they're used for marketing, surveillance and social control. Indeed, since 2014, Chinese Big Brother Dictatorship deploys personal scorecards to control everyone and rank individuals on behavior. Under a social credit scheme (800 points), they instantly gain or lose points from being judged through a sophisticated network of 200 million surveillance cameras, which should triple by 2020 to be fully effective all around the country (for now only 12 big cities are under control with no dead angles).
The program focuses on facial recognition, body scanning and geo-tracking. The data is combined with information collected from individuals' public behavior — including medical and educational — along with their financial and internet browsing histories. Their score can also be affected by people they associate with, friends or family. "If your best friend or your dad says something negative about the government, you'll lose points too." "keeping trust is glorious and breaking trust is disgraceful". Keeping promises or not, you will reap the consequences of your words and acts. You obtain special privileges, incentives and rewards such as VIP treatments at hotels, airports, cheap loans, fast tracks to universities and jobs. If you are at the bottom, you are socially discredited, banned, discarded, from travels, credit or governmental jobs…. Your scorecard level impacts positively or negatively your children who can have a good start in life or undergo the unfair contrary.

**Elsewhere in the world:**
In GB, in France, in the US, in Canada, etc… the use of this video surveillance is already widely spread for the use of private companies, Airports for security reasons…. In meetings and events, in malls and shops to gauge attendee satisfaction, customers' behavior and preferences … but the use of facial

recognition technology is still limited. As seen on the video in the UK, it is already used for the third year trial period, without proper protective legislation, by the police on special events like carnival. The police holds more than 20 million facial recognition images - which the Government says don't need to be deleted. At the end of the trial period however, a public debate should be organized.

Facial recognition technology is also found all around the world in smartphones to lock and unlock, your phones, your apps, to enhance security of personal information from attacks, personal enhanced photos taken and shared through snapchat or many others apps…

**Quick survey**: How many of you already use facial recognition applications on smartphones?
How many of you send pictures on social media? Tagged pictures with names, answer messages with tags, namely on Facebook for example?
We are all aware that everything we post, every person we tag (and even not tagged) is thoroughly collected and processed into big data to be exploited, by Facebook, the adverts and other companies and states? Especially if those photos and comments are published on the open public space, but even privately.

**Interestingly,** I came across, in my little research on the Internet on this topic, on a **study** made by 2 **students** of the **Business School of Stanford University**, M. WANG Yilun and M. Michal KOSINSKI. Their work of 47 pages on AI and social and behavioral sciences was published in September 2017 in the Journal of Personality and Social Psychology and titled the following way: "*Deep Neural Networks (DNN) are more accurate than human at detecting sexual orientation from facial images"*. I was already shocked to read the title, that the study would come from a prestigious and serious BS, published work, and also because it is commonly agreed that such morphological profiling can be particularly biased and dangerous. What was the purpose of this work? Especially targeting a special minority group of people that could be even more ostracized? There was no point to me to write such a work. But I read it to understand where and if there was an underlying purpose.
They advanced the thesis that the science from judging one's character from their facial characteristics or physiognomy dated back to ancient China and Greece (under Aristotle and Pythagoras). They also underlined that physiognomy was also recently analyzed as "a mix of superstition and racism disguised as science" (Jenkinson 1997). But nevertheless, insisted to draw a link between facial appearance and character, saying that the first influences the second. They argued that the link was supported by the fact that people can accurately judge other's character, psychological state and demographic traits from their faced. Quoting Brown and Perrett (1993), they said: "for example, we can easily identify other's gender, age, race or emotional state even from a glimpse of their faces".
**Method**. So, they undertook to collect a huge number of faces publicly available on Facebook, public websites and profiles posted on a US dating website, displaying sexual orientation. They collected 130.741 images of 36.630 men and 170.360 images of 38.593 women. And they used algorithms to match some facial features and criteria common to each sexual orientation to draw their conclusions and checked with as many pictures as they could through the AI technology. They extracted features to classify sexual orientation with an accuracy of the algorithm around 91% for men and 83 % for women, which represents 30% more than with the human brain.
**NOW, they raised the issues**:

- what about privacy, which is the biggest critic of available data + machine learning tools to build whatever morphological study without a person's consent or knowledge?
- What, if the findings were made public?

According to the study, it seems that governments and companies are already deploying face-based classifiers aimed at detecting intimate traits (Chin & Lin 2017, Lubin 2016) and there is an urgent need for making policies. It was a way to alert on unethical use of algorithms, to arise awareness about the technological ability and the dangers to make such a study without proper regulations to prevent it and to protect people. They just exploited the digital footprints left on the Internet. "*They did not create a privacy-invading tool, but showed that basic and widely used methods pose serious privacy threats*", to foster policymakers to introduce legislation to protect people from the digital environment. They said:" *Data can be easily moved across borders, stolen, recorded without user's consent*". Moreover, "*facial profiling could be dangerously inaccurate and biased*" as expert warned (Lubin 2016, Oct. 12).

About recent yellow vest demonstrations and violence events and riots, some public authorities raised the issue of rolling out video surveillance enhanced with the facial recognition technology to save time in apprehension of suspects and maintain public order. This possibility was highly criticized regarding the fundamental right of individual privacy. But even in our country of fundamental liberties and human rights, the question popped-up, which commits us to think about it seriously.

Facial recognition is a computerized technology which permits to put a name and other identification on a face. If it was discovered in the early 70s, it began to be used in the 90s and is being enhanced since then to be used for less than 10 years now in certain countries.

As this facial recognition technology is already widely spreading around the world, let us see what it is expected to bring positively and negatively (I) to reflect upon how the legal vacuum could be filled and implemented to prevent misuses, in France, in Europe, and Globally (II).

## I – WHAT IS TO EXPECT FROM FACIAL RECOGNITION TECHNOLOGY, POSITIVELY AND NEGATIVELY?

**SOME ISSUES RAISED:** security, business, facilitating tools, Big brother's spectrum – no more freedom, no privacy - Big data collection – use and misuse – discrimination and ostracism – threats on democracy and fundamental rights. Regulatory issues.
Let us see the pro and cons.

### A) PRO – FACIAL RECOGNITION

We may wonder why in China people agree to deploy facial recognition in big cities and all around the Country. Chinese people basically believe that they need this technology for many positive reasons:

- **Security, safety, stability of the country**. "*people in every country want a stable and safe society*"
- The best way to manage a complex country with the world's biggest population
- They can benefit from the system by obtaining special privileges, incentives… parents score is transmitted to their children who can have access to the best schools, health care, Party's protection bestowed upon him …
- They have no other choice.

They believe that with this system of social credit, the promise [propaganda] of President XI Jing Ping will become a reality: “we will help each other, love each other, and help everyone, become prosperous, we will be rich and democratic, cultural, harmonious and beautiful”. “It is XI’s hope, it is the whole Chinese nation’s hope”.
It doesn’t mean that they unanimously accept it as the number of fraud and attacks is huge. But for many Chinese people, privacy doesn’t have the same premium as it does in the West and they value community over individual rights. Most feel that social credit based on video surveillance will bring a safer, more secure and stable society. They don’t even have a public debate about implementing the system.

**Initially used for military reasons** in Irak and Afghanistan to fight terrorism, it has been deployed in airports and borders, and is now progressively invading private businesses.

The main argument for the use of the FR technology is **security**, enabling to rapidly find criminals. In real time, the glasses worn by Chinese policemen show the target’s name, gender, address and ethnicity and highlights whether they are wanted for a crime or offense. Police in Zhengzhou said the technology had resulted in seven arrests (including charges of human trafficking). China is turning itself a surveillance state, likewise Orwell’s novel “1984”. In December 2017, a BBC reporter was tasked with testing out the capabilities of China’s massive CCTV surveillance network by trying to evade it. He was tracked down in seven minutes.
Banks, airports, railways stations, sport events, hotels, even public toilets are trying to verify people’s identities through face analysis, officially to:

- track and find criminals and dissidents.
- Spot suspiscious behaviors
- Predict crime
- Coordinate emercengy services
- Monitor the coming and going of 1.4 billion people, where they go, who they meet, what they see, what are their interests, what they believe, who they associate with…

Thanks to “Trackchild”, Police in New Delhi recently trialed facial recognition technology and identified almost 3.000 missing children in four days.
For the same reasons, identification and authentication of people would be more accurate.

Another use of the technology: **health sector**
It has been already discovered that certain rare diseases can be identified through FR technology, so that a cure can begin at the earliest stage. In a recent study (Dec 2018) carried out by a team at Stanford University, scientists found that face and speech software can identify signals of **depression** with reasonable accuracy. The research was led by **Fei-Fei Li**, a prominent AI expert who recently returned to Stanford from Google, saying at the NeurIPS AI conference in Montreal: “*Compared to physical illnesses, mental disorders are more difficult to detect. “The burden of mental health is exacerbated by barriers to care such as social stigma, financial cost, and a lack of accessible treatment options […] This technology could be deployed to cell phones worldwide and facilitate low-cost universal access to mental health care*.”

Another use of the technology: **Business, marketing and sales**
Used in malls, shops, private enterprises, hyper personalized marketing, banks.
Control of employees to enter the corporate building: tracking employees for HR managers and individual performance.

China is, no surprise, the 1st digitalized country in the world with the most advanced technology.

SenseTime is a young Chinese Start-up which raised beyond us$ 1.5 billion funds to achieve unprecedent performance of this technology, with the Japanese Softbank. With more than 170 M cameras of video-surveillance equipped with this technology, China intends to triple this number in 5 years and utilize the massive data collected by deep learning machines. How will it be used? What are the kinds of derives?

B) **CONS – FACIAL RECOGNITION**

Under alleged security reasons, there are many risks of abuse, misuse, misinterpretation of data collected, and serious concerns regarding individual privacy rights.

Main dangers are pointed out with facial recognition technology:

- Treatment of the information collected on people, faceprints and other physical and psychological characteristics, with automatic and biased automatic decisions-making;
- Mass surveillance of the population (like in China);
- Discrimination over misinterpretation of data collected (it is particularly true that women and colored people are less easily identified as the technology is not yet accurate enough and could be misleading and dangerous);
- Intrusion in the private life of individuals through cameras of surveillance, including through smartphones and computers.

Once the ultra-performant technology is in the hands of one powerful, authoritarian person, it will become one of the most powerful tool to deprive individuals from fundamental rights.

The different companies currently working on this technology (GAFA, Samsung, SenseTime, etc…) are trying to enhance it so that to reduce/eliminate bias and potential discrimination by increasing the accuracy of recognition. What, if people cover their faces with masks, bandanas or anything else to avoid to be identified, or try to display someone else's face? In China, the best technologies distinguish a real person and face from an image, recognize the real person wearing a mask and through sunglasses or different haircut style or make-up. But not all technologies are as performant as they should be and there are many deficiencies. For example, Dong Ming Zhu was recently identified in the town of Ningbo to have crossed roads out of the crossing pedestrian passage whereas it was only a picture of her on a bus… What if a person is disfigured or undergoes facial surgery? Can the system be faked? It is reported that with certain products, it is easy to fake it (Adam Harvey), whereas with others, it becomes more and more difficult to cheat the system.

Low rating people (Jaywalking, late payments on bills or taxes, buying too much alcohol or speaking out against the government, too long-playing video games, wasting money on frivolous purchases, posting "bad" words or "bad thinking" on social media, according to Business Insider) = banned from traveling, from finding a good job, …. The system results in destroying people's lives, their carriers, isolate them, outcast them and the whole family and friends related to them. They are exposed to reprisals from the state. But who gives the credits? On what criteria?
For a Chinese journalist, Liu Hu, who was arrested and condemned to prison for alleged political dissidence "*This kind of social control is against the tide of the world. The Chinese people's eyes are blinded and their ears are blocked. They know little about the world and are living in an illusion*."

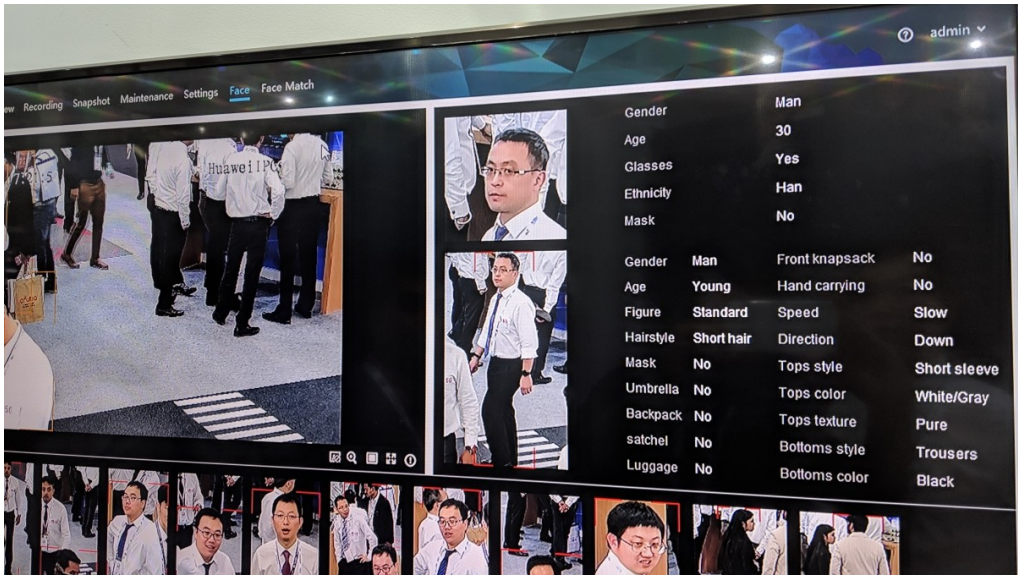
In France, proposition to suppress subsidies to parents of wrong doer child … Social credit. We do not have the technology spread yet, but we have the social/medias and it is very easy to discredit people through rumors and false news. Social credit is working somehow in France and in other western countries in a different way.

The rapid growth of biometric scanning system has led to a brunch of commercial applications being designed for use in gyms, restaurants and even public toilets. Human rights activists, however, warn that mass data collection is likely to be abused.
In 2017, it emerged that Chinese law enforcement was using a system known as "Police Cloud", built by the Ministry of Public Security, to monitor "extreme thoughts". The program, according to Human Rights Watch (HRW), will be rolled out nationwide. It is believed to collect personal information including medical histories, flight and train records, biometrics, national ID numbers, addresses, family relations, whose people they meet, what they've been viewing online, birth control methods, religious affiliations and even supermarket delivery records. The high-tech cameras offer 720-degree, high-definition recording and already thousands of police officers are equipped with this technology, reportedly focusing on "aggressive suspects".

Contributors: Yilun WANG and Michal KOSINSKI. Collection of data can be sold to private companies, to states organizations….

Mass surveillance risk. The association ACLU (*American Civil Liberties Union*) denounced the risks of derive in the utilization of the Amazon « Rekognition » by local police. Google already collects all the data of our different geolocalization, our moves from a place to another, the mode of transportation, our schedules, the amount of time spent between each move, our environment, … even if we have no Internet connection or if we are in plane mode.

Security risks: not as secure as pretended. Most companies are working on the improvement of the technology to prevent easy unlocks of bank accounts, smartphones applications, etc, through a simple image of the person. For example, regarding smartphones, Apple (Face ID) has created a projector able to create a unique profile by analyzing 30 000 points of the face, through a special camera capturing an infrared image and confirming the corresponding face modelized in 3 D, whereas google has just created a flat image in 2D, which is much easier to fake and bypass.



This is what Huawei's technology offers.
(Photo: The Quint)

If in China, we acknowledge the fact that a legislation protective of human rights is almost inexistent, which enables the central and local authorities to mis-use the technology almost unlimitedly, what is the legal framework in France, Europe, the US and on a global scale?

## II – LEGAL VACUUM TO BE THOROUGHLY FILLED AND IMPLEMENTED TO PREVENT MISUSES OF THE FACIAL RECOGNITION TECHNOLOGY

France is only authorized to use the technology in Roissy and Orly Airports and Gare du Nord Eurostar terminal and just to verify in real time the identity of the person travelling at these localizations, not to store any data, thanks to the GPDR restrictive legislation. Many other Member States test the technology, like Germany in Berlin's railway station, with the same level of protection uniformized in the EU, but the legal framework still needs to be reinforced. In the rest of the world, the legal vacuum needs to be thoroughly filled and implemented to prevent misuses and abuses.

### A) **A protective GPDR in France and in the UE to be extended and adapted to facial recognition technology?**

In July 2016, a legislative proposal to the French parliament suggested to authorize facial recognition processes as part of the fight on terrorism, which would only target people listed by EU State members as potential terrorists. Currently, the data base counts 60 M French citizens.
Since January 2018, the Yvelines department is the first to test smart cameras in 12 buildings, including 6 schools and a town hall, to identify abnormal behaviors, but without using facial recognition. In February 2018, the CNIL authorized Societe Generale's subsidiary, the online banking "Boursorama", to use its fully automated biometric technology (DELIBERATION n°2018-051 du 15 FEVRIER 2018 https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000036659672). Under art. 22 of GPDR, each customer has to give his express consent to the use of the technology and can ask at any moment for an alternative measure of identification. Data are only collected for the time of identification (3 seconds).
In February 2019, the Mayor of Nice has implemented, as experimental for the first time in France, of the use of facial recognition technology in the streets of Nice, for a testing period of the 2 days of Carnival, on the 19th and 20th of the month. The authorization of the CNIL was not required (something to be changed), but the population would be informed of the whole process of this experimentation. The City of Nice counts already 2.350 cameras, one for each 145 inhabitants.

In France, the Data protection Act of 6 January 1978 was applicable and after it the GPDR (General Data Protection Regulation) adopted by the European Parliament and Council of April 27, 2016 (EU Regulation 2016/679) which became fully effective on May, 25, 2018, applicable in the EU and the European Economic Area (EEA). The main principles are the prohibition of free treatment of biometric data (article 9 of the RGPD), the need to collect the consent of the person concerned (article 9-2-a) of the RGPD) and the obligation made to the controller to carry out an impact analysis (article 35 of the RGPD).
Police forces and governmental authorities need an authorization by decree from the State Council, and a favorable vote by the National Commission on Informatics and Liberty (CNIL), before deploying facial recognition technology. For business use, a declaration to the CNIL is necessary of there is no

specific person appointed in the corporation to report to the CNIL. For personal use (smartphone), there is no need of declaration to the CNIL.

In 2013, in the UK, a British authority on the security industry (BSIA) counted 5.9 million surveillance cameras in the country, making the Uk the most surveilled country in the world, with about one camera every 11 people. But experimental facial recognition in the UK is regulated only by a "code of conduct" with no legal value, leaving police forces a free hand on using this technology. It allowed them to achieve some significant arrests.

In the case of Brexit, what would be the applicable legal framework?

How could the EU GPDR regulation be extended and adapted to protect human rights and sensitive data collected out of this technology?

Considering the amount of data collected by enterprises, it has become obligatory to create a system organized to collect and treat these data and to appoint a DPO (Data Protection Officer) who will be responsible for the whole system of information and protection of data. Controllers of personal data must put in place appropriate technical and organizational measures to implement the data protection principles such as:

- Compulsory Register (aim, categories of data, the identified person responsible for the data and who has access to the data)
- The obligation of information and transparency toward the people whose data are collected and processed

On

- Objectives of the data collected
- What legitimates the enterprise to collect the data
- Who is the authorized identified person who have access to the data
- Duration of conservation (5 years after the end of the contractual relationship)
- Modalities under which the person concerned can exercise its right to access the data
- If the data are transferred outside the EU, information about the country and the legal framework that maintains the same level of protection of the data

EU regulation and implemented in France issued a guideline for the new function of DPO (data protection officers) – CNIL (cf in documents).

If faceprints are collected, we should follow the same principles.

A few days ago (February, 14, 2019), as 2 high schools in the south of France (Marseille and Nice) have installed facial recognition technology at the entry of the school to detect outsiders and potential attacks, several associations of human rights have sued them in front of the Administrative Tribunal to constraint them to remove this technology, deemed to be disproportionate with the goals pursued. If no legal framework actually exists or is adopted meanwhile, the tribunal will have to create law accordingly.

## B) **A global ethical issue and concern: toward an international extended "GPDR"?**

Dec, 7, 2018, assessing AI's dangers, Canada and France were calling for a coordinated international debate about ethical standards and the urgent need for regulation. Canada wants to formulate

appropriate policies. Trudeau said at the end of the G7 multi stakeholder Conference on Artificial Intelligence: "*if Canada is to become a world leader on AI, we must also play a lead role in addressing some of the ethical concerns we face in this area and work with France on convincing other nations to join the cause, inviting also China to work on standards and norms for the technology*" .

A coalition of more than 85 activist groups sent letters to Microsoft, Amazon, and Google pressuring them not to sell their facial surveillance technology to the government. In-mid January 2019, Google revealed that it won't sell face recognition for now but said it would be hard to slow its use. Kent Walkers, senior VP of Global Affaires wrote: "*like many technologies, with multiple uses, facial recognition merits careful consideration to ensure its use is aligned with our principles and values and avoid abuse and harmful outcomes*".

Google's Privacy Policy fails however to respect the obligation of information, laid down in section IV of the Data protection directive and gives incomplete or approximate information about the purposes and the categories of data collected.

**Microsoft clearly stated an urgent need for public regulation and corporate responsibilities**. Its leaders initiated talking with technologists, companies, civil society groups, academics and public officials around the world to "*build a floor of responsibility that supports healthy market competition*", within thoughtful government regulation. First to alert the public authorities on the potential misuse and abuses of this technology given the broad societal ramifications, and to call for regulation in July 2018, Microsoft has been working, since then, on a draft of legislation and should submit it in March 2019 to the American Congress as a basis of reflections and proposals.

Indeed, Brad Smith, at the head of Microsoft legal affairs, announced: « *Facial recognition technology raises issues that go to the heart of fundamental human rights protections like privacy and freedom of expression. These issues heighten responsibility for tech companies that create these products. In our view, they also call for thoughtful government regulation and for the development of norms around acceptable uses. In a democratic republic, there is no substitute for decision making by our elected representatives regarding the issues that require the balancing of public safety with the essence of our democratic freedoms. Facial recognition will require the public and private sectors alike to step up – and to act*" (…) "*the world is at risk of a "race to the bottom" as companies are forced to choose between being responsible to society or improving their market share*" (…) "***A world with vigorous regulation of products that are useful but potentially troubling is better than a world devoid of legal standards* ». "*People have to know and trust the government about how this technology will be used well, that people's rights need to be protected***." To ensure transparency on quality of the products, it is advised to test the technology by enabling impartial third-party testing groups and published comparisons of different products**. "**A sensible approach would be to require tech companies that make their facial recognition services accessible using the internet also make available an application programming interface or other technical capability suitable for this purpose".

He also insisted on **companies' responsibilities**, to increase **consumers' confidence**. Indeed, the ability of computer vision gets better and faster in recognizing people's faces in real time and in producing massive ID and sensitive data stored online. **Accuracy and performance of this technology** need to be enhanced to **avoid bias and discrimination** (deficiencies: misinterpretations occur more frequently among women and colored people). Companies must innovate in ways that benefit society and not put other people's lives at risk. They must be encouraged to **collaborate with the academic**

**community and other companies** to ensure to have a diverse and well-trained workforce with the capabilities needed to be effective in reducing risks of bias. A special effort must be made for **transparency with the public and consistency of the products under the UN's guiding principles on business and human rights** (periodical human rights impact assessment) with a lot of listening to stakeholders, including customers, human rights and privacy groups focused on facial recognition technology. For example, governments cannot rely on flawed or biased technological approaches to decide who to track, investigate or even arrest for a crime. In London's carnival experimental approach, facial recognition technology was reported to have only 2% of accuracy.

Microsoft proposed to commit and address new laws based on **6 principles**:

- **Transparency** with the public on the capacities and the limitations of this technology, clear rules for everyone to follow; Legislation should therefore require tech companies that offer facial recognition services to provide documentation that explains the capabilities and limitations of the technology in terms that customers and consumers can understand.
- **Responsibility/accountability** so that this technology is always human centered (for human benefits and related decisions taken by humans. "*New legislation should therefore require that entities that deploy facial recognition undertake meaningful human review of facial recognition results prior to making final decisions for what the law deems to be "consequential use cases" that affect consumers. This includes where decisions may create a risk of bodily or emotional harm to a consumer, where there may be implications on human or fundamental rights, or where a consumer's personal freedom or privacy may be impinged*".
- **Fairness.** All people should be treated fairly, in the same way;
- **Non-discrimination**; It is of paramount importance that companies or entities that deploy facial recognition services are committed to comply with laws prohibiting discrimination against individual consumers or groups of consumers, which reinforce the need for human accountability on control and review for lawful decisions based on the use of facial recognition.
- **Notice and clear prior consent** of the consumer, on the model of the EU GPDR, for the deployment of this technology.
- **Proportionality/lawful surveillance** and limitation in time of the implementation of this technology, collection and use of personal data; Adopt safeguards for people's democratic freedoms in law enforcement surveillance scenarios, and make sure not to deploy facial recognition technology in scenarios that will put these freedoms at risk. (for example, the proportionality to use facial recognition for terrorism purposes or banal thieves or delinquency and suppress almost all privacy?)

**Surveillance compliant with the law and protection of people's privacy.** Imagine every public establishment installs cameras connected to the cloud with real-time facial recognition services. Where is "the right to be let alone", the "right to privacy" if you are recognized by a computer wherever you go? Imagine a mall owner builds-up longer-term histories pieced together over time from multiple cameras at different locations and sells this record of information with every store for predictive purpose and personalized marketing. This would be part of the consumer experience, but it deserves to know when this type of technology is used. New legislation could provide this transparency by ensuring clear notice of use of this technology and make sure that the customer understands it and consent to its use by entering in the premises or proceeding to use online services with this technology. In our opinion, this constraint represents a limitation to the freedom of movement if this technology is generalized in the future. "*Facial recognition services could be subject to background privacy principles, such as limitations on the use of the data beyond the initially defined purposes and the rights of individuals to access and correct their personal data. But from our*

*perspective, this is also an area, perhaps especially in the United States, where this new regulation might take one quick step and then we all can learn from experience before deciding whether additional steps should follow*".

**Protecting democratic freedoms and human rights**

The use of facial recognition technology by a government can severely undermine democratic freedoms and human rights, based on freedom to move and assemble, to meet and discuss views both in private and in public. There is a potential use for facial recognition technology abuse "when combined with ubiquitous cameras and massive computing power and storage in the cloud, a government could use facial recognition technology to enable continuous surveillance of specific individuals. It could follow anyone anywhere, or for that matter, everyone everywhere. It could do this at any time or even all the time. This use of facial recognition technology could unleash mass surveillance on an unprecedented scale". Based on a recent case law (Carpenter v. United Sates – June 2018) depriving the Government any right to track moves through cellular phone without warrant because of privacy rights (4th Amendment to the Constitution), Microsoft recommends that **Government surveillance for specific individuals should be possible in public spaces only if authorized by a court order and when there is an emergency involving imminent danger or risk of death or serious physical injury to a person**.

Other meaningful set of questions raised by Microsoft in the drafting of the legal framework:

- Should law enforcement use of facial recognition be subject to human oversight and controls, including restrictions on the use of unaided facial recognition technology as evidence of an individual's guilt or innocence of a crime?
- Similarly, should we ensure there is civilian oversight and accountability for the use of facial recognition as part of governmental national security technology practices?
- What types of legal measures can prevent use of facial recognition for racial profiling and other violations of rights while still permitting the beneficial uses of the technology?
- Should use of facial recognition by public authorities or others be subject to minimum performance levels on accuracy?
- Should the law require that retailers post visible notice of their use of facial recognition technology in public spaces?
- Should the law require that companies obtain prior consent before collecting individuals' images for facial recognition? If so, in what situations and places should this apply? And what is the appropriate way to ask for and obtain such consent?
- Should we ensure that individuals have the right to know what photos have been collected and stored that have been identified with their names and faces?
- Should we create processes that afford legal rights to individuals who believe they have been misidentified by a facial recognition system?

Microsoft believes that "US lawmakers have an opportunity to blaze a trail that can serve as a model for effective privacy legislation nationwide".

The **American National Telecommunications and Information Administration** also proposed a few guidelines in order to operate an ethical, privacy-protective facial recognition system. It says an entity must embrace the **following principles** (which are derived from well-understood fair information practice principles):

• **Collection**. An entity must receive informed, written, and specific consent from an individual before enrolling him or her in a face recognition database. Enrollment is defined as storage of a faceprint or photograph for the purpose of performing face recognition.
• **Use**. An entity must receive informed, written consent from an individual before using a facial recognition system or faceprint in a manner not covered by existing consent. When an individual consent to the use of a facial recognition system for one purpose, an entity may seek consent from that individual for its use for a secondary purpose. However, the entity may not compel the individual to give that consent. Consent may be withdrawn by the individual at any time. An entity may not use a face recognition system to determine an individual's race, color, religion, sex, national origin, disability or age.
• **Sharing**. A faceprint or any information derived from the operation of a face recognition system may not be sold or shared except with the informed, written consent of the individual whose information is being sold or shared.
• **Access**. An individual must have the right to access, correct, and delete his or her faceprint information. An individual may also access and request correction of information about him or her derived from operation of a face recognition system including information maintained in the audit trail.
• **Misuse**. An entity that maintains publicly accessible data sets linking an individual's identity to a biometric (such as large social networking sites that contain names and photographs) must take all appropriate technical and procedural measures to prevent access to those data sets for the purpose of creating a faceprint database. These measures may include technical degradation of individual images, limiting automated access to relevant databases, and creating contractual obligations binding partners to follow this Ethical Framework.
• **Security**. An entity must keep securely information contained in a face recognition system.
• **Accountability**. An entity must maintain a system which measures compliance with these principles including an audit trail memorializing the collection, use, and sharing of information in a facial recognition system. The audit trail must include a record of date, location, consent verification, and provenance of the faceprint and other data. It must also allow evaluation of the faceprint algorithm for accuracy. This data may also be incorporated in a watermark to ease the ability to audit.
• **Government Access**. An entity must treat a faceprint and other information associated with its collection, use, and sharing as the content of communications. Government access to information from a face recognition system that is not covered by the Privacy Act of 1974 should only be authorized pursuant to a warrant issued with probable cause.
• **Alternatives**. When an entity uses a facial recognition system to authenticate the identity of an individual, a reasonable alternative means of authentication must also be offered to the individual.
• **Children and Teens**. An entity must take special precautions when using a facial recognition system with teens. In providing notice and obtaining informed consent from a teen, the entity must take account of the teen's age and level of understanding. There must be verifiable parental consent for children under 13.
• **Transparency**. An entity must describe its policies for compliance with these principles including the duration it retains data, how the data is used, how the government might access the data, and the necessary technical specifications to verify accountability. An entity must prominently notify individuals when face recognition is in operation.

Signatories to this framework recognize that while voluntary codes of conduct represent an important step in protecting biometric information from exploitation and misuse, it is impossible to protect against the negative effects of this powerful technology fully without government intervention and statutorily created legal protections.

The ultimate goal would be to adopt an international binding and enforceable rule of law that would protect every country from misuse or abuse of its sovereign rights. Although we must ensure that the year 2024 doesn't look like a page from the novel "1984", as Brad Smith said, we are right to wonder if China will also contribute and abide to an international legal framework. World leader on artificial intelligence, there is no barrier in China, whether social, legal or from the media. No law regulates the power of the police, nobody can access to the data collected and potentially used by one of the most powerful dictatorship in the world. How to make sure that the Chinese most advanced technologies in this field will not, if spread in the world, harvest and centralize all data through their software for global surveillance purpose? Beijing plans to be able to identify anyone, anytime, anywhere in China within three seconds. This is not dystopia, but the reality. Not regulating the GAFA "*stunts innovation and ethics in technology where the West is now forced to copy China just to keep up*".

**Bibliography**:


https://www.cnil.fr/fr/la-videosurveillance-videoprotection-sur-la-voie-publique
https://www.washingtonpost.com/gdpr-consent/?destination=%2fopinions%2ffacial-recognition-threatens-our-fundamental-rights%2f2018%2f07%2f19%2fa102703a-8b64-11e8-8b20-60521f27434e_story.html%3f&utm_term=.10b1b86782f8
https://www.youtube.com/watch?v=Fq1SEqNT-7c
https://www.youtube.com/watch?v=eViswN602_k
https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278
https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?noredirect=on&utm_term=.2091200864f5
https://medium.com/@Michael_Spencer/china-goes-full-black-mirror-the-future-of-freedom-31e99215c96f
https://www.hongkongfp.com/2018/02/08/black-mirror-technology-chinese-police-don-high-tech-glasses-nab-suspects/
https://www.news.com.au/technology/online/big-brother-chinas-chilling-dictatorship-moves-to-introduce-scorecards-to-control-everyone/news-story/6c821cbf15378ab0d3eeb3ec3dc98abf
https://www.bbc.com/news/uk-england-london-46584184
https://unitysunday.wordpress.com/2018/02/12/chinese-police-deploy-black-mirror-facial-recognition-scans-using-smart-glasses/
https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?noredirect=on&utm_term=.2091200864f5
https://www.bbc.com/news/uk-england-london-46584184
https://www.bbc.com/news/technology-44089161

https://ainowinstitute.org/
https://symposium.ainowinstitute.org/
https://www.thequint.com/tech-and-auto/tech-news/facial-recognition-tech-smart-cameras-and-glasses-in-india
https://www.narcity.com/news/malls-across-canada-are-using-facial-recognition-technology-to-track-shoppers-and-it-sounds-like-an-episode-of-black-mirror
https://www.abc.net.au/triplej/programs/hack/how-ai-is-using-facial-recognition-to-decipher-your-personality/10025634

https://skift.com/2017/09/14/face-value-the-rise-of-facial-recognition-event-software-meetings-innovation-report/
https://mashable.com/2017/09/13/black-mirror-iphone-x-animojis-waldo-moment/?europe=true
https://psyarxiv.com/hv28a/

https://www.technologyreview.com/s/612499/your-smartphones-ai-algorithms-could-tell-if-you-are-depressed/?utm_campaign=site_visitor.unpaid.engagement&utm_source=hs_email&utm_medium=email&utm_content=69310086&_hsenc=p2ANqtz-92LDZc0podFxOp86ERYzmhjSydHLA4OgHt5a1vw5KakUV9cQ3vqq47QYjzjgdt9lvgxIxWt7r5i5SSP4x9H1F0v3mFks21lwUksSUmDloBZ22Eqeg&_hsmi=69310086
https://www.technologyreview.com/the-download/612606/google-will-stop-providing-face-recognition-but-it-will-be-hard-to-curb-its-use/?utm_campaign=site_visitor.unpaid.engagement&utm_source=hs_email&utm_medium=email&utm_content=69310086&_hsenc=p2ANqtz-92LDZc0podFxOp86ERYzmhjSydHLA4OgHt5a1vw5KakUV9cQ3vqq47QYjzjgdt9lvgxIxWt7r5i5SSP4x9H1F0v3mFks21lwUksSUmDloBZ22Eqeg&_hsmi=69310086
https://www.technologyreview.com/s/612555/canada-and-france-propose-an-international-panel-to-assess-ais-dangers/
https://sputniknews.com/europe/201901201071650120-met-police-facial-recognition-spending-report/

http://nettechnews.com/police-face-legal-action-over-use-of-facial-recognition-cameras/

https://sputniknews.com/europe/201901201071650120-met-police-facial-recognition-spending-report/
https://www.cnil.fr/fr/definition/reconnaissance-faciale
https://www.technologyreview.com/the-download/612606/google-will-stop-providing-face-recognition-but-it-will-be-hard-to-curb-its-use/?utm_campaign=site_visitor.unpaid.engagement&utm_source=hs_email&utm_medium=email&utm_content=69310086&_hsenc=p2ANqtz-92LDZc0podFxOp86ERYzmhjSydHLA4OgHt5a1vw5KakUV9cQ3vqq47QYjzjgdt9lvgxIxWt7r5i5SSP4x9H1F0v3mFks21lwUksSUmDloBZ22Eqeg&_hsmi=69310086
https://www.technologyreview.com/s/612555/canada-and-france-propose-an-international-panel-to-assess-ais-dangers/
https://www.technologyreview.com/s/612552/facial-recognition-has-to-be-regulated-to-protect-the-public-says-ai-report/

https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/
https://www.usine-digitale.fr/article/validation-du-systeme-d-identification-par-reconnaissance-faciale-de-boursorama-par-la-cnil.N677574
https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/
https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/
https://blogs.microsoft.com/on-the-issues/2018/12/10/the-universal-declaration-of-human-rights-an-important-anniversary-for-people-and-for-technology/

https://blogs.microsoft.com/on-the-issues/2017/11/10/need-modernize-international-agreements-create-safer-digital-world/
https://ainowinstitute.org/
https://symposium.ainowinstitute.org/
https://symposium.ainowinstitute.org/conduct
https://www.cnil.fr/fr/reglement-europeen-protection-donnees
https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology
https://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
https://www.technologyreview.com/s/612499/your-smartphones-ai-algorithms-could-tell-if-you-are-depressed/?utm_campaign=site_visitor.unpaid.engagement&utm_source=hs_email&utm_medium=email&utm_content=69310086&_hsenc=p2ANqtz-92LDZc0podFxOp86ERYzmhjSydHLA4OgHt5a1vw5KakUV9cQ3vqq47QYjzjgdt9lvgxIxWt7r5i5SSP4x9H1F0v3mFks21lwUksSUmDloBZ22Eqeg&_hsmi=69310086
https://www.huffingtonpost.fr/2014/03/20/deepface-reconnaissance-faciale-facebook_n_5000872.html
https://www.telegraph.co.uk/technology/2018/12/07/microsoft-president-calls-new-rules-facial-recognition-technology/
https://newmedialaw.proskauer.com/2019/01/31/new-york-city-considers-facial-recognition-bill-will-new-york-be-the-next-forum-for-biometric-privacy-litigation/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=inter-article-link
https://medium.com/futuresin/chinese-facial-recognition-will-take-over-the-world-in-2019-520754a7f966