ANGLAIS

Durée : 3 heures

En vous appuyant *uniquement* sur les documents du dossier thématique qui vous est proposé, vous rédigerez une synthèse répondant à la question suivante :

Facial recognition : to what extent should its use be restricted?

Votre synthèse comportera entre 450 et 500 mots et sera précédée d'un titre. Le nombre de mots rédigés devra être indiqué à la fin de votre copie.

Liste des documents **:**

   1. Facial recognition cameras may bring exit checks to U.S.-Mexico border (San Antonio Express News)

   2. California could become the largest state to ban facial recognition in body cameras (The Washington Post)

   3. The Business of Your Face (Fortune)

   4. survey (Pew Research Center)

   5. cartoon (www.editorialcartoonists.com)

Document 1 – Facial recognition cameras may bring exit checks to U.S.-Mexico border

Lynn Brezosky, San Antonio Express News – Nov 1, 2018

Facial recognition technology that is fast becoming a means to access iPhones, board international flights and even order food may now address a post-9/11 mandate to make sure visitors aren't overstaying their visas.

Competing vendors are testing cameras that capture travelers' images through windshields at the Anzalduas International Bridge in Mission as part of a yearlong trial announced Aug. 29.

"Basically it's a nonobtrusive way to make sure that the person that comes in goes back out," said David Gonzalez, port director for the Hidalgo, Pharr and Anzalduas bridges on the Texas-Mexico border. (…)

Customs and Border Protection (CBP) for years has experimented with biometric technologies such as fingerprinting in 2004 and iris scans in 2010. (…)

Gonzalez, the port director, said the beauty of the program is that it's seamless and does not slow bridge traffic. Asked about privacy concerns and the fear of "Big Brother," he said people have largely moved past that.

"The public has pretty much given that up to almost any other program," he said. "You're giving it up to your iPhone. I think there are now some banking systems that are doing video face capturing. … I mean, they're tracking you already right now at the grocery store to find out how much time you spend in there, what aisles you're going down, where your eyes follow. I've seen all that technology."

CBP already has partnered with airlines on facial recognition systems for some noteworthy results, snagging foreigners with fraudulent passports, previous deportation orders and multiple identities.

But privacy advocates say airports are nothing like land ports and exit checks were never meant to put identities of U.S. citizens into a vast biometric database. There's also evidence that the technology is less effective with people who have darker complexions.

Data breaches at the U.S. Department of Veteran Affairs and U.S. Office of Personnel Management show the government has a poor record of safeguarding privacy, said Jennifer Lynch, a senior staff attorney with the San Francisco-based Electronic Frontier Foundation.

"We don't know that's what's happening with the data," Lynch said. "The government is also partnering with private companies. We don't know what the companies are doing with the data."

The Washington, D.C.-based Electronic Privacy Information Center has urged the federal government to suspend facial recognition at land ports until the benefits are weighed against the 10-year, $1 billion investment and there is public discussion of potential privacy and civil liberties risks.

Document 2 – California could become the largest state to ban facial recognition in body cameras

Reis Thebault, The Washington Post – 11 September 2019

California could soon become the largest state to ban the use of facial-recognition technology in law enforcement body cameras, a milestone in the regulation of the fast-developing but loosely controlled technology.

The state Senate approved the three-year moratorium on Wednesday, sending the legislation back to the Assembly, where it is expected to pass. The ban has earned praise from privacy

and civil rights advocates, who have long argued that the technology could be deployed for mass surveillance and lead to more false arrests.

Assembly member Phil Ting (D), who wrote the bill, said the artificial-intelligence software "isn't ready for prime time," and he predicted it would undermine the police-community relationship.

"Body cameras have been used as a tool to build trust between communities and law enforcement and to provide more transparency," he told The Washington Post. "Putting facial recognition software into those body cameras helps destroy that trust. It turns a tool of transparency and openness into a tool of 24-hour surveillance."

If the legislature passes the bill, it will go to the desk of California Gov. Gavin Newsom (D), whose office told The Post the governor wouldn't comment on pending legislation. The Northern California branch of the American Civil Liberties Union (ACLU) urged the state to enact the law and called for the rest of the country to follow suit.

"Face-scanning police body cameras have no place on our streets, where they can be used for dragnet surveillance of people going about their private lives, including their locations and personal associations," Matt Cagle, the Northern California branch's technology and civil liberties attorney, said in a statement.

But the legislation has also faced ardent opposition from some law enforcement groups — particularly the influential and well-funded California Peace Officers' Association, which included Ting's bill on its list of proposed laws that "threatens the future of effective policing and crime reduction."

Police unions argue that any barrier to the technology could threaten public safety and leave agencies without the best, most up-to-date equipment for securing marquee events, such as the 2028 Olympics in Los Angeles, and annual festivities such as the Coachella music festival and the Rose Bowl.

"By banning this technology, California will be announcing to the nation and world that it doesn't want our law enforcement officers to have the necessary tools they need to properly protect the public and attendees of these events," the Riverside Sheriff's Association wrote in a statement on the legislation. (…)

Ting represents parts of San Francisco, which in May became the country's first city to issue a total ban on facial-recognition software by local agencies and police. Oakland, Calif., and Somerville, Mass., banned the technology soon after. New Hampshire and Oregon both have laws on the books similar to Ting's bill.

However, there are no federal laws governing the use of facial recognition nationwide, and more than 50 state or local police agencies across the country have at some point used the technology in attempts to identify criminal suspects or verify identities.

Such regulation could pressure Amazon and other companies that have sought to sell facial-recognition technology to police agencies. In May, Amazon's shareholders rejected proposals that would have asked the company to stop selling Rekognition, its software, to the government.

But other companies — including body camera manufacturer Axon — have self-regulated. Microsoft's president, Brad Smith, has even urged Congress to regulate the technology, saying companies should not be left to police themselves because of the technology's "broad societal ramifications and potential for abuse."

The ACLU recently put Rekognition's software to the test, using it to compare pictures of California lawmakers against a database of 25,000 mug shots. The group found about 20 percent of legislators were incorrectly matched to someone who had been arrested.

Among those mixed up: Assembly member Ting.

Document 3 – The Business of Your Face

Jeff John Roberts, Fortune, March 27, 2019

Facial recognition software is a powerful technology that poses serious threats to civil liberties. It's also a booming business. Today, dozens of startups and tech giants are selling face recognition services to hotels, retail stores—even schools and summer camps. The business is flourishing thanks to new algorithms that can identify people with far more precision than even five years ago. (…)

As more companies start to sell facial recognition, and as our faces end up in more databases, the software could catch on with voyeurs and stalkers. Merchants and landlords could also use it to identify those they deem to be undesirable, and quietly withhold housing or services. (…)

There's also the risk of hacking. Andrei Barysevich of Gemini Advisors, a cybersecurity firm, says he has seen profiles stolen from India's national biometrics database for sale on "dark web" Internet sites. He has yet to see databases of American faces for sale, but added, "It's just a matter of time." If such a thing were to occur, a stolen collection of customer faces from a hotel or retailer could help criminals carry out fraud or identity theft.

As the technology spreads with little government oversight, the best hope to limit its misuse may lie with the software makers themselves. In interviews with *Fortune*, the CEOs of facial recognition startups all stated they were deeply attuned to privacy perils. A number, including Peter Trepp, the CEO of FaceFirst (a California-based facial recognition company that helps retailers screen for criminals entering their stores), cited the spread of face surveillance systems in China as a cautionary tale.

(…) At the same time, Trepp of FaceFirst believes anxiety over the technology will diminish as we become more familiar with it. He even argues that facial recognition scenes in the 2002 sci-fi movie *Minority Report* will start to feel normal.

"Millennials are much more willing to hand over their face. That [*Minority Report*] world is coming," he says. "Done properly, I think people are going to enjoy it and it's going to be a positive experience. It won't feel creepy."

Others, including the American Civil Liberties Union (ACLU), are less sanguine. Still, despite the growing controversy around the technology, there is, for now, almost nothing in the way of laws to limit the use of your face. (…) At the federal level, lawmakers have so far devoted little attention to the matter. This may be changing, however, as Senators Brian Schatz (D-Ha.) and Roy Blount (R.MO) this month introduced a bill that would require companies to get permission before using facial recognition in public places and or share face data with third parties.
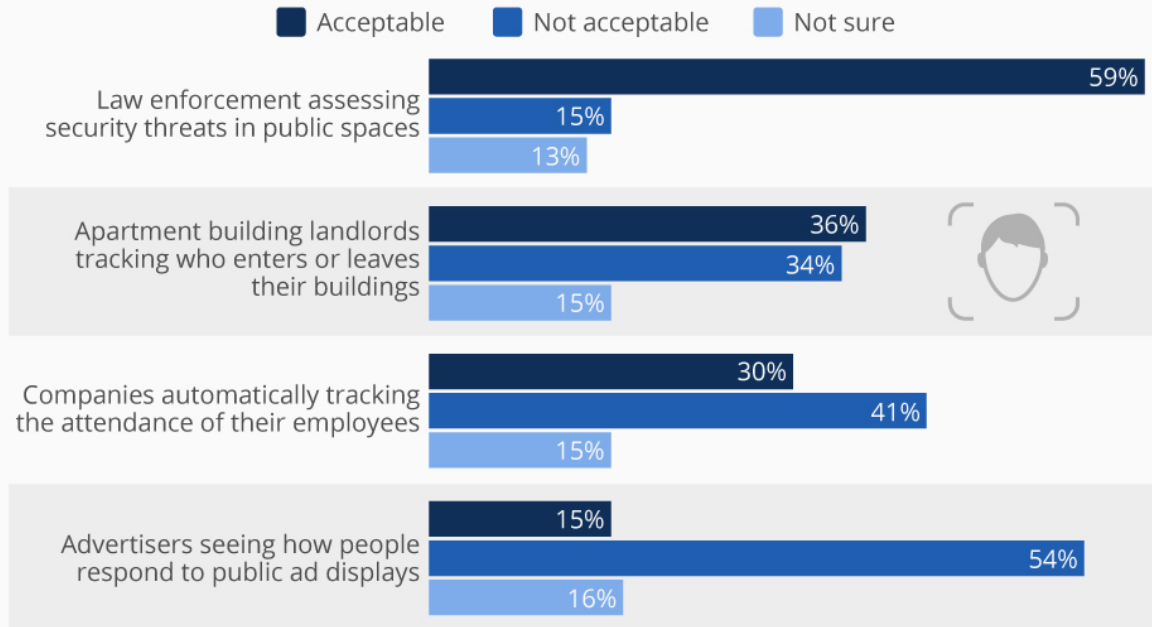
Clare Garvie, a Georgetown University professor who published an influential report on facial recognition technology, is in favor of laws to oversee the technology. But she says it has been difficult for lawmakers to keep up.

"One challenge of facial recognition is it's been incredibly quick on the uptake because of legacy databases. There are so many instances where our faces were captured," she says. "Unlike fingerprints, where there have long been rules on how and when they're collected, there are no rules for face technology."

Document 4 – 2019 survey by Pew Research Center

Americans Accept Face Recognition for Public Safety
% of U.S. adults who say the use of facial recognition tech in the following situation is...

■ Acceptable ■ Not acceptable ■ Not sure

Law enforcement assessing security threats in public spaces
- Acceptable: 59%
- Not acceptable: 15%
- Not sure: 13%

Apartment building landlords tracking who enters or leaves their buildings
- Acceptable: 36%
- Not acceptable: 34%
- Not sure: 15%

Companies automatically tracking the attendance of their employees
- Acceptable: 30%
- Not acceptable: 41%
- Not sure: 15%

Advertisers seeing how people respond to public ad displays
- Acceptable: 15%
- Not acceptable: 54%
- Not sure: 16%

Results do not add up to 100% because 13% of U.S. adults have not heard of facial recognition. 4,272 people were surveyed between June 3-17, 2019.
Source: Pew Research Center
@StatistaCharts   statista

Document 5 - www.editorialcartoonists.com – September 17, 2019

TSA = Transportation Security Administration