



Center for AI and
Digital Policy

AISCI-2020: Facial Recognition

REPORT ON FACIAL RECOGNITION

summarizing

ARTIFICIAL INTELLIGENCE AND
DEMOCRATIC VALUES: ARTIFICIAL
INTELLIGENCE SOCIAL CONTRACT
INDEX 2020

(February 2020)

Table of Contents

FOREWORD – Gov. Michael Dukakis	1
Findings	1
Recommendations.....	1
The Global AI Policy Landscape	1
Belgium.....	3
Facial Recognition.....	3
Brazil	4
Facial recognition	4
Evaluation	5
China.....	5
Facial Recognition.....	5
AI and Surveillance	5
France	6
Facial Recognition.....	6
Germany	7
Facial Recognition.....	7
Israel	8
Facial recognition	8
Evaluation	8
Facial Recognition.....	9
Japan.....	9
Facial Recognition.....	9
Evaluation	10
Kazakhstan.....	10
Facial Recognition and Smart Cities.....	10
Russia.....	11
Facial Recognition Controversy	11
Evaluation	12
Sweden	12
Facial recognition	12
Taiwan	13

Facial Recognition.....	13
Evaluation.....	14
Thailand	14
Evaluation.....	14
United Kingdom.....	14
Facial Recognition.....	14
United States	15
Facial Recognition.....	15
Evaluation.....	16

[NOTE – This CAIDP Special Report on Facial Recognition excerpts key references to facial recognition contained in the 2020 report *Artificial Intelligence and Democratic Values / The AI Social Contract Index 2020*, prepared by the Center for AI and Digital Policy. This summary and other related materials will be found at <https://caidp.dukakis.org/aisci-2020/>]

FOREWORD – Gov. Michael Dukakis

“We must recognize that the choices about AI carry real consequences for the rights and freedoms of citizens. We already see how authoritarian governments can use AI techniques to monitor social protest through facial recognition and analysis of communications and travel records. And once these systems are established, they will be difficult to dismantle. World leaders will need to speak clearly about the need to protect democratic values even as they promote this new technology.”¹

Findings

Facial Surveillance as an AI “Red Line.” Few AI applications are more controversial than the use of AI for surveillance in public spaces. The use of facial recognition on a general population has raised widespread controversy with many NGOs stating it should be prohibited. Other controversial AI applications include the scoring of citizens, criminal sentencing, administrative service decisions, and hiring assessments.²

Recommendations

1. Countries must establish national policies for AI that implement democratic values
2. Countries must ensure public participation in AI policymaking and also create robust mechanisms for independent oversight of AI systems
3. Countries must guarantee fairness, accountability, and transparency in all AI systems
4. **Countries must commit to these principles in the development, procurement, and implementation of AI systems for public services**
5. **Countries must halt the use of facial recognition for mass surveillance³**

The Global AI Policy Landscape

Following the U.S. election in November 2020, the European Commission developed a new framework for transatlantic relations. On December 2, 2020, the European Commission proposed a New EU-US Agenda for Global Change. The New Agenda covers a wide range of topics, but it is notable that the Commission states, “we need to start acting together on AI - based on our shared belief in a human- centric approach and dealing with issues such as facial

1 Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, iii, December 2020, <https://caidp.dukakis.org/aisci-2020/>

2 Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 2, December 2020, <https://caidp.dukakis.org/aisci-2020/>

3 Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 4, December 2020, <https://caidp.dukakis.org/aisci-2020/>

recognition. In this spirit, the EU will propose to start work on a **Transatlantic AI Agreement** to set a blueprint for regional and global standards aligned with our values.”⁴⁵

The influential LIBE Committee has also highlighted concerns about AI and fundamental rights and AI in criminal justice.⁶ In February 2020, the Committee held a hearing on Artificial Intelligence and Criminal Law, and examined the benefits and risks of AI, predictive policing, facial recognition, as well as the ethical and fundamental rights implications. LIBE worked in association with the United Nations Interregional Crime and Justice Research Institute (UNICRI), the European Union Agency for Fundamental Rights (FRA), and the Council of Europe (COE). In November 2020, LIBE issued an opinion concerning on AI and the application of international law.⁷⁸

In a June 2020 letter to several members of the European Parliament about facial recognition and the company ClearView AI, EDPB Chair Jelinek stated “Facial recognition technology may undermine the right to respect for private life and the protection of personal data . . . It may also affect individuals’ reasonable expectation of anonymity in public spaces. Such technology also raises wider issues from an ethical and societal point of view.” But Jelinek failed to state whether the use of facial recognition in public spaces was permissible under the GDPR.⁹¹⁰

The European Data Protection Supervisor also expressed support for a moratorium on facial recognition in public space, “so that an informed and democratic debate can take place and until the moment when the EU and Member States have all the appropriate safeguards.”¹¹

In 2020, the Global Privacy Assembly also adopted a Resolution on Facial Recognition Technology.¹² The GPA Resolution reiterated several key principles for data protection, such as fairness and transparency, but stopped short of endorsing a formal ban which had been urged by many human rights advocates at the 2019 conference in Tirana. More than 100 organizations and 1,200 experts recommended that “countries suspend the further deployment of facial recognition technology for mass surveillance” and “establish the legal rules, technical standards, and ethical guidelines necessary to safeguard fundamental rights and comply with legal obligations before further deployment of this technology occurs.” The Assembly said it would consider the “circumstances when facial recognition technology poses

4 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the European Council and the Council: A New EU-US Agenda for Global Change (Dec. 2, 2020) (emphasis in the original), https://ec.europa.eu/info/sites/info/files/joint-communication-eu-us-agenda_en.pdf

5 Center for AI and Digital Policy, Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020, p. 9, December 2020, <https://caidp.dukakis.org/aisci-2020/>

6 CAIDP Update 1.8 LIBE Committee of EU Parliament Examines AI Practices, Data Protection, (Sept. 9, 2020), <https://dukakis.org/center-for-ai-and-digital-policy/caidp-update-libe-committee-of-eu-parliament-examines-ai-practices-data-protection/>

7 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013 (INI)), (Nov. 23, 2020), https://www.europarl.europa.eu/doceo/document/LIBE-AD-652639_EN.pdf

8 Center for AI and Digital Policy, Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020, p. 10, December 2020, <https://caidp.dukakis.org/aisci-2020/>

9 EDPB Letter Members of the European Parliament (OUT2020-0052) (June 10, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf

10 Center for AI and Digital Policy, Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020, p. 14, December 2020, <https://caidp.dukakis.org/aisci-2020/>

11 Center for AI and Digital Policy, Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020, p. 14, December 2020, <https://caidp.dukakis.org/aisci-2020/>

12 Global Privacy Assembly, *Adopted Resolution on Facial Recognition Technology* (Oct. 2020), <https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Facial-Recognition-Technology-EN.pdf>

the greatest risk to data protection and privacy rights,” and develop a set of principles that could be adopted at the next conference.¹³

In 2020, in response to growing concerns about the use of facial recognition technologies in public spaces, ACM, an international society of computer scientists and professionals, released a statement addressing the unique issues of biometric data systems and the potential bias and inaccuracies that have significant consequences for violation of human rights.¹⁴¹⁵

In the fall of 2020, more than a dozen NGOs in Europe joined together to ban biometric mass surveillance.¹⁶ The Reclaim Your Face coalition demands “transparency, red lines, and respect for humans,” and has specifically objected to the deployment of facial recognition in Belgrade. According to the organizations, “ReclaimYourFace is a European movement that brings people’s voices into the discussion around biometric data used to monitor the population. We question why these sensitive data are being used and raise the alarm on the impact on our freedoms in public spaces.”¹⁷¹⁸

Fight for the Future, an independent NGO, organized a national campaign in the US to ban facial recognition.¹⁹ Amazon also came under widespread criticism from many US NGOs in 2018 about the company’s facial recognition system Rekognition.²⁰ In June 2020, Amazon agreed to “pause” the police use of its facial recognition software.²¹ IBM and Microsoft also agree to halt the development of facial recognition. According to MIT Technology Review, the decision “mark[s] a major milestone for researchers and civil rights advocates in a long and ongoing fight over face recognition in law enforcement.”²²²³

Belgium

Facial Recognition

According to AlgorithmWatch, the Belgian government is using AI for facial recognition at the Brussels Airport, at school registrations, football matches, and for healthcare.²⁴ A “smart” video surveillance system is also in use to locate criminals, solve theft cases and collect

¹³ Center for AI and Digital Policy, Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020, p. 18 & 19, December 2020, <https://caidp.dukakis.org/aisci-2020/>

¹⁴ ACM, US Technology Policy Committee, *Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies* (June 30, 3030), <https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf>

¹⁵ Center for AI and Digital Policy, Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020, p. 27, December 2020, <https://caidp.dukakis.org/aisci-2020/>

¹⁶ Reclaim Your Face, <https://reclaimyourface.eu>

¹⁷ Reclaim Your Face, The Movement, <https://reclaimyourface.eu/the-movement/>

¹⁸ Center for AI and Digital Policy, Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020, p. 29, December 2020, <https://caidp.dukakis.org/aisci-2020/>

¹⁹ Fight for the Future, *Ban Facial Recognition*, <https://www.banfacialrecognition.com>

²⁰ *Letter from Nationwide Coalition to Amazon CEO Jeff Bezos Regarding Rekognition* (June 18, 2018), <https://www.aclu.org/letter-nationwide-coalition-amazon-ceo-jeff-bezos-regarding-rekognition>

²¹ Karen Weise and Natasha Singer, *Amazon Pauses Police Use of Its Facial Recognition Software*, New York Times (June 10, 2020), <https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html>

²² Karen Hao, *The two-year fight to stop Amazon from selling face recognition to the police*, MIT Technology Review (June 12, 2020), <https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/>

²³ Center for AI and Digital Policy, Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020, p. 30, December 2020, <https://caidp.dukakis.org/aisci-2020/>

²⁴ AlgorithmWatch, *Automating Society 2020*, (Oct. 2020), <https://automatingsociety.algorithmwatch.org/report2020/belgium/>

statistical information. According to AlgorithmWatch, there is no legal framework governing this activity by police. The Belgian Oversight Body for Police Information (COC) has criticized the use of facial recognition at the Brussels airport, stating that there is “too little information about the implementation and risks of the technology as there was no clear policy or data protection impact assessment conducted to come to a conclusion or offer advice.” They are asking for a temporary ban of the pilot project.²⁵²⁶

Brazil

Facial recognition

Facial Recognition is implemented by both the public and private sectors in Brazil. According to *Instituto Igarapé*, a Brazilian think tank, there were at least 48 facial recognition applications throughout 16 Federal States between 2011 to 2019.²⁷ The main use sectors are (i) public security, (ii) border control, (iii) transportation and (iv) education.²⁸

In August 2018, the Brazilian Institute of Consumer Protection (IDEC) filed a public civil action²⁹ for breach of privacy and consumer legislation against the São Paulo Metro operator, regarding an AI crowd analytics system that claimed to predict the emotion, age, and gender of metro passengers without processing personal data.³⁰ The operator was ordered to stop collecting data and remove the cameras, but the case moved forward, and a decision is now expected to be made soon.

Another monitoring system with facial recognition to be installed in the São Paulo subway network is being challenged in Court. Early 2020, the operating company was requested to provide clarifications on risk and impact assessment expected with the implementation of the new technology, on how personal data will be processed, on technical databases and security systems issues, and on actions to mitigate the potential risk of a data breach.³¹

The Brazilian police has also been using live facial recognition for Carnival with now plans to use the technology in events involving crowds to find wanted criminals. In 2020, police forces rolled out facial recognition in six capitals across the country. When announcing the use of live facial recognition, the São Paulo police said a "situation room" would monitor the images from the cameras, which are then compared with a database managed by a biometrics lab.

²⁵ COC, *Visitatie-Toezichtrapport Executive Summary Publieke Versie, 2020*,

https://www.contrôleorgaan.be/files/DIO19005_Onderzoek_LPABRUNAT_Gezichtsherkenning_Publiek_N.PDF

²⁶ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 45, December 2020, <https://caidp.dukakis.org/aisci-2020/>

²⁷ Instituto Igarapé, *Facial Recognition in Brazil*, <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/> (“Facial recognition became especially popular in 2019. The year began with the announcement of a PSL delegation to China to acquire the technology.”)

²⁸ Thiago Moraes, *Facial Recognition in Brazil*, *Wired* (Nov. 20, 2019), <https://medium.com/@lapinbr/face-recognition-in-brazil-f2a23217f5f7>

²⁹ Instituto Brasileiro de Defesa do Consumidor (Aug. 30, 2018), https://idec.org.br/sites/default/files/acp_viaquatro.pdf.

³⁰ AccessNow, *Facial recognition on trial: emotion and gender “detection” under scrutiny in a court case in Brazil* (June 29, 2020), <https://www.accessnow.org/facial-recognition-on-trial-emotion-and-gender-detection-under-scrutiny-in-a-court-case-in-brazil/>

³¹ Tozzini Freire, *Facial Recognition is Disputed in Court* (Feb. 14, 2020), <https://tozzinifreire.com.br/en/boletins/facial-recognition-is-disputed-in-court>

According to the police, the aim is to reduce the likelihood of mistakes, such as wrongly arresting people.³²³³

Evaluation

Brazil does not yet have a national strategy for AI. Brazil has endorsed the OECD/G20 AI Principles and has promoted public participation in the development of AI policy. Brazil has established a comprehensive law for data protection and has a fairly good record on human rights. But the growing use of facial recognition and the absence of new safeguards for AI systems are matters of concern. Consumer groups have objected to the use of AI crowd analytics on metro passengers.³⁴

China

Facial Recognition

There are many reports on China's use of facial recognition technology against ethnic minorities.³⁵ The discriminatory ways in which state organs, companies and academics have researched, developed and implemented facial recognition in China would seem not to comply with the OECD AI Principles or as the Governance Principles for the New Generation Artificial Intelligence. The deployment of facial recognition has also provoked opposition within China.³⁶³⁷

AI and Surveillance

As early as the 2008 Beijing Olympics, China began to deploy new technologies for mass surveillance.³⁸ China put in place more than two million CCTV cameras in Shenzhen, making it the most watched city in the world.³⁹ In recent years the techniques for mass surveillance have expanded rapidly, most notably in Shenzhen, also to oversee the Muslim minority group the Uyghurs, and in Hong Kong. Modern systems for mass surveillance rely on AI techniques for such as activities as facial recognition, communications analysis and location tracking. As one industry publication has reported, "In the world of surveillance, no country invests more in its AI-fueled startups and growth-stage businesses than China. And no technology

³² Angelica Mari, *Brazilian police introduces live facial recognition for Carnival*, Brazil Tech (Feb. 25, 2020), <https://www.zdnet.com/article/brazilian-police-introduces-live-facial-recognition-for-carnival/>

³³ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 54-56, December 2020, <https://caidp.dukakis.org/aisci-2020/>

³⁴ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 56 & 57, December 2020, <https://caidp.dukakis.org/aisci-2020/>

³⁵ Joi Ito, *My talk at the MIT-Harvard Conference on the Uyghur Human Rights Crisis* (May 2, 2019), <https://joi.ito.com/weblog/2019/05/02/my-talk-at-the-.html>

³⁶ Seungha Lee, *Coming into Focus: China's Facial Recognition Regulations*, Center for Strategic and International Studies (May 4, 2020), <https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations>

³⁷ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 69, December 2020, <https://caidp.dukakis.org/aisci-2020/>

³⁸ EPIC/Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (2006) (Report on People's Republic of China), http://www.worldii.org/int/journals/EPICPrivHR/2006/PHR2006-People_s.html

³⁹ Naomi Wolf, *China's All-Seeing Eye With the help of U.S. defense contractors, China is building the prototype for a high-tech police state. It is ready for export*, Rolling Stone (May 15, 2018), <https://www.commondreams.org/views/2008/05/15/chinas-all-seeing-eye>

epitomises this investment more than facial recognition—a technology that courts more controversy than almost any other.”⁴⁰⁴¹

Protests in Hong Kong over the use of facial surveillance are widespread. Umbrellas once used to deflect pepper spray, are now deployed to shield protester activities from the digital eyes of cameras.⁴² It is notable that the battle over the use of facial surveillance in Hong Kong began with widespread public protests about a national security law that extended police authority over the semi-autonomous region.⁴³ According to the AP, “Young Hong Kong residents protesting a proposed extradition law that would allow suspects to be sent to China for trial are seeking to safeguard their identities from potential retaliation by authorities employing mass data collection and sophisticated facial recognition technology.”⁴⁴ China is also exporting the model of mass surveillance by facial recognition to other parts of the world.⁴⁵⁴⁶

France

Facial Recognition

Facial recognition is a processing of sensitive personal data prohibited in principle by the GDPR and the French data protection law, subject to exceptions such as individual’s consent or for important public interests. In the latter case, facial recognition can be authorized by a Decree of the Conseil d’État informed by an opinion from the CNIL.

Facial recognition has long been used in France, on a voluntary basis, for passport control in airports. Facial recognition is also implemented in some banks and tested in a number of colleges. The French government is considering the deployment of facial recognition for access to public services. The ID program, called Alicem,⁴⁷ to be deployed in November 2019, was however put on hold following an appeal of NGOs to the Conseil d’État requesting the annulment of the decree authorizing its creation. Early November, the Conseil d’État dismissed the appeal.⁴⁸

⁴⁰ Zak Doffman, *Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine* (Aug. 26, 2019),

<https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/>

⁴¹ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 72, December 2020, <https://caidp.dukakis.org/aisci-2020/>

⁴² Paul Mozur and Lin Qiqing, *Hong Kong Takes Symbolic Stand Against China's High-Tech Controls*, *New York Times* (Oct. 3, 2019), <https://www.nytimes.com/2019/10/03/technology/hong-kong-china-tech-surveillance.html>

⁴³ BBC, *Hong Kong security law: What is it and is it worrying?* (June 30, 2020), <https://www.bbc.com/news/world-asia-china-52765838>

⁴⁴ Christopher Bodeen, *Hong Kong protesters wary of Chinese surveillance technology* (June 13, 2019), <https://apnews.com/article/028636932a874675a3a5749b7a533969>

⁴⁵ Ross Anderson, *The Panopticon is Already Here*, *The Atlantic* (Sept. 2020), <https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/>

⁴⁶ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 73, December 2020, <https://caidp.dukakis.org/aisci-2020/>

⁴⁷ <https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee> (in French) - ; Charlotte Jee, *France plans to use facial recognition to let citizens access government services*, *MIT Technology Review* (Oct. 3, 2020), <https://www.technologyreview.com/2019/10/03/132776/france-plans-to-use-facial-recognition-to-let-citizens-access-government-services/>

⁴⁸ Marion Garreau, *Le ministère de l'Intérieur va pouvoir lancer l'application Alicem, basée sur la reconnaissance faciale*, *L'Usine Nouvelle* (Nov. 5, 2020), <https://www.usinenouvelle.com/editorial/le-ministere-de-l-interieur-va-pouvoir-lancer-l-application-alicem-basee-sur-la-reconnaissance-faciale.N1024754>

In November 2019, the CNIL published guidance on the use of facial recognition.⁴⁹ The document, primarily directed at public authorities in France that want to experiment with facial recognition, presents the technical, legal and ethical elements that need to be considered.

After recalling that facial recognition, experimental or not, must comply with the European GDPR and the "police justice" directive, the CNIL sets out three general requirements: (1) facial recognition can only be used if there is an established need to implement an authentication mechanism that ensures a high level of reliability, and there are no other less intrusive means that would be appropriate ; (2) the experimental use of facial recognition must respect the rights of individuals (including consent and control, transparency and security); and (3) the use of facial recognition on an experimental basis must have a precise timeline and be based on a rigorous methodology setting out the objectives pursued and the criteria for success. In December 2019, the Observatoire des Libertés Numériques⁵⁰ and 80 organisations signed an open letter calling on the French Government and Parliament to ban any present and future use of facial recognition for security and surveillance purposes.⁵¹

Earlier this year the administrative tribunal of Marseille rendered a decision on facial recognition that ruled illegal a decision by the South-East Region of France (Provence-Alpes-Côte d'Azur) to test facial recognition at the entrance of two High schools.⁵² Following an analysis from the CNIL,⁵³ the court ruled that there was no opportunity for free and informed consent and also that there were other, less intrusive means to manage entrance to high schools. The French NGO La Quadrature du Net brought the successful challenge to the regional program.⁵⁴ This was the first decision ever by a court applying the General Data Protection Regulation (GDPR) to Facial Recognition Technologies (FRTs).⁵⁵

In 2020, real-time facial recognition on public roads in France is still not authorized. However, many experiments are already taking place, and companies are positioning themselves, with the Olympic Games in Paris in 2024 in their sights, and a market of seven billion euros at stake.⁵⁶⁵⁷

Germany

Facial Recognition

⁴⁹ CNIL, *Reconnaissance faciale - pour un débat à la hauteur des enjeux* (Nov. 2020), https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf (in French).

⁵⁰ The Observatoire des Libertés Numériques federates several French NGOs monitoring legislation impacting digital freedoms: Le CECIL, Creis-Terminal, Globenet, La Ligue des Droits de l'Homme (LDH), La Quadrature du Net (LQDN), Le Syndicat des Avocats de France (SAF), Le Syndicat de la Magistrature (SM).

⁵¹ *Joint Letter from 80 organisations: Ban Security and Surveillance Facial Recognition* (Dec. 19, 2019), <https://www.laquadrature.net/en/2019/12/19/joint-letter-from-80-organisations-ban-security-and-surveillance-facial-recognition/>

⁵² Tribunal Administratif de Marseille, *La Quadrature du Net*, No. 1901249 (27 Nov. 2020), https://forum.technopolice.fr/assets/uploads/files/1582802422930-1090394890_1901249.pdf

⁵³ CNIL, *Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position* (Oct. 29, 2019), <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position>

⁵⁴ La Quadrature du Net, *First Success Against Facial Recognition in France* (Feb. 27, 2020), <https://www.laquadrature.net/en/2020/02/27/first-success-against-facial-recognition/>

⁵⁵ AI Regulation, *First Decision of a French Court Applying GDPR to Facial Recognition* (Feb. 27, 2020), <https://ai-regulation.com/first-decision-ever-of-a-french-court-applying-gdpr-to-facial-recognition/>

⁵⁶ France Culture, *Quand la reconnaissance faciale en France avance masquée* (Sept. 4, 2020), <https://www.franceculture.fr/societe/quand-la-reconnaissance-faciale-en-france-avance-masquee>

⁵⁷ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 91-93, December 2020, <https://caidp.dukakis.org/aisci-2020/>

In 2018 facial recognition technology at a large crossing in Berlin, set up by the government, sparked opposition from civil society.⁵⁸ There was further outcry in 2020, when *Der Spiegel* wrote that there are plans to set up cameras capable of identifying people at 134 train stations and 14 airports.⁵⁹⁶⁰

Israel

Facial recognition

Facial Recognition in Israel is implemented in border control and Israel has a biometric database of face photos and fingerprints of citizens and residents, as well as foreigners accessing Israel. A biometric database was enacted in law in 2009.⁶¹ The law provides the basis for the Israeli national ID-Card. The database includes biometric face-photos, and voluntary supplied fingerprints. According to the biometric database law, the information can be used for severe crime enforcement, and for state security tasks. In May 2020 the Israeli State Comptroller reported that the data of about 4.5 million Israeli drivers' licenses, including facial pictures, are not sufficiently protected from misuse or outside hacking.⁶²

Still, Israel's military has invested tens of millions of dollars to upgrade West Bank checkpoints with AnyVision facial recognition technology to verify Palestinian workers' identities and ease their entry into Israel. The new system, which began rolling out late 2018, drew criticism about the role the controversial technology plays in Israel's military control over Palestinians.⁶³

Microsoft, which was part of a group that had invested \$74 million in AnyVision, hired a team of lawyers to audit the Israeli firm and determine whether AnyVision's technology applications complied with Microsoft's ethical principles against using facial recognition for mass surveillance. In March 2020, Microsoft said it was pulling investments from AnyVision although the outcomes of the audit did not substantiate claims that the startup's technology was used unethically.⁶⁴⁶⁵

Evaluation

The current circumstances of Israel's AI policies and practices are confusing and complex. Although Israel is a leader in AI research and development, efforts to develop a coherent

⁵⁸ Janosch Delcker, *Big Brother in Berlin*, Politico (Sept. 13, 2018), <https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/>

⁵⁹ Phillipp Grüll, *Germany's plans for automatic facial recognition meet fierce criticism*, Euractiv (Jan. 10, 2020), <https://www.euractiv.com/section/data-protection/news/german-ministers-plan-to-expand-automatic-facial-recognition-meets-fierce-criticism/>

⁶⁰ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 101, December 2020, <https://caidp.dukakis.org/aisci-2020/>

⁶¹ Wikipedia, *Biometric Database Law*, https://en.wikipedia.org/wiki/Biometric_Database_Law

⁶² The Jerusalem Post, *4.5 million citizens' details insufficiently protected, comptroller says* (May 4, 2020), <https://www.jpost.com/Israel-News/45-million-citizens-details-insufficiently-protected-comptroller-says-626847>

⁶³ Daniel Estrin, *Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, But Raises Concerns* (Aug. 22, 2019), <https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc>

⁶⁴ Matt O'Brien, *Microsoft divests from Israeli facial-recognition startup* (March 28, 2020), <https://www.timesofisrael.com/microsoft-divests-from-israeli-facial-recognition-startup/>

⁶⁵ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 129, December 2020, <https://caidp.dukakis.org/aisci-2020/>

national AI strategy have stalled. There is good work underway on AI ethics and a well-established legal system for data protection, but the general population tracking for sensitive medical condition by the internal security agency with AI technique is of concern. Also troubling is the use of facial recognition technology without clear legal basis and the reluctance to support limits on lethal autonomous weapons. Israel has endorsed the OECD AI principles, and works in cooperation with other countries on AI policy, but has not yet expressed support for the Universal Guidelines for AI or the Social Contract for the Age of AI.⁶⁶

Italy

Facial Recognition

According to Privacy International, the municipality of Como, Italy, purchased a facial recognition system “with little transparency and despite the lack of a clear legal framework.”⁶⁷ Privacy International reported that Como “embraced a narrative of technological innovation pushed by Huawei” within the broader concept of smart city and innovation tech, but was forced, after the intervention of the Italian Data Protection Authority, to suspend the system. The Garanti determined that there was no legal basis to collect facial images. Subsequent reporting by Wired indicated that the municipality had changed vendors and also that the system installed most recently failed to work as proposed.⁶⁸ In September 2020, AlgorithmWatch also reported that Italy is exploring the use of facial recognition in football stadiums.⁶⁹

Japan

Facial Recognition

Japan has deployed facial recognition in several sectors, including transportation, banking (ATMs), police and immigration. According to Japan Times, Japan plans to use facial recognition technology, originally intended for security purposes, to prevent the spread of the novel coronavirus when it hosts the Tokyo Olympics and Paralympics in 2021.⁷¹ Osaka Metro Co. has developed automated ticket gates with facial recognition with a view to equip all metro stations in Osaka by 2024, ahead of the 2025 World Expo.⁷³ Likewise, the Japanese

⁶⁶ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 131, December 2020, <https://caidp.dukakis.org/aisci-2020/>

⁶⁷ Privacy International, *How facial recognition is spreading in Italy: the case of Como* (Sept. 17, 2020), <https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como>

⁶⁸ Laura Carrer, *The Municipality of Como has discovered that his facial recognition system is not what he had bought: The testing of the video surveillance system with facial recognition revealed inconsistencies and discrepancies with the tender specifications* (Sept. 28, 2020), <https://www.wired.it/attualita/tech/2020/09/28/como-riconoscimento-facciale-collaudato/>

⁶⁹ AlgorithmWatch, *In Italy, an appetite for face recognition in football stadiums* (Sept. 16, 2020), <https://algorithmwatch.org/en/story/italy-stadium-face-recognition/>

⁷⁰ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 140 & 141, December 2020, <https://caidp.dukakis.org/aisci-2020/>

⁷¹ The Japan Times, *Facial Recognition*, <https://www.japantimes.co.jp/tag/facial-recognition>.

⁷² Find Biometrics, *Japan to Pair Face Recognition with Mask and Temperature Detection During Tokyo Olympic* (Oct. 22, 2020), <https://findbiometrics.com/japan-pair-face-recognition-mask-temperature-detection-during-tokyo-olympics-102209/>

⁷³ The Japan Times, *Osaka Metro unveils ticket gate with facial recognition tech* (Dec. 10, 2019), <https://www.japantimes.co.jp/news/2019/12/10/business/corporate-business/osaka-metro-facial-recognition/#:~:text=on%20Tuesday%20started%20testing%20a,around%201%2C200%20Osaka%20Metro%20employees>.

Ministry of Economy, Trade and Industry is testing facial recognition ticketing on driverless buses in several cities across the country.⁷⁴

In September 2020, Japan Times reported that Japanese Police Forces have been using facial recognition technology across the nation since March 2020 to locate criminal suspects. Critics warned that the system could transform the country into a surveillance society unless it run under strict regulations, a senior National Police Agency (NPA) official said “we are using the system only for criminal investigations and within the scope of the law. We discard facial images that are found to be unrelated to cases.”⁷⁵ The NPA manages and utilizes facial images under rules set by the National Public Safety Commission,⁷⁶ as it does with fingerprints and DNA. The agency’s database currently holds 10 million facial images of criminal suspects.

Japan does not have specific legislation for facial recognition in the government sector. As of September 2020, the Japanese APPI covers the use of facial biometric data gathered from security cameras.⁷⁷ Law enforcement is however exempt from this type of privacy regulations. The APPI also allows the use of anonymized facial recognition data beyond the intended purposes as long as such data is sufficiently protected from being restored to its original form.⁷⁸

Evaluation

Japan is a pioneer in the field of AI policy and has endorsed the OECD/G20 AI Principles. The Conference toward AI Network Society, established in 2016, is broadly influential. The Japanese R&D Guidelines provided the basis for the OECD AI Principles. Japan also hosted the G20 Leaders’ meeting in Osaka in 2019 at which time the G20 nations endorsed the OECD AI Principles. And former Prime Minister Shinzo Abe promoted the concept of Data Free Flow with Trust (DFFT), a core concept for human-centric AI, that carries forward in the policy recommendations of the OECD, the G20, and the European Commission. However, concerns about the unregulated use of facial recognition remain. While there has been no express support for the Universal Guidelines for AI or the Social Contract for the Age of AI, Japan’s policies reflect elements found in these documents.⁷⁹

Kazakhstan

Facial Recognition and Smart Cities

⁷⁴ NFCW, *Japanese passengers test facial recognition ticketing on driverless buses* (Sept. 10, 2020) <https://www.nfcw.com/2020/09/10/367826/japanese-passengers-test-facial-recognition-ticketing-on-driverless-buses/>

⁷⁵ Biometric Update, *Police in Japan reveal use of facial biometrics in criminal probes* (Sept. 16, 2020), <https://www.biometricupdate.com/202009/police-in-japan-reveal-use-of-facial-biometrics-in-criminal-probes>

⁷⁶ The National Public Safety Commission is a Japanese Cabinet Office commission which guarantees the neutrality of the police system by insulating the force from political pressure and ensuring the maintenance of democratic methods in police administration. It administers the National Police Agency, and has the authority to appoint or dismiss senior police officers. [https://en.wikipedia.org/wiki/National_Public_Safety_Commission_\(Japan\)](https://en.wikipedia.org/wiki/National_Public_Safety_Commission_(Japan))

⁷⁷ Biometric Update, *Police in Japan reveal use of facial biometrics in criminal probes* (Sept. 16, 2020), <https://www.biometricupdate.com/202009/police-in-japan-reveal-use-of-facial-biometrics-in-criminal-probes>

⁷⁸ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 150 & 151, December 2020, <https://caidp.dukakis.org/aisci-2020/>

⁷⁹ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 152, December 2020, <https://caidp.dukakis.org/aisci-2020/>

Facial recognition surveillance technology is becoming increasingly widespread in Kazakhstan. In October 2019, facial recognition technologies were first installed on buses.⁸⁰ Notably, President Tokayev had even paid a visit and discussed future cooperation with Hikvision,⁸¹ a Chinese state-owned surveillance company under U.S. sanctions⁸² that provided the hardware for Kazakhstan's newly established surveillance system. In the same year, the small city of Akkol was proclaimed the first complete "Smart City" in Kazakhstan. Akkol is digitally monitored by an AI-based facial recognition surveillance system, the functions of which include thermal imaging, searching for a car by number plates, recognizing missing persons, detecting the presence of weapons in schools, hospitals and other public places.⁸³ Similarly, over 4,000 cameras blanket Nur-Sultan, the capital.⁸⁴ In 2020, the authorities announced that Kazakhstan would be spending \$23 million to install facial recognition software in its largest city, Almaty.⁸⁵

While the government insists that the main goal is to maintain public safety, many activists are worried that this will ultimately create a totalitarian surveillance state,⁸⁶ especially since the companies that are behind the surveillance system in Kazakhstan are under U.S. sanctions for unethical use of AI technology.⁸⁷

Russia

Facial Recognition Controversy

Russia is moving rapidly to deploy AI-based face surveillance across the country, often with government funding that goes to business associates of President Putin. According to the *Moscow Times*, more than 43,000 Russian schools will be equipped with facial recognition cameras ominously named "Orwell."⁸⁸ The system will be integrated with face recognition developed by NTechLab, a subsidiary of Russian President Vladimir Putin's associate Sergei Chemezov's Rostec conglomerate. NTechLab has already deployed facial recognition technology in Moscow to identify criminal suspects across a network of almost 200,000 surveillance cameras. "Critics have accused the technology of violating citizens' privacy and have staged protests against the system by painting their faces," reported *Moscow Times*.

In September 2020, Kommersant daily reported that CCTV cameras with facial recognition software, already used in Moscow, will be installed by the regional authorities in public spaces and at the entryway of apartment buildings in 10 pilot cities across Russia with the purported

⁸⁰ The Four Big Issues Central Asia Faced In 2019 (And They're Not Going Away), Radio Free Europe, <https://www.rferl.org/a/central-asia-2019-challenges-security-china-facial-recognition/30356077.html>

⁸¹ «Распознает даже людей в масках». Нужны ли Казахстану камеры Hikvision? "It even recognizes people in masks." Does Kazakhstan need Hikvision cameras? Radio Free Europe, <https://rus.azattyq.org/a/kazakhstan-china-surveillance-camera/30210035.html>

⁸² <https://www.bloomberg.com/news/articles/2019-10-07/u-s-blacklists-eight-chinese-companies-including-hikvision-k1gvpq77>

⁸³ Видеонаблюдение, безопасность и комфорт. Как живет самый умный город Казахстана - Smart Akkol Video surveillance, security and comfort. How the smartest city of Kazakhstan lives - Smart Akkol, Tengrinews, <https://tengrinews.kz/article/videonablyudenie-bezopasnost-komfort-jivet-samyiy-umnyiy-1353/>

⁸⁴ Как работает проект "Серпек". Репортаж Informburo.kz How the Sergek project works. Informburo.kz report <https://informburo.kz/stati/kak-rabotaet-proekt-sergek-reportazh-informburokz.html>

⁸⁵ На камеры с распознаванием лиц в Алма-Ате выделили \$23 млн (Alma-Ata allocated \$ 23 million for cameras with face recognition), (Feb. 8, 2019), <http://fergana.agency/news/105020/>

⁸⁶ Kazakhstan embraces facial recognition, civil society recoils, Eurasianet, <https://eurasianet.org/kazakhstan-embraces-facial-recognition-civil-society-recoils>

⁸⁷ Center for AI and Digital Policy, Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020, p. 155 & 156, December 2020, <https://caidp.dukakis.org/aisci-2020/>

⁸⁸ Moscow Times, *Russia to Install 'Orwell' Facial Recognition Tech in Every School – Vedomosti* (June 16, 2020), <https://www.themoscowtimes.com/2020/06/16/russia-to-install-orwell-facial-recognition-tech-in-every-school-vedomosti-a70585>

aim of protecting public safety.⁸⁹ Moscow authorities are also planning to expand the use of this technology, installing CCTV cameras with facial recognition software in trams and underground trains.⁹⁰

Human Rights Watch said “The authorities’ intention to expand the use of invasive technology across the country causes serious concern over the potential threat to privacy. Russia’s track record of rights violations means that the authorities should be prepared to answer tough questions to prove they are not undermining people’s rights by pretending to protect public safety.”⁹¹ HRW also stated that Russian national security laws and surveillance practices enable law enforcement agencies to access practically any data in the name of protecting public safety.

Earlier in the year, Amnesty International criticized Russia’s plans to broaden the use of widespread facial-recognition systems, saying their expected deployment during public gatherings will “inevitably have a chilling effect” on protesters.^{92,93}

Evaluation

Russia’s development of a National AI Strategy, endorsement of the G20 AI Principles, its efforts to develop laws for digital rights and regulation for AI, as well as initiatives to involve the public in the development of AI policy count favorably. But beyond data protection legislation, the absence of robust measures to limit surveillance and protect human rights, coupled with the rapid adoption of facial recognition in public places raise concerns about the future of Russia’s AI program.⁹⁴

Sweden

Facial recognition

In March 2020, the data protection officer for the Swedish police undertook an investigation to determine whether the police may have used ClearView AI, an AI product for mass surveillance enabled by facial recognition.⁹⁵ The Swedish police confirmed that they have used Clearview AI, after previously denying use of the face surveillance tool.⁹⁶

⁸⁹ Kommersant, *Regions will recognize by sight: Moscow video surveillance system will be launched in ten more cities* (Sept. 25, 2020) [GT], <https://www.kommersant.ru/doc/4503379>

⁹⁰ Government of Russia, Unified information system in the field of procurement, Implementation of work on equipping the rolling stock of the State Unitary Enterprise "Moscow Metro" with video surveillance equipment (Aug. 3, 2020), https://zakupki.gov.ru/epz/order/notice/ea44/view/documents.html?regNumber=0173200_001420000752&backUrl=89687dbf-73a1-4346-a608-3634c2a98681

⁹¹ Human Rights Watch, *Russia Expands Facial Recognition Despite Privacy Concerns - Lack of Accountability, Oversight, Data Protection* (Oct. 2, 2020), <https://www.hrw.org/news/2020/10/02/russia-expands-facial-recognition-despite-privacy-concerns>

⁹² Radio Free Europe, *Watchdog Warns About 'Chilling Effect' Of Russia's Use Of Facial-Recognition Technology* (Jan. 31, 2020), <https://www.rferl.org/a/watchdog-warns-about-chilling-effect-of-russia-s-use-of-facial-recognition-technology/30410014.html>

⁹³ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 194 & 195, December 2020, <https://caidp.dukakis.org/aisci-2020/>

⁹⁴ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 197, December 2020, <https://caidp.dukakis.org/aisci-2020/>

⁹⁵ SVT NYHETER, *Intern utredning: Polisen får inte använda kritiserad AI-tjänst – skulle bryta mot lagen* (Mar. 6, 2020) [MT], <https://www.svt.se/nyheter/inrikes/svensk-polis-forbjuds-att-anvanda-kontroversiella-ai-tjansten>

⁹⁶ Mikael Grill Peterson and Linea Carlén, *Polisen bekräftar: Har använt omdiskuterade Clearview AI*, SVT NYHETER, (March 11, 2020) [MT], <https://www.svt.se/nyheter/inrikes/ekot-polisen-bekraftar-anvandning-av-kontroversiell-app>

Subsequently, the Swedish DPA “initiated an inspection to find out whether Swedish authorities use the face recognition technology provided by the US company Clearview AI.”⁹⁷ The DPA noted that the European Data Protection Board “will produce guidance on how law enforcement authorities should approach facial recognition technology. Sweden is one of the driving countries in the world.”

In 2019, the Swedish DPA did approve the use of facial recognition technology by the police to help identify criminal suspects. However, such an authorization relates to the use of biometric templates in databases under the control of public authorities and established under Union or Member States law.⁹⁸ As Andrea Jelinek, Chair of the European Data Protection Body, subsequently emphasized, “[t]he possible use of a service such as offered by Clearview AI by law enforcement authorities would, however, be fundamentally different, in that it would imply, as part of a police or criminal investigation, the sharing of personal data with a private party outside the Union and the biometric matching of such data against the latter’s mass and arbitrarily populated database of photographs and facial pictures accessible online.”⁹⁹ She also clearly questions the legality of the use of Clearview AI by public authorities.

In 2019, the Swedish DPA issued its first fine in a case involving facial recognition. A school in northern Sweden conducted a pilot using facial recognition to keep track of students’ attendance in school. The Swedish DPA concluded that the test violates the GDPR and imposed a fine on the municipality of approximately 20,000 euros. The school processed sensitive biometric data unlawfully and failed to do an adequate impact assessment including seeking prior consultation with the Swedish DPA. The school based the processing on consent but the Swedish DPA considers that consent was not a valid legal basis given the clear imbalance between the data subject and the controller.¹⁰⁰¹⁰¹

Taiwan

Facial Recognition

Facial recognition is implemented in Taiwan in various sectors, such as banks,¹⁰² retail stores,¹⁰³ airports,¹⁰⁴ and law enforcement.¹⁰⁵ In June 2019, the Taiwan Railways Administration announced that, due to privacy concerns, its surveillance system trial would

⁹⁷ The Swedish Data Protection Authority, The Data Inspectorate initiates supervision due to Clearview AI, <https://www.datainspektionen.se/nyheter/datainspektionen-inleder-tillsyn-med-anledning-av-clearview-ai/>.

⁹⁸ Official Journal of the European Union, *Directive EU 2016/680 of the European Parliament and of the Council* (Apr. 27, 2016), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN>

⁹⁹ EDPB response to MEPs Sophie in ’t Veld, Moritz Körner, Michal Šimečka, Fabienne Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI (June 10, 2020) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf.

¹⁰⁰ <https://www.datainspektionen.se/nyheter/2019/facial-recognition-in-school-renders-swedens-first-gdpr-fine/>.

¹⁰¹ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 237-239, December 2020, <https://caidp.dukakis.org/aisci-2020/>.

¹⁰² Luana Pascu, *Public Bank of Taiwan rolls out Kneron edge AI facial recognition*, *Biometric Update* (Sept. 24, 2019), <https://www.biometricupdate.com/201909/public-bank-of-taiwan-rolls-out-kneron-edge-ai-facial-recognition>

¹⁰³ Telpo, *7-Elevm Open the 2nd Face Recognition Unstaffed Store in Taiwan* (Nov. 20, 2018). <https://www.telpo.com.cn/blog/7-eleven-taiwan-face-recognition-store.html>

¹⁰⁴ Gorilla, *Taiwan’s International Airports Implement Gorilla Biometrics Technology to Improve Airport Operations and Security* (Dec. 23, 2016), <https://www.gorilla-technology.com/Press-Room/Taiwan’s-International-Airports-Implement-Gorilla-Biometrics-Technology-to-Improve-Airport-Operations-and-Security>

¹⁰⁵ AsiaOne, *Privacy not violated by facial recognition technology, says Taiwan police agency* (May 28, 2014), <https://www.asiaone.com/asia/privacy-not-violated-facial-recognition-technology-says-taiwan-police-agency>

not include facial recognition.¹⁰⁶ The artificial intelligence–based surveillance will still be capable of monitoring passenger behavior, including trespassing, loitering in restricted areas and prohibited acts.¹⁰⁷

More recently, Liao Wei-min, associate professor at Taiwan National Chung Hsing University’s Department of Law called for legislation regarding facial recognition and data collection.¹⁰⁸ He wrote, “What is essentially a beneficial technology is deeply problematic given the lack of precise and targeted legislation, and this is the fault not of civil servants, but their politically appointed masters. Something needs to be done to address this.”¹⁰⁹

Evaluation

Although Taiwan is not an OECD member country many of its AI policies align with the OECD AI Principles. There is also a robust public debate about the use of AI for facial recognition, medical data, and autonomous vehicles. But privacy concerns arise with the integration of government data sets while the government has not established an independent data protection agency that could oversee AI applications from a privacy perspective.¹¹⁰

Thailand

Evaluation

Thailand has launched an ambitious plan for AI. The Bangkok Statement on Ethics is significant as is the work of the NXPO in the field of AI ethics. But the absence of protections for fundamental rights as the country seeks to expand national identification and systems for facial recognition is troubling. Legal safeguards should precede AI deployment to ensure trustworthy AI. Thailand should ensure that Personal Data Protection Act goes into effect with an independent data protection authority.¹¹¹

United Kingdom

Facial Recognition

Human rights organizations have long criticized the UK government for the almost unparalleled deployment of CCTV. (Chongqing, China has now overtaken London as the most surveilled city in the world.¹¹²) Earlier this year, London’s Met Police deployed live facial recognition. The Met says its use of the controversial technology will be targeted to “specific

¹⁰⁶ Focus Taiwan, *TRA to cut facial recognition feature from surveillance system trial* (Nov. 6, 2019), <https://focustaiwan.tw/society/201911060011>

¹⁰⁷ IAPP, *Taiwan Railways Administration excludes facial recognition from surveillance trial* (Nov. 7, 2019), <https://iapp.org/news/a/taiwan-railways-administration-excludes-facial-recognition-from-surveillance-trial/>

¹⁰⁸ Liao Wei-min, *Legislation needed for advances in surveillance*, Taipei Times (Dec. 28, 2019), <http://www.taipeitimes.com/News/editorials/archives/2019/12/28/2003728301>

¹⁰⁹ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 260 & 261, December 2020, <https://caidp.dukakis.org/aisci-2020/>

¹¹⁰ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 264, December 2020, <https://caidp.dukakis.org/aisci-2020/>

¹¹¹ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 272, December 2020, <https://caidp.dukakis.org/aisci-2020/>

¹¹² Matthew Keegan, *Big Brother is watching: Chinese city with 2.6m cameras is world's most heavily surveilled*, The Guardian (Dec. 2, 2019) <https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled>.

locations where intelligence suggests we are most likely to locate serious offenders.”¹¹³ Silkie Carlo, the director of Big Brother Watch, called the move “an enormous expansion of the surveillance state and a serious threat to civil liberties in the UK”. Noel Sharkey, a leading human rights campaigner, tweeted “FACE RECOGNITION - After 2yrs trials which an independent review showed 9% accuracy, the Met police start live facial recognition in London. This is a shameful disrespect of the British people & we know it’s racially biased. STOP IT.”¹¹⁴ Privacy International recently urged regulatory authorities to investigate Facewatch, a company that specializes in facial recognition analysis and biometric watchlists.¹¹⁵¹¹⁶

United States

Facial Recognition

There are wide-ranging protests in the United States against the deployment of facial recognition technology. In May 2019, San Francisco became the first city in the U.S. to ban the use of facial recognition technology by city agencies.¹¹⁷ The city supervisor said, “It’s psychologically unhealthy when people know they’re being watched in every aspect of the public realm, on the streets, in parks.” Other cities, including Cambridge, Oakland, and Portland followed. In October 2019, California enacted a moratorium on the use of facial recognition technology in police body cameras.¹¹⁸ The bill prohibits the use of biometric surveillance technology, which includes facial-recognition software, in police body cameras. It also prohibits police from taking body-camera footage and running it through facial-recognition software at a later time. It does not prevent state and local police from using facial-recognition technology in other ways, such as in stationary cameras, and it does not apply to federal agencies such as the FBI.¹¹⁹

A bill introduced in the United States Congress would ban the use of facial recognition by law enforcement agencies.¹²⁰ The Facial Recognition and Biometric Technology Moratorium Act would make it illegal for any federal agency or official to “acquire, possess, access, or use” biometric surveillance technology in the US. It would also require state and local law enforcement to bring in similar bans in order to receive federal funding.¹²¹ The bill was introduced by Senators Ed Markey Jeff Merkley, and Representatives Pramila Jayapal and Ayanna Pressley.¹²²

¹¹³ Vikram Dodd, *Met police to begin using live facial recognition cameras in London*, The Guardian (Jan. 24, 2020), <https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras>

¹¹⁴ @NoelSharkey (Jan. 24, 2020), <https://twitter.com/NoelSharkey/status/1220722848337211394>

¹¹⁵ Privacy International, *Authorities Must Act on Police Face Surveillance Network by the Backdoor* (Oct. 15, 2020), <https://privacyinternational.org/news-analysis/4218/authorities-must-act-police-face-surveillance-network-backdoor>

¹¹⁶ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 283 & 284, December 2020, <https://caidp.dukakis.org/aisci-2020/>

¹¹⁷ Kate Conger, Richard Fausset and Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology* (May 14, 2019), <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>

¹¹⁸ California Legislative Information, *AB-1215 Law enforcement: facial recognition and other biometric surveillance* (Oct. 9, 2019)

¹¹⁹ Rachel Metz, *California lawmakers ban facial-recognition software from police body cams* (Sept. 13, 2019), <https://www.cnn.com/2019/09/12/tech/california-body-cam-facial-recognition-ban/index.html>

¹²⁰ Congress.gov, *S.4084 - Facial Recognition and Biometric Technology Moratorium Act of 2020* (June 25, 2020), <https://www.congress.gov/bill/116th-congress/senate-bill/4084>

¹²¹ MIT Technology Review, *A new US bill would ban the police use of facial recognition* (June 26, 2020), <https://www.technologyreview.com/2020/06/26/1004500/a-new-us-bill-would-ban-the-police-use-of-facial-recognition/>

¹²² Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 291 & 293, December 2020, <https://caidp.dukakis.org/aisci-2020/>

Evaluation

The United States endorsed the OECD/G20 AI Principles. The White House has issued two Executive Orders on AI that reflect democratic values, a federal directive encourages agencies to adopt safeguards for AI, and the US Chief Technology officer has underscored US commitment to democratic values. The most recent Executive Order also establishes a process for public participation in agency rulemaking on AI through the Office of Management and Budget. But the overall US policy-making process has been opaque, the National Security Commission on AI has resisted public participation, and the Federal Trade Commission has failed to act on several pending complaints concerning the deployment of AI techniques in the commercial sector. Concerns have been raised about the export of facial surveillance technology by such US companies as Clearview AI. The absence of a legal framework to implement AI safeguards and a federal agency to safeguard privacy also raises concerns about the ability of the US to monitor AI practices.¹²³

[NOTE – This CAIDP Special Report on Facial Recognition excerpts key references to facial recognition contained in the 2020 report *Artificial Intelligence and Democratic Values / The AI Social Contract Index 2020*, prepared by the Center for AI and Digital Policy. This summary and other related materials will be found at <https://caidp.dukakis.org/aisci-2020/>]

¹²³ Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values: The AI Social Contract Index 2020*, p. 297, December 2020, <https://caidp.dukakis.org/aisci-2020/>