Universiteit Utrecht

Facial Recognition Technology: Challenges for International Collaboration & Governance

17 November 2021

istock/Scharfsinn86

Workshop Report

Machiko Kanetake
January 2022

Workshop Objective

On 17 November 2021, Utrecht University hosted an interdisciplinary workshop on facial recognition technologies. One of the aims of the workshop was to address ethical and regulatory challenges associated with *international collaboration* on the research and development of facial recognition and related Artificial Intelligence (AI) technologies.

Simultaneously, the workshop aimed at contextualising political debates within the EU about facial recognition technologies from international standpoints. In so doing, the workshop allowed us to consider whether the EU's approaches to the regulation of facial recognition may need to be adjusted.

The workshop was live-streamed from Paushuize in Utrecht to allow participants to join online.

José van Dijck (Utrecht University) opened the workshop on behalf of Utrecht University's focus area 'Governing the Digital Society'.

1. Prevalence & controversies

Facial recognition technology (FRT) is one of the most widely debated and contested technologies. As one application in the field of computer vision, facial recognition technology refers to a set of systems which collect, analyse, verify, and/or identify a person's face. The technology is widely used. For instance, it has been applied in health care to identify and monitor patients as well as to diagnose medical conditions.[1] Facial recognition has been deployed for security at airports,[2] registration and security at schools,[3] and to prevent shoplifting.[4] More controversial, however, is the use of the technology by the police to prevent and investigate criminal conduct by the police.[5] According to Ragazzi et al. (2021), 11 out of 27 EU member states use (ex-post) facial recognition against biometric databases for forensic purposes, and it is anticipated that seven additional EU member states would acquire such capabilities.[6]

The prevalent use of facial recognition has been accompanied by growing concerns over its infringement on privacy, its exacerbation of discriminatory practices, and its perpetuation of political oppression. As the UN's special rapporteur remarked in his report on surveillance and human rights, the use of facial recognition technology potentially leads to 'profiling individuals based on their ethnicity, race, national origin, gender and other characteristics' often against the principle of non-discrimination.[7] He furthermore acknowledged that '[p]erhaps no other environment demonstrates the comprehensive intrusiveness of these [facial and affect recognition] technologies better than China',[8] where a combination of various digital technologies has been deployed to track Muslim Uighur minorities in Xinjiang

[1] Nicole Martinez-Martin, 'What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?' (2019) 21 *AMA Journal of Ethics* E180.

[2] Nimra Khan and Marina Efthymiou, 'The Use of Biometric Technology at Airports: The Case of Customs and Border Protection (CBP)' (2021) 1 *International Journal of Information Management Data Insights* 100049.

[3] Mark Andrejevic and Neil Selwyn, 'Facial Recognition Technology in Schools: Critical Questions and Concerns' (2020) 45 *Learning, Media and Technology* 115.

[4] Matt Burgess, 'Co-op is Using Facial Recognition Tech to Scan and Track Shoppers', *Wired* (10 December 2020), https://www.wired.co.uk/article/coop-facial-recognition (last accessed 3 January 2022).

[5] E.g., Joe Purshouse and Liz Campbell, 'Automated Facial Recognition and Policing: A *Bridge* Too Far?' (2021) *Legal Studies* 1.

[6] Francesco Ragazzi and others, 'Biometric & Behavioural Mass Surveillance in EU Member States', Report for the Greens/EFA in the European Parliament (October 2021) 38–39.

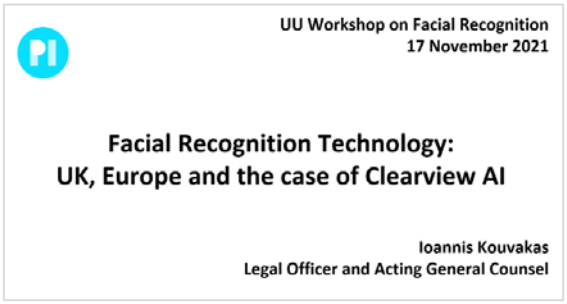
[7] UN Human Rights Council and Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Surveillance and Human Rights' UN Doc. A/HRC/41/35 (28 May 2019) para 12.

[8] Ibid.

province.[9] In various parts of the world, facial recognition technology is part of digital surveillance technologies that can serve as 'geopolitical tools of population selection'.[10] Privacy International expressed its concern with the 'normalisation' of the use of facial recognition, and its 'seismic impact on the way our society is monitored or policed'.[11]

Controversies on facial recognition technology are abundant. One of the developments which garnered international criticism, especially after the publication of a *New York Times* report in January 2020, was Clearview AI.[12] This private facial recognition platform automatically scraped images from social media sites and a variety of websites, extracted facial features, and created a system (with '10+ billion facial images', according to the company[13]) to allow the biometric matching of individuals.[14] The database has been made available to law enforcement authorities and companies for security purposes.[15] It has been reported that the Dutch police force, to name just one of those authorities, used a free trial of Clearview AI's facial recognition software.[16] Law enforcement agencies were provided 'with an enormous number of immediately available facial images,' including those pertaining to 'citizens who may never find themselves in situations that could lead to a criminal proceeding'.[17]

During the workshop, Ioannis Kouvakas (Privacy International) shared his insights into the legal challenges raised against Clearview AI.[18] Kouvakas pointed out that public bodies and private companies often work in partnership, which blurs the public-private divide: 'Companies are invited, compelled, or even volunteer to team up with law enforcement to



[9] James Leibold, 'Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement' (2020) 29 *Journal of Contemporary China* 46.

[10] Veronika Nagy, *Crime Prevention, Migration Control and Surveillance Practices: Welfare Bureaucracy as Mobility Deterrent* (London, Routledge, 2018) 150.

[11] Privacy International, 'Facial Recognition', https://privacyinternational.org/learn/facial-recognition (last accessed 3 January 2022).

[12] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It', *The New York Times* (18 January 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html?action=click&module=Top%20Stories&pgtype=Homepage (accessed 3 January 2022).

[13] Clearview AI, 'Company Overview', Clearview AI, Inc., https://www.clearview.ai/overview (accessed 3 January 2022).

[14] Hill (n 12).

[15] Ibid.

[16] De Volkskrant, 'Nederlandse politie gebruikte controversiële gezichtsherkenningssoftware 'minimaal vijftig keer' (26 August 2021), https://www.volkskrant.nl/nieuws-achtergrond/nederlandse-politie-gebruikte-controversiele-gezichtsherkenningssoftware-minimaal-vijftig-keer~b6aa77d4/?referrer=https%3A%2F%2Fwww.google.com%2F (accessed 3 January 2022).

[17] Isadora Neroni Rezende, 'Facial Recognition in Police Hands: Assessing the "Clearview Case" from a European Perspective' (2020) 11 *New Journal of European Criminal Law* 375, 389.

[18] Challenge against Clearview AI in Europe, https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe (accessed 3 January 2022).

install CCTV systems, facilitate smart cities, provide access to personal data or even carry out policing functions traditionally entrusted to the state'.

Various NGOs, researchers, and public institutions have called for the prohibition of the use of facial recognition technology by law enforcement authorities. In June 2020, UN High Commissioner for Human Rights, Michelle Bachelet, recommended that states establish 'a moratorium on the use of facial recognition technology' in the context of peaceful protests until certain safeguards are in place.[19] In October 2021, the European Parliament called for 'a moratorium on the deployment of facial recognition systems for law enforcement purposes that have the function of identification' unless 'strictly used for the purpose of identification of victims of crime' until certain criteria are fulfilled—including the condition that 'the technical standards can be considered fully fundamental rights compliant'.[20]

2. Varied Public Perception

Given that the use of facial recognition technology is enthusiastically embraced within various industries and institutions yet also heavily contested, it is also important to understand how citizens perceive the technology. Citizens' perception—however (ill-)informed—would have an impact on regulators' responses (and presumably vice versa) to the development and use of facial recognition technologies.

Variations in citizens' acceptance 'raise questions about the feasibility of finding a global regulatory response'.

(Kostka et al. (2021), p. 686)

Photo by Matthew Henry on Unsplash

[19] Report of the United Nations High Commissioner for Human Rights, 'Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests', UN Doc. A/HRC/44/24 (24 June 2020), para 53(j).

[20] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), P9_TA(2021)0405, para 27.

During the workshop, Genia Kostka (Freie Universität Berlin) shared her and her co-authors' studies published in *Public Understanding of Science* (2021)[21] on public perception and acceptance of facial recognition technology in different political contexts.

They conducted an online survey of 6,633 citizens in China, Germany, the UK, and the US between August and September 2019. The survey showed 'a high level of general awareness' about facial recognition technology, in as much as 92% (6,099 respondents) had previously heard about it.[22] Forty-eight percent of the respondents had used the technology at least once. Among the respondents (except for those who had never heard about facial recognition technology), the study showed that 51% of the respondents accept the use of facial recognition in general. Interestingly, according to Kostka et al. (2021), acceptance rates turned out to be even higher for the *private* use of facial recognition technology, rather than its public use. Among the respondents, 52% accepted the technology for private use, while 42% accept it for public use.[23] On this basis, the study demonstrated how the acceptance of facial recognition technology varies across countries:[24]

- China:
  - 67% (strongly or somewhat) accept facial recognition technology
  - 71% accept the *private* use of the technology
  - 51% accept the *government* use of the technology
- Germany (where private/public acceptance rates differ from other countries' results):
  - 38% accept the technology
  - 33% accept the *private* use of the technology
  - 38% accept the *government* use of the technology
- UK:
  - 50% accept the technology
  - 50% accept the *private* use of the technology
  - 42% accept the *government* use of the technology
- US:
  - 48% accept the technology
  - 52% accept the *private* use of the technology
  - 37% accept the *government* use of the technology

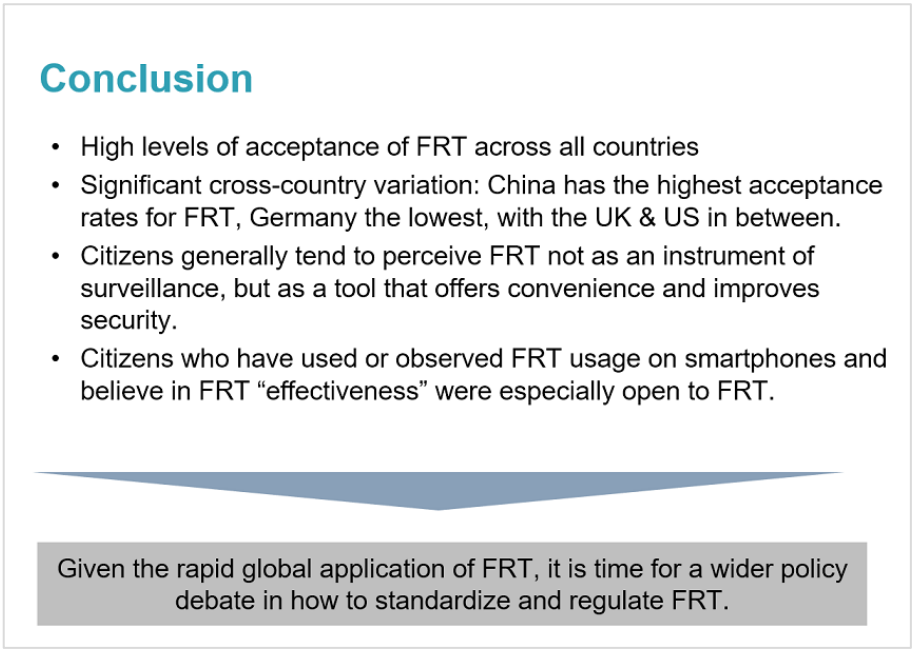
[21] Genia Kostka, Léa Steinacker and Miriam Meckel, 'Between Security and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the United Kingdom, and the United States' (2021) 30 *Public Understanding of Science* 671.

[22] Ibid., 679.

[23] Ibid., 679–681.

[24] Ibid.

The study by Kostka et al. (2021) further demonstrates differences in perceived benefits and risks regarding the use of facial recognition technology. The findings 'show that perceiving improved security to be a consequence is a particularly strong, positive factor' accounting for the acceptance of the technology across all countries.[25] 'Improved efficiency and convenience also appear to be a key factor influencing attitude toward FRT, particularly in China'. 'In contrast, in Germany, convenience was not associated with FRT acceptance'.[26] During the workshop, Kostka summarised her findings as follows:



Kostka et al. observed that their results would 'raise questions about the feasibility of finding a global regulatory response'.[27] Presumably, this is not necessarily because of the variance in public acceptance, but rather because of the differences in political and technological contexts that affect public perception.

3. Implications for International Collaboration

Just as the public perception of facial recognition technology varies, regulatory responses differ depending on countries and local authorities. Within the EU, a wide range of initiatives have been developed to analyse, and set standards for, the development and use of facial recognition technology. At the EU's level, the EU's proposed Act for AI of April 2021 has focused on the risks arising from facial recognition technologies.[28] Under the proposal, third-

[25] Ibid., 685.
[26] Ibid.
[27] Ibid., 686.
[28] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative

party assessment would be required for AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons.

On another front, facial recognition has also been given particular importance in the political debate surrounding the EU's 'dual-use' regulation adopted in May 2021, as illustrated by the European Parliament's video which aimed at informing the public of the significance of the new regulation.[29] Dual-use items are those which serve both civil and military purposes. A variety of technologies that serve civilian purposes could also be employed for building military capacities.

Facial recognition is featured in the European Parliament's video on the EU's dual-use export controls.

Some of these regulatory responses add a new layer of complexity regarding ***international collaboration*** to foster technological development. The complexity is captured in Communication adopted by the European Commission in May 2021, entitled the 'Global Approach to Research and Innovation'.[30]

Photo by Christian Lue on Unsplash

> ***'Openness** has always been a cornerstone in our cooperation with the rest of the world'.*
>
> *(Executive Vice-President for A Europe Fit for the Digital Age, European Commission)*

Acts', COM(2021) 206 final, 2021/0106 (COD) (21 April 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (accessed 3 January 2022).

[29] European Parliament News, 'Dual-Use Goods: What Are They and Why Are New Rules Needed?' (24 March 2021), https://www.europarl.europa.eu/news/en/headlines/world/20210319STO00424/dual-use-goods-what-are-they-and-why-are-new-rules-needed (accessed 3 January 2022).

[30] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on the Global Approach to Research and Innovation Europe's Strategy for International Cooperation in a Changing World' COM(2021) 252 final (18 May 2021).

On the one hand, the Commission reaffirmed the EU's commitment to preserve '**openness** in international research and innovation'.[31] 'Openness' in research and innovation remains to be 'a cornerstone' in the EU's 'cooperation with the rest of the word', as reiterated by the Commission's Executive Vice-President for A Europe Fit for the Digital Age.[32] On the other hand, however, such 'openness' should be based upon '**a level playing field**' and '**reciprocity underpinned by fundamental values**', according to the Commission.[33]

The Commission's 'Global Approach to Research and Innovation' highlights the multi-faceted tensions among: (i) the EU's openness in research collaboration and the EU's commitment to own rules and values; (ii) the EU's values and those of non-EU countries; and (iii) the idea of reciprocity and the promotion of rules and values, as a basis for international cooperation.

*'The EU should engage with non-EU countries in a nuanced and modulated approach, based **on levels of reciprocity, a level playing field, and the respect for fundamental rights and shared values**'.*[1]

The EU's dual-use export controls

One of the EU's instruments that **embody tensions** between 'openness in international research and innovation' and 'rule- and value-based cooperation' is the EU's export control regulation.[34] While it may not be self-evident, **trade controls such as export controls would be relevant for international research collaboration**. Trade controls apply, not just the cross-border transfer of tangible goods, such as computer hardware, but also the 'intangible' transfer of items, goods, and technologies, including technical data, knowledge, and know-how.[35]

Within the EU, the export of dual-use items is governed by Regulation (EU) 2021/821.[36] It was adopted on 20 May 2021 and entered into force on 9 September 2021 to replace the predecessor Regulation (EC) 428/2009.[37] Regulation 2021/821 was adopted as the result of

[31] Ibid., at 1.

[32] European Commission, Press Release, 'Europe's global approach to cooperation in research and innovation: strategic, open, and reciprocal' (18 May 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2465 (accessed 3 January 2022).

[33] European Commission, 'Global Approach' (n 30) at 1.

[34] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) [2021] OJ L206/1.

[35] On the intangible transfer, see Mark Bromley, Kolja Brockmann and Giovanna Maletta, 'Controls on Intangible Transfers of Technology and Additive Manufacturing', *SIPRI Yearbook 2018* (Oxford University Press, 2018) 437, 437–443.

[36] Regulation (EU) No 2021/821 of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) [2021] OJ L 206/1.

[37] Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community Regime for the control of exports, transfer, brokering and transit of dual-use items [2009] OJ L 134/1.

several years of debates,[38] especially after the European Commission submitted in September 2016 a proposal to recast and replace Council Regulation (EC) 428/2009.[39]

One of the core characteristics of Regulation 2021/821 is to tighten export controls over 'cyber surveillance items'.[40] Facial recognition technologies may fall under the definition of 'cyber surveillance items',[41] which triggers risk assessment under the dual-use regulation on the part of exporters. What matters for the sake of the workshop's theme was that **international research collaboration on facial recognition technologies and related AI** may be affected by the EU's dual-use regulation.

During the workshop, Mark Bromley (Stockholm International Peace Research Institute, SIPRI) shared his insights into the EU's dual-use regulation, which aimed at strengthening the EU's export controls over 'cyber-surveillance items'.[42]

While there is nothing new about extending export controls to research activities, Regulation 2021/821 explicitly refers to 'researchers' as one of the categories of persons that should be 'aware of the risks associated with the export and the provision of technical assistance regarding sensitive items'.[43] On this basis, on 15 September 2021, the European Commission adopted the 'Guidance' under Recommendation (EU) 2021/1700 for research organisations to identify and mitigate risks associated with research involving dual-use items.[44] The Guidance

[38] For the EU's legislative processes to recast Council Regulation No 428/2009, see Machiko Kanetake, 'The EU's Dual-Use Export Control and Human Rights Risks: The Case of Cyber Surveillance Technology' (2019) *Europe and the World: A law review*; Machiko Kanetake, 'Converging Dual-Use Export Control with Human Rights Norms: The EU's Responses to Digital Surveillance Exports' in E. Fahey (ed.), *Framing Convergence with the Global Legal Order: The EU and the World* (Oxford, Hart Publishing, Bloomsbury Publishing Plc, 2020) 65.

[39] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (recast)' COM(2016) 616 final (28 September 2016) Art 2(1).

[40] Regulation (EU) No 2021/821 of 20 May 2021 (n 36), Articles 2(20), 5, and 26(2). For the interpretation of Article 5, see, e.g., Federal Office for Economic Affairs and Export Control, 'Leaflet on Art. 5 of the EU Dual-Use Regulation (Regulation (EU) 2021/821)' (2021) (October 2021).

[41] See O.L. van Daalen and others, 'The New Rules for Export Control of Cyber-Surveillance Items in the EU' (Institute for Information Law (IViR) University of Amsterdam, 2021) (June 2021) 37–41, 54–55.

[42] For an overview of the EU's dual-use regulation 821/2021, see Mark Bromley and Kolja Brockmann, 'Implementing the 2021 Recast of the EU Dual-Use Regulation: Challenges and Opportunities' Non-Proliferation and Disarmament Papers, No. 77 (September 2021).

[43] Regulation (EU) No 2021/821 of 20 May 2021 (n 36), Recital 13.

[44] Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items [2021] OJ L 338/1 ('Guidance').

broadly refers to computer science, 'artificial intelligence and machine learning' and 'cyber surveillance items' as part of the research areas that are 'more likely to be impacted' by dual-use export controls.[45]

During the workshop, building on the presentation by Bromley, Claire Stalenhoef and Machiko Kanetake (Utrecht University) presented their views regarding the implications of the EU's export controls on international research collaboration, including academic research involving universities.

[45] Ibid., Annex I, at 38-39.

4. Towards Global Standards?

Collaboration across different institutional & normative contexts

International collaboration in the field of AI would thus have to address the varied acceptability or permissibility of technology across multiple communities. Governments differ in terms of how they problematize the development and use of facial recognition technology. Such variance across states, jurisdictions, and communities creates critical challenges for international technological collaboration, especially without any effective international normative frameworks. During the workshop, some speakers shared their insights into some pragmatic challenges in carrying out international research collaboration in the wider domains of computer vision.

International and regional human rights norms as one of the frameworks

In discussing the role of international normative frameworks, it is important to be aware of the applicability of existing international human rights norms to the use of facial recognition technology and related AI. For example, the UN High Commissioner for Human Rights published, in June 2020, the report concerning the impact of new technologies—including facial recognition technology—on the promotion and protection of human rights in the context of assemblies, including peaceful protests.[46] The UN High Commissioner recommended, among other things, the systematic implementation of human rights due diligence, compliance with privacy and data protection standards, the absence of significant accuracy issues and discriminatory impacts, oversight mechanisms, and full transparency about the use of image recordings and facial recognition technology.[47] Furthermore, in June 2021, the Council of Europe published the Guidelines on Facial Recognition, suggesting that states should adopt a robust legal framework applicable to the different cases of facial recognition technology and implement a set of safeguards.[48]

At the same time, in the age of automated decision making, some of the established legal frameworks on privacy and non-discrimination may not always provide a robust framework to assess *how* exactly one's data—including biometric data—is being evaluated and what kind of assumptions or predictions are made with regard to one's behaviour.[49]

---

[46] Report of the United Nations High Commissioner for Human Rights, 'Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests', UN Doc. A/HRC/44/24 (24 June 2020).

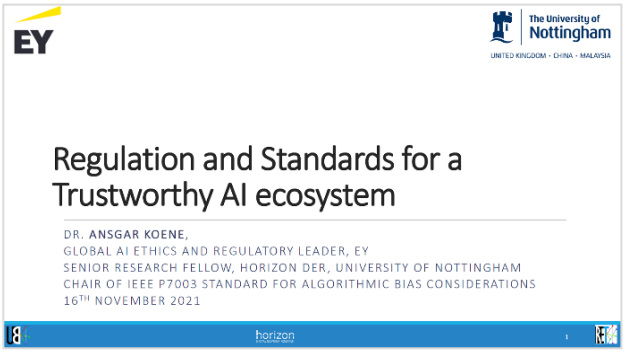
[47] Ibid., para 53(j).

[48] Council of Europe, 'Guidelines on Facial Recognition', adopted by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (June 2021), https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html (accessed 3 January 2022).

[49] See Machiko Kanetake, Lucky Belder, and Karin van Es, "Reflection on the GDS webinar by Sandra Wachter: 'The (im)possibility of algorithmic fairness'", GDS Blog (3 February 2021), https://www.uu.nl/en/opinion/reflection-on-the-gds-webinar-by-sandra-wachter-the-impossibility-of-algorithmic-fairness (accessed 3 January 2022).

Need for multi-level initiatives, involving both technical and political communities

During the workshop, Ansgar Koene (EY; University of Nottingham) shared his insights into multi-level initiatives in setting AI ethics and norms. Koene discussed, for instance, the role of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) in setting international standards for AI. Koene also referred to the work of the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems.



Translating the frameworks into technical reality: importance of interdisciplinary platforms

In discussing the role of existing and emerging regional and international normative frameworks, the workshop reminded us of problematic gaps between 'technical' communities and 'political' conversation, which can hinder the effectiveness of regulatory frameworks. There remains a great deal of uncertainties regarding how to translate some of the abstract principles and norms into technical realities. During the workshop, Yi Zeng (Chinese Academy of Sciences) shared his insights regarding some of the technical and cross-cultural challenges for responsible biometric recognition. Lynda Hardman (Centrum Wiskunde & Informatica (CWI) and Utrecht University) pointed out some of the gaps between technical communities and political debates. Hardman elucidated the need for long-term collaborations to allow academic communities—and their wider audience—to get to know each other and learn more about contexts in which colleagues carry out their respective research.

Overall, the workshop underscored the critical importance of interdisciplinary platforms in building the governance of facial recognition and related AI, including the aspect of international collaboration on the research and development of the technologies. The workshop itself provided a unique opportunity for mutual learning among participants from computer science, political science, higher education studies, and law. It is the intension of the organisers to facilitate the creation of such opportunities in the future as part of the initiatives of Utrecht University.

10.15-10.30 Opening & introductory remarks
José van Dijck (Utrecht University) & **Machiko Kanetake** (Utrecht University)

1. International collaboration on FR technology & political and cultural contexts

10.30-12.00 Chair & discussant: **Albert Salah** (Utrecht University)

Lynda Hardman (Centrum Wiskunde & Informatica (CWI) and Utrecht University): 'Open or Exposed? Conflicting Forces in International AI Research'

Yi Zeng (Chinese Academy of Sciences): 'Technical and Cross-cultural Challenges for Responsible Biometric Recognition'

Genia Kostka (Freie Universität Berlin): 'Between Security and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the United Kingdom, and the United States'

12.00-13.00 Break

2. The EU's ethical and regulatory approaches concerning international collaboration on FR technology

13.00-14.00 Chair & discussant: **Marijk van der Wende** (Utrecht University)

Mark Bromley (Stockholm International Peace Research Institute, SIPRI): 'Export Controls and Surveillance Tools: The Use of Export Controls by the EU and Wassenaar Arrangement to Regulate the Trade in Cyber-Surveillance Items and their Potential Application to Biometric Systems'

Claire Stalenhoef & Machiko Kanetake (Utrecht University): 'EU's Export Controls, AI Regulation, and International Collaboration on Facial Recognition Technologies'

14.00 Break

3. Global policies on FR technology and related international collaboration

14.30 Chair & discussant: **Lucky Belder** (Utrecht University)

Ioannis Kouvakas (Privacy International): 'Facial Recognition Technology in Europe and the Case of Clearview AI: A Need for Regulation or Enforcement?'

Ansgar Koene (EY; University of Nottingham): 'Developments for AI Governance through Regulation and Standards: Globally Coordinated Deliberative Approaches vs. Reactive Policy Making'

Cong-rui Qiao (Vrije Universiteit Amsterdam) (commentator)

15:30 Closing observations from the organisers

Workshop Organisers

The event was supported by Utrecht University and Gerda Henkel Stiftung and organised by Lucky Belder, Karin van Es, Arthur Gwagwa, and Machiko Kanetake, as part of the following UU research groups:

- Research platform on *Disrupting Technological Innovation? Towards an Ethical and Legal Framework* within the Utrecht Centre for Global Challenges
- Special Interest Group on *Principles by Design: Towards Good Data Practice* within Governing the Digital Society
- Digital building block, the Utrecht Centre for Regulation and Enforcement in Europe (RENFORCE)

The present report is written by Machiko Kanetake, one of the co-coordinators of the Special Interest Group within Governing the Digital Society, based on the input from other organisers. Any errors regarding the description of the workshop are hers alone and not those of the speakers of the workshop.

RENFORCE
UTRECHT CENTRE FOR REGULATION AND ENFORCEMENT IN EUROPE

CENTRE FOR GLOBAL CHALLENGES

GERDA HENKEL STIFTUNG