


Research Brief – December 2021



Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement

By Catarina Fontes and Christian Perrone

Data dependency is one of AI's intrinsic features. Personal data is paramount to feed the datasets used to train machine learning systems and build algorithmic models. Once the models are set, they can be applied to personal data and used to analyze or make inferences and predictions concerning particular individuals. This also applies to live facial recognition systems, implying risks for several individual rights, particularly privacy. In this Brief, we frame the implementation of these systems in the particular context of public space surveillance by public authorities for law enforcement purposes. Privacy, consent and proportionality are three intertwined aspects needed to describe the ethics of public space surveillance and to consider the responsible implementation of such AI-enabled systems.

Facial recognition technology (FRT) is one of the available biometric technologies that aim to identify individuals by measuring and analyzing human physiological or behavioral characteristics. The process implies that a person's facial image is compared against other samples in a database, delivering a score which indicates the likelihood that compared images refer to the same person. Beyond identification or identity verification, the processing of biometric data can be used for profiling individuals by collecting and categorizing personal characteristics such as age, sex and ethnic origin. Further advancements refer to the possibility of drawing more complex interpretations and even predictions, involving, for instance, emotion analysis and future actions. This means AI-enabled systems would have the ability to analyze patterns and make inferences on normal/abnormal behavior and emotions (Ryoo, 2011; Kong & Fu, 2018; Yang, et al., 2018; Singh & Vishwakarma, 2019; Pauwels, 2020).

FRT's applications range from identifying faces on photos on social networks and matching them to respective profiles, to validating a person's identity in order to grant access, supporting in diseases' diagnostics and patients monitoring, evaluating candidates in interviews and verifying attendances in many situations (Chen, et al., 2018; Jeon, 2019; Sawhney et al., 2019; Su, 2021). We focus in this Brief on potential uses of FRT for **surveillance of public spaces by public authorities**, acknowledging that FRT's applications for security and law enforcement go beyond that, covering for instance, border control (Tucker, 2020) and many other specific policing activities (Introna & Nissenbaum, 2010). We then reflect upon the ethics of surveillance and how AI poses new challenges and calls for increasing proportionality and transparency to ensure respect for individual rights and liberties. Between fairness and other ethics principles in public health surveillance technologies.

While the potential of biometric systems is recognized in multiple spheres, the idea that their deployment is in the public interest or "for good" is counterbalanced by societal and ethical concerns. These concerns have been triggering controversy around the use of AI-enabled biometric systems and increasing resistance towards them, particularly towards the use of FRT's in public spaces for law enforcement purposes. The countermovements underpin how the technology and its deployment may be beyond the rule of law (Big Brother Watch, 2018; van Brakel, 2021), pose a threat to fundamental and human rights (FRA, 2019; LPEP, 2019; Pauwels, 2020) or represent a risk to the undermining of democratic values due to a potential chilling effect (Selinger & Hartzog, 2019; Fussey & Murray, 2019). Moreover, they may alter public life in public spaces, by impacting on privacy and consequently promoting exclusion, affecting particularly specific vulnerable groups (Koskela, 2003; Hirose, 2017; Fontes & Lütge, Forthcoming).

AI-enabled Surveillance and Security Around the Globe

The use of biometric identification technologies for law enforcement is not a novelty. Fingerprint and DNA matching are widely deployed to assist in the reliable identification of individuals within the public security realm. Additionally, CCTV systems have been deployed in many urban spaces around the world, as tools for surveillance in support of public security. For CCTV, cameras are the visible interface for surveillance, yet human agency and oversight is a cornerstone of the system. The use association with CCTV systems (often called "Smart CCTV") relies on AI to analyze the data and make certain inferences and decisions in real time, without requiring human

intervention. The surveillance of public spaces using FRT can be adopted to, for instance, identify known or suspected criminals, terrorists, missing persons or tracking down suspicious behavior, by continuously monitoring public spaces and consequently human activities and presence.

Police forces use two types of FRT: facial matching and live facial recognition (LFR). The difference between them is that facial matching uses historical data only, while live facial recognition, assisted by AI, is based on an assistive recognition technology that works with the probability of a match between a live captured image and an image on a watchlist. This means that crowds exposed to Smart CCTV cameras are scrutinized, faces are scanned and analyzed, subjecting every person within view to an on the

spot biometric identity check. The resultant information can trigger police actions, but identified images could also be stored for eventual future investigations (Skogan, 2019).

This AI-enabled technology is already being employed around the world. In the UK, the Leicestershire Police, the South Wales Police (SWP) and the Metropolitan Police Service (MPS) have already used FRT to monitor public spaces (Big Brother Watch, 2018). The Leicestershire Police used automated or LFR in June 2015 during the Download Festival. During the event, 90,000 people were checked against a Europol watchlist and the Leicestershire Police stated that the captured images were deleted afterwards. The SWP has been using FRT in the context of public surveillance operations at large gatherings, such as outdoor festivals, sports events or public protests (Davies, et al. 2018). According to public reports, between 2017 and 2019 over 70 events were targeted and 60 persons were arrested. Between 2016 and 2019, the MPS conducted 10 test deployments, trialing automated facial recognition technology looking at both examining technical accuracy and assessing implications for policing operations (Fussey & Murray, 2019). The debate around the use of FRT for law enforcement in the UK continues and has reached the media backed by civil society organizations.

In Germany, in 2016, the Cologne Police deployed 26 stationary video cameras at the main station forecourt, around the Cologne Cathedral and at Breslauer Platz. The captured images would be stored for 14 days to be used as evidence, should any crimes in those locations be reported. The Hamburg police force has also trialed the use of automated facial recognition technology during the G20 Summit in 2018. In 2017, federal authorities launched a trial for FRT at Berlin Südkreuz train station. In December 2020, the federal government and Deutsche Bahn announced as part of increased security measures at train stations, the deployment of cameras with possible recourse to LFR (Montag et al., 2021).

In June 2001, Tampa, Florida became the first American city to start using Smart CCTV. The experiment involved using a 36-camera system along two of the main streets. The system was integrated with a “smart software” that intended to recognize wanted individuals. The project was

discontinued after two years since it was not accurate (Gates, 2010). In the last decade, initiatives spring up in the US generating great controversy. Several municipalities, starting with San Francisco, proposed to ban the technology. The discussion covers public safety, the technology’s accuracy and pervasiveness, and its fair use. Different levels of regulation have been pushed forward. In some cases, regulation allows research, development and implementation of the technology, in others a more restrictive approach has been adopted, prohibiting or limiting FRT deployment to specific circumstances.

China is very likely the country that most widely develops and implements FRT, using a surveillance system of more than 626 million facial recognition cameras. The applications of FRT cover different spheres of public life, not only public security but also mundane situations. However, a Chinese Supreme People’s Court case involving the use of FRT to enter a Zoo presents a drawback to the use of FRT in the private sector. It is worth mentioning that the guidelines do not refer to the government and how it comes in parallel to the approval of data protection regulations in the country.

In the Global South, cities such as Buenos Aires, Montevideo, Medellín, Rio de Janeiro have tested or even implemented the technology in public areas. The political arguments focus on the need to increase public security and/or find missing persons. The processes follow similar paths, however, starting with trialing the technology, investing to acquire the needed components to expand the system, implementing it and then discussing forms of regulation, mostly authorizing its use in public spaces with little safeguards and guarantees. Civil society organizations have raised concerns in terms of accuracy and fairness especially for persons and groups traditionally more vulnerable, such as women, black people, indigenous populations and trans people. The debate on regulation is, however, at an initial stage, even if the public security agenda seems to resonate particularly strongly with significant parts of the population.

The Relationships between Ethical and Human Rights Concerns in FRT for EU Regulation

Considering the opportunities and risks AI-enabled technologies represent to society, Floridi et al. (2018) defined an ethical framework for AI, based on the principles beneficence, non-maleficence, autonomy, justice and explicability. In order to approach the topic from an ethical and legal perspective, we will focus on the principles non-maleficence, autonomy and justice and how they overlap with respect for human rights, craving a path to the lawful, human-centered and responsible uptake of AI.

According to Kriebitz and Lütge (2020) three main human rights principles are to be addressed when thinking about AI regulation: the rights of an individual can be transferred only by his or her consent (principle of consent), the only justification for the use of power against the will of a person is the prevention of harm (harm principle), the use of force must be proportionate to the threat (principle of proportionality).

When we consider the use of LFR in public spaces, proportionality implies balancing existing societal problems with those that might arise by introducing a new potential solution.

Floridi et al.'s "principle of autonomy" can also be interpreted in relation to the principle of consent, since it deals with the idea that individuals have the right to make decisions for themselves, without the interference of coercive forces and by having access to the facts that lead to an informed decision. Floridi et al. (2018) approach autonomy by mainly focusing on the relation between humans and machines and how humans may delegate certain decision power on AI but should always be in control in the process and have the possibility to withdraw and regain full autonomy. However, we argue that when we look at the implementation of FRT in public spaces, autonomy and consent actually overlap to address the relationship between individuals, public authorities and technology, looking at the acceptance of surveillance technologies and acknowledging that the functioning of LFR implies certain loss of privacy for individuals.

This leads us to Floridi et al.'s "principle of non-maleficence", which we link to the prevention of harm principle from Kriebitz and Lütge. Floridi et al. (2018) consider here the use of personal data (infringement of privacy) a potential perverse impact of AI on society. Privacy can be looked at from these two angles, intertwining consent with prevention of societal harms. Thus, its loss represents a compromise or a trade-off that individuals (and the society) might be available to consent (at least, up to a certain and dynamic extent) to prevent other societal harms such as crime.

The third aspect of this discussion is the relation between the "principles of justice" and "proportionality" from Floridi et al. and Kriebitz and Lütge, respectively. When it comes to the infringement of individual rights to prevent other societal harms, the principles of justice and proportionality present complementary perspectives. Floridi et al. (2018) suggest that justice relates to equity and solidarity, this means eliminating all forms of unfair discrimination, the sharing of the benefits AI creates (at least ensuring that they are shareable) and preventing that AI introduces new harms, such as the undermining of existing social structures or excluding individuals and groups to access to certain goods and services. When we consider the use of LFR in public spaces, proportionality implies balancing existing societal problems with those that might arise by introducing a new potential solution.

The EU approach to regulating AI has been progressively laying down a framework where ethical and legal principles are intertwined, while underpinning the importance of sectoral regulations (COM, 2020). The ethical principles were defined early on: respect for human autonomy, prevention of harm, fairness and explicability (COM, 2019). Legal aspects include international law, rights and social values enshrined in the EU charter and treaties. The sectoral regulations relate, for instance, to the application of data protection law, consumer protection and competition law (COM, 2020).

In terms of FRT, the Artificial Intelligence Act (COM, 2021) states that the use of real-time remote biometric identification in publicly accessible spaces by public authorities is of unacceptable risk, as it contravenes EU values

and Fundamental Rights. The use of facial recognition technologies for law enforcement purposes potentially meet the conditions to fall under the mentioned prohibited AI systems. Nevertheless, some exceptions are considered, when it comes to leverage on these systems to search for victims of crime, prevention of a substantial and imminent threat to life or physical safety of natural persons or of a terrorist attack, detection, localization, identification or prosecution of a perpetrator or suspect of a criminal punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years. This opens the possibility to justify these surveillance systems' deployment within the EU Member States.

In response to the proposed AI regulation, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) called for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces, such as faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals, in any context. Remote biometric identification of individuals in publicly accessible spaces poses a high-risk of intrusion into individuals' private lives, with severe effects on the populations' expectation of being anonymous in public spaces (EDPB & EDPS, 2021, pp.2-3).

It is then a matter of respect for individual rights, as well a matter of recognizing and cherishing people's expectations around meanings of public space and associated democratic and cultural values, not to mention personal development. Public spaces are also areas where the individual meets the group and the community. These places are crucial to foster democratic movements promoting public assemblies, public debate and to claim rights.

Trust and FRT

Trust and accounting for privacy are paramount requirements to the uptake of AI-enabled technologies. While the concepts have been broadly theoretically defined, they highly depend on contextual circumstances, be they of cultural origin or of an even more volatile nature, to be understood at a local level. Thus, they require a

multi-dimensional analysis and respective adjustments when we look at the deployment of a specific AI system in a particular territorial, political and social context.

Local responses to the implementation of LFR in public spaces have proved diverse in different parts of the world (even from city to city within the same country). Some cities in the USA have opted out, banning the use of such technologies, while China is progressively naturalizing it (notwithstanding its recent move to limit its use for the private sector). The Global South is running a middle course. The technology is seen as useful to assist in public security and law enforcement. However, civil society organizations are slowly raising concerns that individuals, particularly from vulnerable groups, may be highly and adversely impacted by it. In the EU, the general trend seems to go towards highly restrictive regulation, even if some countries have been trailing the technology and exploring possible implementation.

Remote biometric identification of individuals in publicly accessible spaces poses a high-risk of intrusion into individuals' private lives, with severe effects on the populations' expectation of being anonymous in public spaces.

The idea of creating an ecosystem of trust to foster the uptake of AI has been one of the EU's core messages. This means that technologies should be trustworthy in terms of robustness, cybersecurity and inherent design (e.g. should not malfunction, be biased or promote unfair discrimination, be vulnerable to be corrupted) (COM, 2019), but also links to AI governance (Winfield & Jirotko, 2018). Thus, the responsible implementation of an AI system requires that the conditions for public engagement and acceptance are accounted for as well.

A survey conducted by the London Policing Ethics Panel (LPEP, 2019) in London concluded that 57% of respondents agreed that police's use of LFR was acceptable, however the degrees of acceptance depended on the specific purposes and setting in which the technology might be used.

Therefore, while people recognize the technology's potential to assist with law enforcement, the ways they are available to compromise their privacy depend on a critical assessment and valuation of harms. Another survey in the UK reached similar conclusions, 71% of the participants agree that police should be allowed to use facial recognition technology on crowds and in public spaces if it helps reduce crime. However, 46% think that people should be given the opportunity to consent or opt out of being subjected to facial recognition technology, with 28% disagreeing (Ada Lovelace Institute, 2019).

Those who had high levels of trust in the police in general were much more supportive of using LFR, perhaps because they thought the police would use the technology and their data appropriately to make policing more efficient and effective

Trust formed an important lens through which participants in these surveys viewed LFR. Those who had high levels of trust in the police in general were much more supportive of using LFR, perhaps because they thought the police would use the technology and their data appropriately to make policing more efficient and effective (LPEP, 2019, p.7).

The Role of Privacy, Consent and Proportionality

Beyond the issue of trust, to outline the implementation of live facial recognition systems in the context of public space surveillance by public authorities and for law enforcement, privacy, consent and proportionality appear as three intertwined core aspects to describe the ethics of surveillance and responsible use of AI. "Technology will continue to push the boundaries of what society thinks is acceptable" (Kim, 2019, p.118). Considering privacy as a societal value, whose loss represents a pitfall, we propose assessing this potential trade-off by questioning if

informed consent is actually achievable in this case and on a further step, how proportionality issues imply risks for equality and democratic values.

Collecting and using personal data has impacts on privacy. Taking into consideration how AI and particularly LFR or Smart CCTV systems work, part of the discourse interpreted the deployment of such technologies as a potential threat to individual privacy requirements, however privacy issues go beyond that (Möllers & Hälterlein, 2012). It is key to outline privacy beyond the individuals' sphere, not to fall into the trap of reducing privacy to secrecy and assuming that only things that are completely stowed away are worthy of protection. Privacy is a cultural representation of what is consented and socially acceptable to share within specific contexts and spheres of life. Thus, framing it as a concern for individuals, without addressing societal implications represents a narrow view on privacy (Selinger & Hartzog, 2019). This becomes ever more pressing for marginalized groups and communities, privacy may be understood as a way to protect their own lifestyles and unique forms of expression.

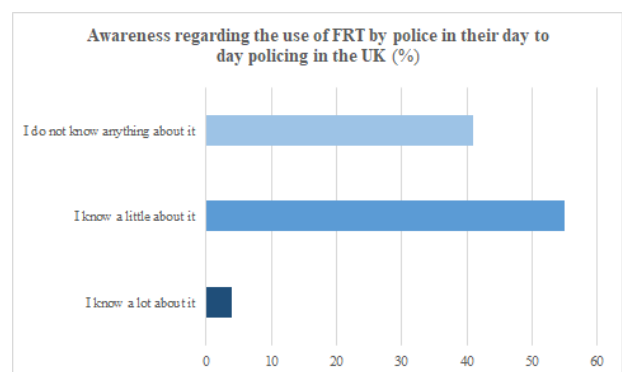


Figure 1. Awareness regarding the use of FRT by police in their day to day policing in the UK

Source: Own representation based on the survey (Ada Lovelace Institute, 2019)

Questioning whether informed consent is achievable leads us firstly to position AI-enabled systems as inherently complex and even opaque in nature. We cannot assume that people possess an appropriate level of knowledge about how the system works and how its deployment interferes with their own autonomy (see Figure 1). Fussey and Murray (2019) describe the attempt of the MPS to ensure public consent. This included uniformed officers explaining the role of the technology to the public, leafleting and signage

boards. However, the authors underpin that what might seem an appropriate level of transparency, in terms of ensuring public adherence, is often not aligned with the conditions to obtain individual consent (e.g. people need time to consider arguments and make an informed decision).

Surveillance tools bestow power on the watcher

Furthermore, if the requests for consent are too frequent people become overwhelmed and desensitized. This opens the possibility to obtain consent by exploiting their exhaustion (Selinger & Hartzog, 2019). Consent also means having the opportunity to exercise a different choice, to opt out (Fussey & Murray, 2019). If the system is deployed in areas people need access to or where they feel that avoiding them will deprive them of certain everyday life practices, their autonomy to make a decision is compromised, as their right to access public space is deemed at risk. The situation may appear as either accepting surveillance and continuing accessing public space, potentially in increased safety, or putting privacy above potentially effective policing actions. The mentioned arguments barely present an alternative. Accessing public space in increased safety, by accepting being under surveillance through systems that can be considered intrusive, seems to be an unquestionable decision when balanced with choosing privacy above effective policing actions to mitigate criminality and risking that the refusal of consent can be interpreted as a “suspicious behavior” - you should not be worried if you have nothing to hide.

Indeed, if the risk of harm is not tangible enough, people will not be able to judge the request for consent. This is even more critical if they are given seemingly good reasons to believe that the social benefits resulting from consenting to surveillance are the complete story. When “harms are framed in terms of abstract notions of privacy and autonomy or the possibility of abuse is too distant to be readily foreseeable, then people’s cost/benefit calculus may be corrupted by an

inability to take adequate stock of the risks” (Selinger & Hartzog, 2019, p.116). Furthermore, individual decisions may be conditioned if people do not feel sure about having the capacity to refuse or withdraw consent without penalty (Fussey & Murray, 2019).

The problem of consent linked with privacy in this specific context implies a high level of transparency as well. This has not always been the case with the deployment of Smart CCTV systems. Indeed, the end-interface that people will eventually need to get used to are the cameras, sometimes discretely added to the urban landscape. When CCTV systems are already deployed the upgraded level of urban surveillance is not an evident or even noticeable change for citizens crossing public space. Therefore, people scanned by such systems are likely not aware that they were subject to identity checks. This makes the need to consent to it, an even more distant conjecture, highly dependent on having access to adequate information. Without confirmation from public authorities, a citizen has only very limited possibilities to understand to which extent surveillance is being conducted and for which purposes. Therefore, surveillance tools bestow power on the watcher (Selinger & Hartzog, 2019, p.111).

LFR enables real-time location tracking and behavior policing of an entire population. The scale of implementation is ultimately in the direction of omnipresence. The banalization of surveillance can create a chilling effect that leads to the naturalization of further constraints to individual and public liberties, hampering autonomy by hindering choice and uncoerced decisions and undermining basilar democratic practices linked to fundamental rights, such as freedom of association and expression.



Figure 2. Reasoning purposes behind surveillance
Source: https://unsplash.com/photos/LkD_IH8_K8klash

The situation calls for more political scrutiny. Civil society organizations and organized groups within the community have been playing a fundamental role in exposing abuse, but also in identifying gaps and errors in the way the technology operates (it has been reported how FRT is less accurate when identifying black people, women and trans people, reproducing patterns of unfair discrimination in society). Therefore, proportionality should be addressed as a scale of balancing the benefits for society in relation to the constraints it may impose to certain rights, together with the reasoning that it might disproportionately affect specific vulnerable groups within society.

Proportionality calls for an effective assessment, starting from evaluating the threat or problem and measuring the extent to which the technology represents a solution to the identified problem. If a certain socio-spatial context experiences minor impacts due to criminality and terrorism, the use of intrusive surveillance systems to massively monitor crowds in urban space obviously cannot be justified under those premises. And even if the problem might justify additional countermeasures, it should be considered whether LFR is the adequate solution by balancing out other options that might be less intrusive and have less implications to acquired rights and established values.

Not only is proportionality about balancing the effectiveness of LFR over other methods, but it is also about explaining why the particular technique or tactic is the least intrusive necessary to achieve the desired aim (Porter, 2020, p.34).

Deploying a system by which the face of every passer-by is analyzed, mapped and their identity verified is a decision that impacts on the whole population. Not only is everyone that uses public space under surveillance without being a suspect of any crime, but the process can trigger an automated decision leading to police action. This means that an individual can be stopped in the street and asked to prove their identity, potentially overstepping the presumption of innocence.

Even if everyone is vulnerable to these harms, they disproportionately affect minorities. Bias in AI is only one of the possible causes. Different groups within the society project different intentions on public space. While some might understand it as a place to fight for rights, protest

against established power and enforce political views, others might consider these actions as threats to the status quo and feel that they should be marginalized. Thus, what one considers adequate behavior in public space is highly subjective and bound to existing social structures in which marginalized groups often have limited voice in projecting the future. The homeless have been considered a group particularly affected and vulnerable to the use of intrusive surveillance systems in public space such as LFR, leading to potential exclusion (Fontes & Lütge, Forthcoming). There are other examples of groups that depend on public space to make their living and could therefore be over exposed to surveillance mechanisms, such as beggars, street artists, musicians and vendors.

Not only is proportionality about balancing the effectiveness of LFR over other methods, but also about explaining why the particular technique or tactic is the least intrusive necessary to achieve the desired aim

Final Thoughts

Live facial recognition for law enforcement presents opportunities to assist police forces in monitoring public space and can be a tool in the fight against and prevention of crime. However, its deployment has impacts on everyone exposed to the system regardless of wrongdoing, placing all citizens in the position of being identified and monitored in public spaces. The fact that the system is highly intrusive, capturing and processing large volumes of data on (innocent) people, leads us to question whether FRT can be used as a proportional measure to fight crime.

Thus, determining whether the benefits outstrip risks means, firstly, balancing the size and scope of the proposed action against the gravity and extent of the perceived crime or harm; explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others to achieve the desired purpose; considering whether the action is of an appropriate use of the legislation; considering all

reasonable alternatives for obtaining the information sought; evidencing other methods that were considered and why they were not implemented or that they have been implemented unsuccessfully in the past (Porter, 2020).

Even if after the first assessment LFR is considered an adequate solution to solve a problem, a further assessment should be carried out, looking specifically at political and social impacts. The surveillance of populations bestows power on public authorities and governments by enabling access to privileged personal data of citizens that might be further used for additional purposes and combined with other records. This is also valid for enterprises providing the technology. Thus it should be made clear how personal data is being handled, by whom and for what purposes. Transparency is key and so is fairness. Even if the whole population is under surveillance, specific groups are disproportionately affected and exposed due to the way they use/interact in public space.

From an overarching perspective, AI's assessment should take place in a socio-technical framework, where individual's rights and social good are harmonized towards inclusive, sustainable and fair human-centered technologies, considering the complete lifecycle (i.e. from development to after deployment). On the other hand, the protection of citizens against the risks resulting from abusive or misuse of AI lies not only on regulation and public enforcement but also on the countervailing power of civil society, which proved fundamental to identify and

report abuses, trigger social movements and debate platforms to impel enforcement and offset negative impacts and undesirable societal change.

¹ Download festival: Leicestershire Police defend facial recognition scans (Jun 15, 2015). Available from <http://www.bbc.co.uk/news/uk-england-leicestershire-33132199> [Accessed Nov. 9, 2021].

² South Wales Police (SWP) on AFR <https://afr.south-wales.police.uk/#deploytitleuth-wales.police.uk> [Accessed Nov. 9, 2021].

³ Metropolitan Police Service (MPS) on LFR https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition?_cf_chl_captcha_tk__=pmd_SjM49tjoSiCT.wo1MY92lmXY0.YxDXIFn.9jakRJx8A-1630587655-0-gqNtZGzNA1CjcnBszQil [Accessed Nov. 9, 2021].

⁴ Steven Morris, Office worker launches UK's first police facial recognition legal action, *The Guardian*, (May 21, 2019)

Owen Bowcott, Police use of facial recognition is legal, Cardiff high court rules, *The Guardian*, (Sep. 4, 2019)

Jamie Grierson, Police trials of facial recognition backed by home secretary, *The Guardian*, (July 12, 2019).

David Davis, Facial recognition technology threatens to end all individual privacy, *The Guardian*, (Sep. 20, 2019).

Josh Taylor, Calls to stop NSW police trial of national facial recognition system over lack of legal safeguards, *The Guardian*, (June 30, 2021).

⁵ Examples of Civil Society Organizations engaging in the debate (UK): [Liberty](#), [Big Brother Watch](#)

⁶ Kate Conger, Richard Fausset and Serge F. Kovalski, San Francisco Bans Facial Recognition, *New York Times* (May 14, 2019).

⁷ For a general view of the different stages in the United States see the interactive map from the organization "Ban Facial Recognition". Available at: <https://www.banfacialrecognition.com/map/>.

⁸ Lauren Dudley, China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash, *The Diplomat*, (March 07, 2020).

⁹ Travis M. Andrews, China uses facial recognition software to crack down on toilet paper theft, *Washington Post* (March 21, 2017).

¹⁰ China built the world's largest facial recognition system. Now, it's getting camera-shy, *Washington Post* (July, 30, 2021).

¹¹ For a broad overview of situation in Latin America, see: Reconhecimento facial na América Latina: tendências na implementação de uma tecnologia perversa. *Al Sur* (Nov. 2021).

References

- Ada Lovelace Institute (2019). *Beyond face value: public attitudes to facial recognition technology*. Report and survey data. <https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/ce> Institute
- Big Brother Watch (2018). Face Off. The lawless growth of facial recognition in UK policing. <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf>
- van Brakel, R. (2021). How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium. *Surveillance & Society*. 19 (2), 228-240.
- Chen, S., Pan ZX., Zhu HJ., Wang, Q., Yang, JJ., Lei, Y., ... Pan, H. (2018). Development of a computer-aided tool for the pattern recognition of facial features in diagnosing Turner syndrome: comparison of diagnostic accuracy with clinical workers. *Sci Rep*. 8 (1).
- Davies, B., Innes, M. & Dawson, A. (2018) Universities' Police Science Institute Crime & Security Research Institute, Cardiff University. <https://afr.south-wales.police.uk/wp-content/uploads/2019/10/AFR-EVALUATION-REPORT-FINAL-SEPTEMBER-2018.pdf>
- European Commission (COM) (2019), Ethics guidelines for trustworthy AI. Available at: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>
- European Commission (COM) (2020), White Paper on Artificial Intelligence - A European approach to excellence and trust. Brussels
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Lütge, C., ... Vayena, E. (2018). AI4People –An Ethical Framework for a Good Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*. 28, 689- 707.
- Fontes, A. C. & Lütge, C. (Forthcoming) Surveillance and power relations. The use of facial recognition technologies and remote biometric identification in public spaces and impacts on public life. *Revista de Direito Público*
- FRA - European Union Agency for Fundamental Rights (2020). Facial recognition technology: fundamental rights considerations in the context of law enforcement. Vienna. <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>
- Fussey, P. & Murray, D. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, Human Rights Centre. <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf>
- Gates, Kelly. (2010). The Tampa "Smart CCTV" Experiment. *Culture Unbound : Journal of Current Cultural Research*. 2. 10.3384/cu.2000.1525.102567.
- Montag, L., Mcleod, R., De Mets, L., Gauld, M., Rodger, F. & Pelka, M. (2021). The Rise and Rise of Biometric Mass Surveillance in the EU. EDRi (European Digital Rights) and EIJI (Edinburgh International Justice Initiative). Brussels
- Hirose, M. (2017). Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology. *Connecticut Law Review*. 377.
- Introna, L. D. & Nissenbaum, H. (2010). Facial Recognition Technology: A Survey of Policy and Implementation Issues. Lancaster University Management School, The Center for Catastrophe Preparedness and Response. Working Paper.
- Jeon, B., Jeong, B., Jee, S., Huang, Y., Kim, Y., Park, G., ... Choi, T. (2019) A Facial Recognition Mobile App for Patient Safety and Biometric Identification: Design, Development, and Validation, *JMIR Mhealth Uhealth*, 7, 4 doi: 10.2196/11472.
- Kim, N. S. (2019) *Consentability. Consent and its Limits*. Cambridge University Press
- Kong, Y., & Fu, Y.R. (2018). Human Action Recognition and Prediction: A Survey. *ArXiv*, abs/1806.11230.

- Koskela, H. (2003). 'Cam Era' – the contemporary urban Panopticon. *Surveillance & Society*, 1(3), 292-313.
- Kriebitz, A. & Lütge, C. (2020). Artificial Intelligence and Human Rights: A Business Ethical Assessment. *Business and Human Rights Journal*. 5(1), 84-104. doi: 10.1017/bhj.2019.28.
- London Policing Ethics Panel (LPEP) (2019). Final Report on Live Facial Recognition. London. <http://www.policingethicspanel.london/reports.html>
- Möllers N. & Hälterlein, J. (2012). Privacy issues in public discourse: the case of "smart" CCTV in Germany, *Innovation: The European Journal of Social Science Research*. doi:10.1080/13511610.2013.723396
- Pauwels, E. (2020). Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention Opportunities and Challenges for the International Community. *Global Center on Cooperative Security*. <https://www.jstor.org/stable/resrep27551>
- Porter, A. (2020). *Facing the Camera. Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales*. Surveillance Camera Commissioner. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf
- Ryoo, M.S. (2011). Human Activity Prediction: Early Recognition of Ongoing Activities From Streaming Videos. *IEEE International Conference on Computer Vision*, Barcelona, Spain. http://cvrc.ece.utexas.edu/mryoo/papers/iccv11_prediction_ryoo.pdf
- Sawhney, S., Kacker, K., Jain, S., Singh, S.N. & Garg, R. (2019). Real-Time Smart Attendance System using Face Recognition Techniques. *9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. doi: 10.1109/CONFLUENCE.2019.8776934.
- Koskela, H. (2003). 'Cam Era' – the contemporary urban Panopticon. *Surveillance & Society*, 1(3), 292-313.
- Selinger, E. & Hartzog, W. (2019). The Inconsistency of Facial Surveillance. *Loyola Law Review*. 66, 101-122.
- Singh, T. & Vishwakarma, D.K. (2019). Video benchmarks of human action datasets: a review. *Artif Intell Rev* 52, 1107–1154. doi:10.1007/s10462-018-9651-1.
- Skogan, W. G. (2019). The future of CCTV. *Criminology & Public Policy*. 1–6. doi: 10.1111/1745-9133.12422
- Su, Y.S., Suen, H.Y. & Hung, K.E. (2021). Predicting behavioral competencies automatically from facial expressions in real-time video-recorded interviews. *J Real-Time Image Proc* 18, 1011–1021. doi:10.1007/s11554-021-01071-5
- Tucker, A. (2020). The Citizen Question: Making Identities Visible Via Facial Recognition Software at the Border. *IEEE Technology and Society Magazine*, 39, 4, 52-59, doi: 10.1109/MTS.2020.3031847.
- Winfield, A. F. T. & Jirotko, M. (2018) Ethical governance is essential to building trust in robotics and artificial intelligence systems. *Phil. Trans. R. Soc. A*. 376: 20180085. doi:10.1098/rsta.2018.0085
- Yang, D., Alsadoon, A., Prasad, P.W.C., Singh, A.K. & Elchouemi, A. (2018). An Emotion Recognition Model Based on Facial Recognition in Virtual Learning Environment, *Procedia Computer Science*, 125, 2-10. doi:10.1016/j.procs.2017.12.003.