THE TWIST OF FATE, OR ALL YOU NEED TO KNOW ABOUT FACIAL RECOGNITION IN DEMOCRATIC POST-GDPR EUROPE

by Olga Kyryliuk, Ph.D.,
Open Internet Leader 2019-2020
for the Open Internet for Democracy Initiative

MAY 2020

CONTENTS

INTRODUCTION

Smile, you are being filmed by a hidden camera! Something that used to be a funny joke of reality shows in the late '90s, does not always bring a smile to our faces in 2020. Today, facial recognition technology is penetrating our life faster than anyone could expect. As individuals, we welcome the speed and convenience gained by using our faces to open our phones, pass through airport security controls, and pay for coffee. Likewise, governments around the world are taking advantage of advancements in facial recognition technology, claiming it helps to make the lives of their citizens safer. For many, the use of this technology does not create much cause for concern. First, because we are unlikely to know all of the circumstances in which facial recognition is applied, and even if we did know, we may tend to feel that the presumed benefits to our safety and security outweigh any arguments against the use of such technology by the police. And second, as law-abiding citizens, many feel they have nothing to hide, and therefore do not mind the potential intrusion by a scanning camera if in fact that footage one day helps to catch a criminal.

A recent study conducted by Freie Universität and the University of St. Gallen among residents of China, Germany, the United Kingdom, and the United States shows that on average, 51 percent of individuals generally accept facial recognition technology, while 22 percent are mostly skeptical of it. China has the highest acceptance rate (67 percent), with the most skepticism voiced by Germans (32 percent). In the US and the UK, acceptance is in the middle with 47 and 50 percent respectively. Private or personal use of facial recognition technology (such as smartphones or other smart devices and cameras used in the household) is met with more acceptance than its use by the government (52 percent versus 42 percent), while there is still a lack of trust in commercial companies as providers. Only 9 percent of Germans and 12 percent of Chinese, English, and Americans are ready to unconditionally tolerate facial recognition performed by state authorities. Germans show the strongest resistance - 18 percent, with 51 percent of respondents ready to accept public use of facial recognition under certain circumstances. In China, the UK and the US strong opposition reaches 4, 14, and 15 percent respectively, with conditional approval ranging from 47 to 57 percent.

... as law-abiding citizens, many feel they have nothing to hide, and therefore do not mind the potential intrusion by a scanning camera...

According to data released by Paris-based consulting company Ipsos, the government's use of artificial intelligence (AI) and facial recognition is supported by the majority only under certain circumstances and subject to strict regulations. French, Americans (16 percent each), Germans,

Chinese, and British (17 percent each) respondents are among those who are the least willing to give up their privacy, while Russians (23 percent) and Swedish (30 percent) are more understanding of government positions and more receptive towards privacy restrictions. At the same time, Germany has the highest rate (24 percent) of total disapproval for the government's use of these technologies, followed by the US (20 percent), China (18 percent), Russia, and Great Britain (14 percent each). Support for limited and restricted governmental use of AI and facial recognition varies from 59 percent in Germany to 69 percent in Great Britain. The figures are slightly different in the above surveys, which can be explained by different methodologies and differently worded questions answered by the respondents.

... while the world is still frantically trying to comply with the rules set by the European Union (EU), the very same countries within the EU are finding loopholes in the GDPR to create surveillance states around the continent.

Nevertheless, any technology can be used for both noble or nefarious purposes. We used to believe (or we've been led to believe) that technology is bad only when it is used by an autocratic government, with China often cited as the most vivid example. Deployment of technology by other countries, especially those considered to be governed democratically, is typically presented as being guided by safety and security concerns, and not intentionally targeted to the detriment of the citizens. Even more so, the last ones you would suspect of any technological abuses at the expense of privacy are the European countries that committed themselves - under the General Data Protection Regulation (GDPR) - to the highest data protection standards in the world. And while the world is still frantically trying to comply with the rules set by the European Union (EU), the very same countries within the EU are finding loopholes in the GDPR to create surveillance states around the continent.

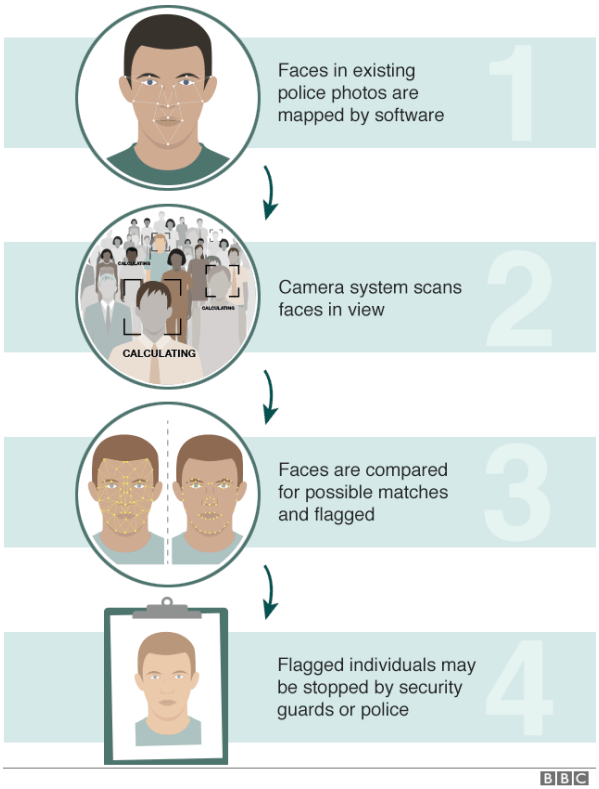
Our faces are central to who we are. They are key to our identity. The GDPR classifies facial images as biometric data when they are processed through a specific technical means, enabling the unique identification or authentication of a person. Biometric data are considered particularly sensitive in relation to fundamental human rights and freedoms and, therefore, require special protection. As a general rule under GDPR, their processing is prohibited but could be permitted, *inter alia*, for the performance of a task carried out in the public

interest, or in the exercise of official authority. As will be described in several cases below, this provision within the GDPR is frequently referenced by national authorities looking for justifications to roll out video surveillance systems with automated facial recognition.

To understand why facial recognition does matter, we need to differentiate it from the simple recording performed by closed-circuit television (CCTV) cameras. As opposed to the videos and images captured on CCTV, when the facial recognition technology is applied, the unique features of our faces (distance between eyes, width, and length of the nose, the shape of cheekbones, etc.) are being scanned and processed by an algorithm that creates a facial map (image) of a person. This image is then compared against other images uploaded to a particular database. If a match is found, the system provides a notification. As image databases grow increasingly larger, and algorithms have more time to train on the collected data, the closer we come to a time in which all persons will be machine-identifiable wherever they are.

Our faces are central to who we are. They are key to our identity.

How does live facial recognition work?



When we provide our fingerprints or DNA samples we do so consciously and generally for a specific purpose. In the case of facial recognition, our biometric data is, as a rule, taken without our knowledge and consent. Even if prior notification is given, it is often difficult - if not impossible - to avoid the cameras, leaving an individual with no option other than having their face scanned.

The adverse effect of surveillance technologies on human rights has been raised by United Nations Special Rapporteur on freedom of opinion and expression, David Kaye. In a 2019 report submitted to the UN Human Rights Council, he mentioned facial recognition technology among highly sophisticated surveillance tools, calling for an immediate moratorium on the sale, transfer, and use of such intrusive technologies until human rights-compliant regulatory frameworks are in place.

Video surveillance is already being tried out by many governments, with some of them becoming especially fascinated by its potential for unlimited and comprehensive real-time monitoring. According to the British research company Comparitech, London is among the top 10 most surveilled cities in the world, the only European city at the top of the list, alongside eight Chinese cities and Atlanta, Georgia, in the United States. The British capital is using 68.4 CCTV cameras per 1000 people. Moscow and Berlin are closing out the top 20 list with 11.7 and 11.18 cameras per 1000 people respectively. Among other European cities that made it to the top 50 are Warsaw, Vienna, St. Petersburg, Madrid, Budapest, Athens, Paris, Sofia, Nice, Prague, Cardiff, Kyiv, and Rome. Although the study did not distinguish between cameras equipped with facial recognition technology and those without, one of the more significant findings is that the presence of more cameras does not necessarily result in improved public safety or a lower crime index.

The scope of AI surveillance around the world, including facial recognition, can be easily checked via an interactive map compiled by the Carnegie Endowment for International Peace. While it does not distinguish between legal or unlawful uses of AI surveillance, it does demonstrate the potential of the technology to transform governance models. Given this paper's specific focus on the deployment of facial recognition technologies by European countries, filtering of the results revealed that quite a few resort to scanning faces of their citizens, including Czechia, Denmark, France, Germany, Malta, the Netherlands, Russia, Serbia, Spain, Switzerland, Ukraine, and the United Kingdom.

With facial recognition making its way across democratic Europe, should we be getting anxious about this potential expansion of digital authoritarianism, or should we be feeling safer under the watchful eyes of so many different governments? This paper will look at specific examples of how facial recognition technology has been applied across Europe and will show how tempting it is for even long-standing democracies to watch their citizens. We will also shed some light on the blurry line between democratic governance using technology to improve public safety, and the Orwellian state of mass surveillance. Despite statements indicating adherence to the former, many states have nevertheless failed to acknowledge or notice that they have crossed to the other side of the blurry line.

Structurally, this paper covers the approach to facial recognition undertaken in Europe both at the EU level and at a national level by the countries traditionally pointed to as an example of democratic governance, such as the United Kingdom, Sweden, France, and Germany. It also provides an insight into the facial recognition practices applied by Russia, which is usually placed at the other extreme alongside other autocratic countries in favor of strict limitations of an individual's privacy. The paper further shows how surprisingly unanimous all of these countries can be in abusing the surveillance potential of facial recognition technology.

ON ONE HAND, THE EU IS UNDECIDED ABOUT FACIAL RECOGNITION TECHNOLOGY

In February 2020, the European Commission released a long-awaited white paper on the European approach to Artificial Intelligence (AI). In the document, the Commission acknowledges that the gathering and use of biometric data for remote identification purposes carry specific risks for fundamental human rights, namely the rights to privacy, personal data protection, freedom of expression, and assembly. Remote biometric identification is defined as a process for establishing the identities of multiple persons with the help of biometric identifiers (e.g. fingerprints, facial image, iris, vascular patterns) at a distance, in a public space and in a continuous or ongoing manner by checking them against data stored in a database. In connection to facial recognition, identification means that the template of a person's facial image is compared to many other templates stored in a database to identify any potential matches. In accordance with the current EU data protection rules and the Charter of Fundamental Rights, AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards. The Commission acknowledged that the use of AI applications for the purposes of remote biometric identification would always be considered high-risk. It also committed itself to launch a broad public debate on the specific circumstances that might justify AI usage for remote identification in public spaces.

It is noteworthy, however, that the final draft of the White Paper differs significantly from the initial text leaked in December 2019, two months prior to the official publication. In the paper's final draft, the term "facial recognition" was omitted (referring now to remote biometric identification in general), as well as specific concerns around the usage of this technology by the public authorities and the implications of collecting and processing personal data without the explicit individual's consent under the GDPR. Perhaps more importantly, the initial draft contained a provision suggesting the introduction of a time-limited ban (three to five years) on the use of facial recognition technology in public spaces. The purpose of this suggestion was to allocate enough time to assess the impact of such technology and to develop possible risk management measures in order to avoid any abuses, as well as provide proper safeguards for human rights. Exceptions were envisioned for research and development activities, as well as for security purposes subject to a court decision. However, this suggested approach came with a caveat that it could potentially slow down technological development in the region. Based on the omission of this component from the February version, it would appear that Europe is firmly determined to keep pace with the US and China, and does not want to put off usage of AI, including facial recognition technology, any longer. It is an interesting change of approach given how much effort had been put into the

creation of the GDPR, and how zealously the EU has been defending its values and adherence to human rights.

...Europe is firmly determined to keep pace with the US and China, and does not want to put off usage of AI, including facial recognition technology, any longer.

The discussions around a possible blanket ban on the use of facial recognition technology in the EU (even if temporary) did not escape the attention of tech giants like Microsoft and Alphabet (parent company of Google). Both companies voiced their positions, which interestingly, appeared to take opposite viewpoints. Microsoft President and Chief Legal Officer Brad Smith criticized the ban as too severe, stressing that the way to improve technology is through its use, not by banning it. However, Alphabet's CEO Sundar Pichai noted that the potential use of facial recognition technology for "nefarious purposes" could provide justification for putting in place the moratorium. Regardless, legislators need adequate time to create effective legal frameworks and to clarify how the technology should and would be used, especially when such technology is both of high risk and high value.

About the same time as the release of the White Paper, European Commission Vice-President for Digital Margrethe Vestager acknowledged that automatic facial recognition contradicts the GDPR since a person has not given their explicit consent. However, she also mentioned that public security concerns would constitute a valid exception from a general ban on automatic identification. And while the European Commission will be considering various options of dealing with facial recognition technology, EU member states have been given full discretion to decide whether or not to deploy remote facial recognition and if so, in what specific ways and cases.

Currently, it appears very unlikely that the Commission will once again review its approach and turn everything upside down by suddenly taking a strong stand on the protection of human rights. If a temporary ban on the deployment of facial recognition technology was going to be introduced, it would have been kept in the final draft of the document. Its ultimate omission, and such a substantial revision of the draft text instead, demonstrates the EU's willingness to prioritize technology over privacy concerns. Despite this, the resulting frustration and criticism coming from human rights advocates from across the EU might leave the door open for possible future revisions, particularly after considering input received during the White Paper's public consultation period, which runs through 14 June 2020.

ON THE OTHER HAND, THE EU IS PRETTY SURE ABOUT FACIAL RECOGNITION TECHNOLOGY

While the EU's paper is still "white" and therefore still open for modification, subject to feedback received during the public consultation period, another initiative happening in parallel leaves little doubt that facial recognition will not only become a reality for the EU citizens but a very controlled version of reality, thoroughly monitored by police forces. Recently, The Intercept, an investigative news organization, announced that it received a leaked EU report drafted by the national police forces of 10 EU member states, led by Austria and circulated internally in November 2019. It unveils plans to create an interconnected network of national police facial recognition databases kept by all member states, with Europol expected to facilitate the exchange of facial and other biometric data with non-EU states. Moreover, the European network might be subsequently connected with similar US databases enabling the transatlantic exchange of huge amounts of biometric data.

Allegedly, the report was produced as part of the discussions on expanding the Prüm system created in 2005 by seven countries (Austria, Belgium, France, Germany, Luxembourg, the Netherlands, Spain). The system, which was eventually joined by seven other countries (Bulgaria, Estonia, Finland, Hungary, Romania, Slovakia, Slovenia), enabled a cross-border exchange of DNA, fingerprint, and vehicle registration data aimed at more effectively combatting terrorism, cross-border crime and illegal migration. Additionally, the European Commission paid a total of 1.2 million Euros for two separate studies conducted by consultancy companies regarding possible adjustments to the Prüm system, such as incorporating the exchange of facial data, and facial recognition deployment in criminal investigations. In response to The Intercept's inquiries regarding the leaked report, a spokesperson for the European Commission acknowledged the prospect of adding facial recognition data to the Prüm network but did not provide any further details.

Looking at the White Paper in conjunction with the proposed changes to the Prüm system extension, it might appear that both initiatives are simply parts of the same puzzle.

Although it appears that these proposals are still in their early stages, and may not ultimately result in the adoption of legislation at the EU level, privacy advocates fear it is merely a sign of things to come. Otherwise, why would the European Commission spend such a significant amount of money studying the potential practical usages of technology so

tempting and powerful as automated facial recognition? Looking at the White Paper in conjunction with the proposed changes to the Prüm system extension, it might appear that both initiatives are simply parts of the same puzzle. In light of the above, the European Commission's shift away from its proposed plan to introduce a moratorium on automated facial recognition in public spaces does not come as much of a surprise. Moreover, it leads one to wonder whether the initial draft containing such an eye-catching component for human rights advocates might have been intentionally leaked in order to distract the attention of the public away from the real intentions of the regulator to entrench its grip on an individual's privacy by making few last-minute amendments.

THE UK's LONG SLIDE TOWARDS FACIAL RECOGNITION

In Europe, the UK is probably one of the most interesting examples of the application of facial recognition technology, both because the country's police forces have been using the technology for a number of years, but also because it is where for the first time, a court looked into the issue of using automated facial recognition (AFR) technology. In a landmark case, Edward Bridges, a civil liberties campaigner, and a former Cardiff councilor, challenged the legality of deploying facial recognition technology within a pilot project called "AFR Locate". Bridges was specifically concerned about the threats that AFR might pose to privacy and personal data protection.

AFR Locate enables the processing of digital facial images from live CCTV feeds by extracting biometric faceprints of passersby and comparing them in real-time to images of wanted persons included in police watchlists. The South Wales Police (SWP) claimed that it always informs the public about usage of AFR Locate at a specific event or in a specific area by installing signs and disseminating information leaflets.

Bridges believes that the use of AFR Locate was contrary to the requirements of the Human Rights Act 1998 and the data protection legislation. His complaint specifically referenced two different occasions in which his face was scanned by the cameras: 1) on Queen Street, a busy shopping area in Cardiff, on 21 December 2017; and 2) when participating in a peaceful protest against the Cardiff Arms Fair during the Defence Procurement, Research, Technology and Exportability Exhibition at the Motorpoint Arena on 27 March 2018.

In the first case, the SWP deployed a single marked AFR-equipped van planning to detect and detain wanted priority and prolific offenders, with 919 names included in the watchlist. The system alerted police of ten possible matches, including two false positives. Of the eight remaining matches, police went on to make two arrests. In the second case, the AFR was deployed based on observations from previous years when the exhibition attracted disorder, and

protesters caused criminal damage. On this occasion, one correct match was detected, but no arrests were made. In both cases, Bridges claimed that the collection and processing of his facial biometric information were conducted without his knowledge or consent. He also stressed that it was impossible to notice a sign warning about AFR screening until it was too late to avoid it. The SWP stated that by the time of the hearing it was no longer possible to check whether Bridges had in fact been scanned by the cameras. Even if his facial biometric information had been processed by the AFR system, he had not matched with any of the individuals on the police watchlist, and therefore all the data had been immediately deleted.

In the span of only two years (2017 and 2018), the SWP deployed AFR Locate on 50 different occasions, resulting in the scanning of approximately 500,000 faces. These are impressive numbers when considering the speed of information processing and the potential consequences for an individual's privacy in the event the government decides not to delete the collected biometric data, but instead use it for strengthening surveillance over the general public, not just those suspected of criminal wrongdoing.

In Bridges' case, the High Court in Cardiff concluded that the SWP's use of AFR Locate did in fact meet the criteria of the Human Rights Act, namely because on each occasion the system was deployed for only a limited time, and for specific and limited purposes. The Court noted that unless the image of a member of the public matched a person on the watchlist, all related data, including personal data, were deleted immediately. Therefore, it found the processing of personal data to be fully lawful.

Two months after the September 2019 judgment, Bridges was granted permission to appeal, with the Court of Appeal expected to hear the case by January 2021. While there is still a long way to go, the appeals process provides some hope for privacy advocates that the initial judgment will be reconsidered, given its potential impact on the public at large. Meanwhile, Bridges strongly maintains his position that indiscriminate AFR scanning poses a significant threat to an individual's privacy. Moreover, if these concerns are being raised in a country purported for the last several centuries to be an example of democratic governance, what then should we expect from authoritarian states now able to dramatically scale up their surveillance tactics due to technological progress?

During 2017-2018 the SWP deployed AFR Locate on 50 different occasions, resulting in the scanning of approximately 500,000 faces.

SAME AS THE WELSH COURT, LONDON POLICE SEE NO REASON NOT TO USE FACIAL RECOGNITION

In January 2020, the London Metropolitan Police Service (MPS) announced the launch of Live Facial Recognition (LFR) technology in locations where, according to intelligence data, serious offenders are most likely to show up. Officially, the MPS claims that LFR is used to improve investigations of serious violence, gun and knife crime, child sexual exploitation, and to better protect the vulnerable. LFR cameras are installed in specific areas, usually with large flows of people, and scan the faces of passersby. These scanned images are subsequently compared to images in a watchlist compiled by the police or the courts. When the system finds a match it sends an alert to police officers present on the scene who then must make a decision whether or not to stop a person flagged by the system. Similar to the Welsh case, the areas under LFR screening are required to be clearly marked. It is mentioned on the MPS website that every person is free in making a choice to avoid scanning and pass through the area not covered by the camera. However, in practice the MPS' tolerance of those wishing to avoid being scanned is much lower, resulting in cases in which the MPS fined individuals for covering their faces where LFR was in place, citing suspicious behavior.

The MPS' adoption of LFR has raised the concern of human rights activists in the UK. Big Brother Watch even started a campaign against facial recognition surveillance and is collecting signatures under a respective petition. Additionally, the UK Information Commissioner's Office (ICO) repeatedly called upon the government to immediately introduce a statutory and binding code of practice for LFR in order to ensure consistency and transparency in its deployment. The ICO stressed the importance of multistakeholder consultations during the code drafting process. According to the ICO, an appropriately governed, targeted and intelligence-led LFR deployment may meet the threshold of a strict necessity for law enforcement purposes. A more categorical stance has been taken by UK Biometrics Commissioner Paul Wiles who emphasized the importance of legislative regulation of new biometric technologies such as LFR, believing that it is up to the Parliament to decide whether LFR has to be used by the police and for what purposes.

The London Policing Ethics Panel prepared a comprehensive review of ten cases between 2016-2019 in which the MPS deployed LFR technology. The Panel acknowledged important ethical concerns related to LFR but did not find them sufficient to fully reject its usage in police operations. At the same time, in order to make LFR deployment ultimately transparent and reduce potential risks, it recommended that for every potential deployment its usage should be checked against five conditions: 1) significant public safety benefits; 2) no gender or racial bias; 3) necessary and proportionate deployment; 4) engagement of skilled staff; and 5) strict guidelines ensuring a balance between LFR benefits and potential intrusion in private life.

MPS' response to the Panel's report followed six months later, at the end of January 2020, providing an overview of MPS' compliance with the Panel's recommendations. It largely referenced the LFR's ability to improve the chances of finding wanted individuals due to the system's function providing proactive notifications. MPS also stated that the decision whether or not to stop a person alerted by the system is taken by a police officer, claiming that it is a human - and not the technology - that plays the deciding role. Moreover, to avoid accusations of potential unconscious bias, all LFR operators and engagement officers undergo special training, and each case of LFR deployment is subject to several levels of oversight.

The introduction of any new technological tool, especially one that is considered as intrusive for an individual's privacy as LFR, should at least be justified by its efficiency in fulfilling a stated goal. It is no wonder that the MPS prominently referred to the improved efficiency of suspect identification in cases of LFR deployment. However, the numbers usually give a better understanding of the situation. Pursuant to an independent report from researchers at the University of Essex, only eight out of 42 (19.05 percent) system-generated alerts resulted in verifiably correct face recognition matches during six cases of LFR deployment in 2018-2019. Notably, the size of the watchlists was considerably longer and ranged in each case from 306 to 2,401 individuals.

The introduction of any new technological tool, especially one that is considered as intrusive for an individual's privacy as LFR, should at least be justified by its efficiency in fulfilling a stated goal.

"MOSCOW NEVER SLEEPS" AND ALWAYS WATCHES YOU

"Moscow never sleeps" claims DJ Smash in his popular eponymous single. In the years since the song's 2008 release, the city's authorities have utilized its resources to make a wakeful city also a watchful city.

With surveillance in mind, Moscow began rolling out facial recognition technology in 2017 with only 1,500 testing cameras; by 2020 the city was equipped with 105,000 cameras, each connected to a facial recognition system. Another 65,000 cameras without facial recognition functionality are deployed across Moscow, bringing the total number of cameras to 170,000. The city authorities purchased their facial recognition technology from a Russian AI developer NtechLab, famous for its mobile application FindFace that was popular in 2010 and enabled image-based person search in the Russian social network, Vkontakte. NtechLab's representatives state that they managed to

overcome ethnic bias intrinsic to similar systems by using special neural networks for image comparison and made the system independent from regular face training. NtechLab revealed that it is currently testing prototypes of high-tech glasses that would alert police officers when wanted persons were in close proximity. However, the company says that so far there has been no agreement with city authorities about the usage of such glasses by Moscow police.

Moscow authorities are trying to create a centralized city-wide system connected to city cameras, intercoms, and traffic lights. The facial recognition system is expected to function in real-time and to be linked to law enforcement databases. By 1 September 2020, the facial recognition system will be fully operational across Moscow's subway system and is also planned to be used in other forms of public transport and in stations. In support of this ambitious initiative, city authorities continue to buy hardware able to process and save such huge amounts of video data, as well as to monitor the public spaces hosting mass events.

Although the system still appears to be in a preparatory phase in the run-up to creating a large-scale surveillance system inside the Russian capital, it has nevertheless already been tested and proven to be efficient, albeit in a very different case. In February 2020, as Moscow began to implement strict quarantine restrictions on those arriving from China due to COVID-19, one recently arrived passenger initially tested positive for the virus and was subsequently hospitalized from home. The passenger's flatmate was ordered to stay at home for the following two weeks but she violated the order by going to meet a friend. What followed subsequently is impressive. Using CCTV footage, authorities were not only able to identify the girl and her friend but also the taxi driver who brought the original passenger home from the airport. It is astonishing how comprehensive the tracking of a person's life can be, even with seemingly innocuous cameras placed here and there around the city. The times when you could go unnoticed in your pajamas to buy milk in a grocery store around the corner are over. We have literally stepped into a world in which it is entirely possible that our loved ones know far less about us than the state officials behind the lens of a city's monitoring cameras.

If implemented according to design, the facial recognition project in Moscow will become the largest surveillance initiative in Eastern Europe, challenging the Chinese leadership in this field, if any leadership is acceptable in implementing such authoritarian practices. It is unsurprising that under such circumstances, civil society activists are expressing their concerns about privacy and data protection, both of which may hardly seem to matter in a society where citizen's every step is closely monitored and analyzed. On top of that, the system itself is not without bugs. It has been reported that access to live recording or camera archives can be easily purchased on the black market, putting citizens' privacy as well as their physical safety under serious and very real threat.

If implemented according to design, the facial recognition project in Moscow will become the largest surveillance initiative in Eastern Europe, challenging the Chinese leadership in this field, if any leadership is acceptable in implementing such authoritarian practices.

A RARE CASE OF JUDICIAL UNANIMITY IN RUSSIA AND THE UK

In April 2018, Moscow resident and activist Alyona Popova was fined by the court for organizing an unauthorized individual protest in front of the parliament building. She claimed afterward that the court managed to identify her based on the recordings from the video monitoring system that enlarged her face at 32 times the scale, a telltale sign of facial recognition. Supported by RosKomSvoboda, an advocacy and human rights organization, she filed a lawsuit demanding a ban on facial recognition technology, citing its illegality. Popova's complaint invoked the collection of biometric data without consent, which violates Russia's data protection law and infringes upon an individual's privacy. In addition, she claimed that there were no procedures in place that would allow a person to check what data is collected, and to request the removal of such data from any databases. Given the regularity with which one may visit locations that are under video surveillance, it could be asserted that an individual's rights are being violated on a daily basis.

However, in November 2019, the court dismissed the lawsuit, stating that the video monitoring system does not perform an identification function, and instead simply compares images taken by a camera with the ones kept in law enforcement databases. According to the court's ruling, the Moscow Department of Information Technologies (DIT), which is in charge of the city's video monitoring system, does not have access to personal data. Moreover, the court believes that the images taken by the cameras and not accompanied by any other identification information do not constitute biometric personal data and therefore do not require obtaining an individual's prior consent.

In court proceedings, DIT noted that Popova's identity was in fact established by a police officer, who checked her passport on the spot, and was not based on the video recordings, as she stated. It was also pointed out that the use of facial recognition technology is not prohibited, and the state was therefore entitled to collect information in this manner. Beyond its use for

recognizing individuals, facial recognition technology was cited as also useful for monitoring public infrastructures, such as identifying roads in need of repair, and locations where garbage removal has not taken place. However, this argument raises a logical question: how are the cameras supposed to identify the "faces" of inanimate objects, and how is the additional technological investment justified in such cases.

As expected, Popova appealed the court's decision, but it was later upheld by the appeals court. Not satisfied with the ruling, Popova stated her intent to take the case to the European Court of Human Rights, but in order to do so, she is required first to exhaust all legal options inside Russia.

In January 2020, Popova filed a second lawsuit requesting to ban facial recognition during mass protests. The lawsuit followed a September 2019 demonstration in support of political prisoners at which Popova claims all security gates at the entrance to the protest area were equipped with facial recognition cameras. She clarified that she is not fighting against video recording in general, but rather against built-in facial recognition technology leading to the collection of personal data. Popova asserts that everyone has a right to know how databases of images are operated, where data is saved, and who has authorized access to them. The court closed the proceedings at the beginning of March explaining that according to the Code of Administrative Proceedings the same issue of contesting actions in violation of the human rights of an indefinite number of people cannot be subject of a court review twice, and made a reference to the valid court decision in Popova's first lawsuit where she made similar claims. Another appeal was filed, pending its hearing as of the end of April 2020. Meanwhile, DIT reiterated that facial recognition technology is in compliance with national legislation, does not collect any biometric data, and is aimed solely at ensuring the safety of city residents.

Separately, RosKomSvoboda, the organization that provided legal support for Popova in her first court case, is running a public campaign against facial recognition, calling for a five-year moratorium on the implementation of facial recognition systems, public oversight over data access procedures, and increased penalties for data access abuses and leaks. They have also launched an online petition to ban the usage of facial recognition technology in the city video monitoring system, which had already collected over 40,000 signatures by the end of April 2020.

MEANWHILE, SWEDEN GAVE FACIAL RECOGNITION A TRY TO MONITOR SCHOOL ATTENDANCE

In August 2019, the Swedish Data Protection Authority (DPA) fined the Skellefteå municipality almost 19,000 Euros (200,000 SEK) for using facial recognition in Anderstorp Secondary School to monitor the class attendance of 22 students over a three-week period. The DPA found facial recognition to be in violation of the GDPR, determining it as a disproportionate use of the technology in relation to the objective it was trying to address. In defending its use of facial recognition, the school board referred to improved efficiency of registering attendance, a process that takes ten minutes per lesson. Based on these calculations, the school board estimated they could save over 17,000 hours spent on attendance taking per year, which could instead be put towards teaching. Despite the school board's optimism for the technology's future uses, the DPA pointed them to the serious breaches of personal data protection rules.

This case marked the first time in which the Swedish DPA issued a fine under the GDPR...

Bearing some of these data protection considerations in mind, the school had in fact received explicit consent of the students' guardians, who were even given the possibility to opt-out of the facial recognition system and remain with the current method of registering attendance. However, the DPA noted that in this particular case, consent cannot constitute a legal basis for the processing of the students' data, as they are in a position of dependence on the school, and therefore, their consent is not really free to give. At the same time, the DPA stated that while administering student attendance is a school's obligation, there is no legal justification for using such an intrusive and disproportionate method as a facial recognition system, given that alternative ways already exist that do not require the processing of sensitive personal data. Children have every right to expect a sufficient level of privacy in their everyday school environment, especially after they enter a classroom, which is not considered to be a public space requiring strict monitoring. Even a very selective and time-limited application of facial recognition did not prevent the DPA from declaring it a substantial infringement of the students' integrity.

This case marked the first time in which the Swedish DPA issued a fine under the GDPR, which could have been bigger if the school board had used facial recognition for a longer period of time. To prevent further usage of facial recognition, the DPA issued a respective prohibitive warning.

A SIMILAR SITUATION IN FRANCE

The French National Data Protection Commission (CNIL) also dealt with a similar issue of facial recognition in schools, finding this practice unacceptable outright. The consent-based experiment was announced in December 2018 for two high schools in Nice and Marseille. The technology, which was provided free of charge by the American company Cisco, was designed to scan all students at the school entrance. Upon completion of a testing phase, the facial recognition system would then be extended to all schools in the southern region of France.

With regard to security concerns, preference should always be given to less intrusive means, while respect for an individual's dignity and human rights should be at the core of any facial recognition deployment.

Unlike in Sweden, French CNIL became aware of the case still before the fact, rather than after it had taken place. Although it took the Commission ten months to issue its official statement, it eventually found that deployment of facial recognition failed to comply with the principles of proportionality and necessity, and declared it to be too intrusive for an individual's privacy compared with the alternative of monitoring attendance by humans. The CNIL is of opinion that facial recognition technology breaches the GDPR and is likely to create a feeling of reinforced surveillance. In contrast to the DPA ruling in Sweden, the CNIL opinion is not legally binding, and it is left to the discretion of the regional authorities as to whether to proceed with the facial recognition experiment. It is anticipated that the authorities will still greenlight the project, given their discontent with the CNIL position, calling it totally outdated and unreasonable. However, the last word, in this case, belongs to the Marseille administrative tribunal with which a group of human rights organizations and parents' union filed a lawsuit requesting to cancel a decision permitting the usage of facial recognition technology at schools.

At the end of 2019, the CNIL issued a paper where it called for a broad public debate on facial recognition. The Commission not only provided extensive descriptions of the different components of facial recognition systems but also defined some prerequisites for their usage. In particular, it stressed the need to use the existing data protection framework (GDPR) as guidance for the legitimate use of facial recognition, noting that even experimental deployment of this technology must be tested against personal data protection safeguards (necessity, proportionality, legitimate aim). With regard to security concerns, preference should always be given to less intrusive means, while respect for an individual's dignity and

human rights should be at the core of any facial recognition deployment. Therefore, obtaining an individual's explicit consent is critical before proceeding to process their data. The CNIL also called for an experimental approach to testing and perfecting technical solutions in compliance with the legal framework in force.

MOREOVER, FRANCE BELIEVES THAT SCHOOLS ARE NOT YET THE LIMIT

Facial recognition in schools is still quite insignificant in comparison with France's national ambitions for facial recognition deployment. The ALICEM initiative, which is way larger in scope and far-reaching in consequences, aims at launching a nationwide digital identity system. To create an account a person would be asked to take a real-time video of themself via smartphone and perform three different actions (smiling, turning head, blinking). This is a so-called dynamic element of a facial recognition system. The static facial recognition will be conducted based on an image extracted from the video and compared with the one kept on the chip contained in their physical ID card. The authorities reassure that once an identity check is completed, all biometric data, including video, are deleted.

The initial launch of the digital ID system was planned for November 2019 but has been postponed until mid-2021. The CNIL largely criticized ALICEM for a lack of an alternative to obtain digital identity without going through a facial recognition process, which, in its opinion, rules out free consent as required by the GDPR. The authorities promised to offer an opt-out option from facial recognition and provide traditional means of verifying an individual's identity. The decision to launch the digital ID program based on facial recognition is also being challenged in the court, while 80 organizations have signed a joint letter calling the French Government and the Parliament to ban any present and future use of facial recognition for security and surveillance purposes.

France is also considering the possibility to deploy a video surveillance experiment in public places allowing facial recognition in real-time, which is planned to be in force from six to twelve months and be monitored by civil society and researches to identify any flaws and human rights implications. The parliament recommends ensuring the respective legal framework is in place before starting an experiment. The GDPR regulations require obtaining consent prior to collecting and processing of biometric data, and this is why the French authorities claim that only those who would agree for their faces to be scanned will participate in the experiment.

GERMANY SURPRISINGLY STEPPED ASIDE FROM FACIAL RECOGNITION FLASH MOB AROUND EUROPE

In 2017, Berlin became a frontrunner for the first German city to try facial recognition as an attempt to improve its efforts to combat terrorism. Surveillance cameras were installed at Südkreuz station, a large train hub, with a plan to monitor approximately 300 pre-selected volunteers for a six-month period. All volunteer photos were saved into a special database, and each was required to carry a special transponder that would allow cameras to identify them in the crowd. First, the Ministry of Interior reported poor results from the Südkreuz facial recognition experiment, which experts tried to explain by Germans' high sense of privacy. According to final estimations, the system proved to be 80 percent accurate, meaning only one in five people went unnoticed by the cameras and only one in 1,000 was falsely identified as a person of interest. The experiment raised significant concerns among human rights advocates. The end of this trial marked some break in the German authorities' efforts to test facial recognition technology.

Early 2020 brought a new concern for privacy advocates in Germany when the media revealed the Ministry of Interior's plans to install automatic facial recognition systems at 134 railway stations and 14 airports around Germany, pending amendments to the Federal Police Act, which would provide police with improved technical possibilities and, where possible and reasonable, extended responsibilities. However, these plans completely changed when the German government decided to postpone facial recognition rollout by deleting respective authorization from a legislative package on the reform of police powers. It was stated that such a move is largely dictated by a pressing need to have a broad public consultation first and to make sure that the reasons behind using this technology are well understood. Additionally, the Federal Data Protection Commissioner pointed out that there is currently no legal basis for automated biometric facial recognition, which must be put in place before any deployment can occur.

First, the Ministry of Interior reported poor results from the Südkreuz facial recognition experiment, which experts tried to explain by Germans' high sense of privacy.

CONCLUSION

Facial recognition is becoming a reality, whether we want it or not. The strategy now should be not to deny the inevitable, but to critically and objectively assess the risks of such systems, and when their use is justified. Whenever these systems are considered or proposed, there should be an open public debate. With facial recognition, each of us is becoming transparent for the government. As such, why then do governments not make their plans for deploying facial recognition transparent for us? Why don't they share when, how, and why our data is being collected and stored, or how law enforcement bodies compile their watchlists? Why are we not given a choice to avoid our faces being scanned?

The prohibition of facial recognition technology by governments should be the default, with exceptions clearly and narrowly defined in legislation. All necessary safeguards should be taken by governments to prevent situations in which surveillance leads to a change in the behavioral patterns of their citizens. No single person should be put under permanent and indiscriminate surveillance, where privacy is only obtained if an individual covers their face, refuses to participate in peaceful protests, and limits the ways and locations in which they interact with others.

Facial recognition systems are usually blamed for a built-in bias based on gender and race. But this is a wrong argument to start with, given that the technology is trained and improved on an ongoing basis. Instead, it is more critical to be looking into both the stated and unstated motives behind the application of this technology. To do so, we should be addressing governments around the world with the right questions. Instead of demanding that automatic facial recognition technologies strictly adhere to human rights standards (e.g. the rights to privacy, freedom of expression, freedom of movement, and freedom of assembly), we often focus on the systems' technical flaws, which can unintentionally send the wrong message that if they simply address these flaws, we would be happy with that perfectly designed surveillance model.

Let's imagine that at some point in the future, remote cameras will identify faces with 100 percent accuracy. Would that be more calming in terms of the level of intrusion into an individual's privacy? Once facial recognition systems reach ultimate precision, we are just one step away from the Orwellian state of mass surveillance while the governments are fixing a few more cameras.

The strategy now should be not to deny the inevitable, but to critically and objectively assess the risks of such systems, and when their use is justified.

HAVE A QUESTION?

Ask the author

LinkedIn: OLGA KYRYLIUK

Email: kyryliuk.olga@gmail.com

OPEN INTERNET for DEMOCRACY

openinternet.global