Forum: SPC1

Issue: The use of Artificial Intelligence in surveillance in the context of freedom of movement

Student Officer: Aidan Leahy

Position: Deputy President

Introduction

Artificial intelligence, or more commonly known by its abbreviation AI was the Collins dictionary word of the year for 2023 and rightly so! The impact that AI has had on the planet is clear to see. Shaking the foundations of academia, education, science, business, politics, international relations and tech alike. Seemingly having popped out of nowhere, the infamous ChatGPT took the world by storm when it was first released on the 30th of November 2022 reaching a million users in just 5 days, doing what took Netflix over three and a half years to do! Yet the foundations of the AI we know and love today would be built by none other than Alan Turing and his original computers used to crack Nazi code in WWII. Turing discussed how computers might learn from their experiences as well as solving new problems using guiding principles—a process now known as heuristic problem solving.

While the true capabilities of AI and its significance might still not be fully understood, what we do know now is that there is huge possibility for damage and mal intent. Many people argue that the Roman Empire never fell and simply became the Roman Catholic Church moving base from Constantinople to the Vatican. While the credibility of this statement might be dubious, a far stronger case can be made in the argument of the Cold War never ending and simply moving online. It's of no doubt to any well-informed individual that the USA, Russia and now China battle it out for international dominance and control in the twenty-first century, and technology such as AI among others play a pivotal role in world conflict. China is seen by many political commentators as the blueprint for the new technologically based autocratic state. One that uses a combination of cutting-edge tech like AI incorporated with existing systems to monitor and by extension control their population. The field of AI and by extension data protection is very unregulated, even more so when it comes to free movement and the intersection with human rights. The need for cohesive and consistent regulation from the international community and

organizations such as the UN is paramount if we want to protect human rights and democracies around the world!

Definition of Key Terms

Biometric Surveillance

Biometric Surveillance is the use of human characteristics/features to identify individuals. Common forms of biometric identifiers include fingerprints scanners and face identification technologies.

AI powered surveillance

AI-powered surveillance is the use of artificial intelligence to enhance surveillance technology to monitor, track, analyse and identify people, places and objects.

Datafication

Datafication is the process of transforming reality features and social behaviours into quantified (numerical) data that can then be analysed.

Surveillance

Surveillance is the process of observing individuals or groups for a purpose and to make inferences/ judgements on their behaviour and future actions.

Dataveillance

Dataveillance is the leveraging of big data/datafication to scale up surveillance. Dataveillance utilises automated systems for continuous and ubiquitous data generation and collection, enabling the monitoring, tracking, regulation, prediction, and potential steering of individual and group behaviour.

Chinese social credit system

The China social credit system (SCS) is a broad regulatory framework intended to report on the 'trustworthiness' of individuals, corporations, and governmental entities across China. The data recorded in this system can be used to limit or enhance the rights and liberties enjoyed by citizens.

Artificial Intelligence

Artificial Intelligence (AI), is the ability of a computer or computer-controlled robot to perform tasks commonly associated with intelligent beings.

Smart (x)

When the term smart comes before something it normally refers to the use of AI to enhance systems operation.

Background Information

When we think about AI surveillance and its implications on freedom of movement (FoM), we need to understand what we actually mean by 'freedom of movement' in the context of the digital age. As laid out in the universal declaration of human rights (UDHR) everyone has the "rights to freedom of movement and residence within the borders of each state (...) rights to leave any country, including his own, and to return to his country". But analysing this critically we must pose the question, to what extent does the increase of AI surveillance have on our freedoms of movement and why? The current answer for most of us is not much. For most people AI surveillance wont physically stop you from leaving your home country or returning. Your ability to move freely around your home country will remain protected by things like constitutions and intergovernmental agreements. Most people living in robust western democracies as of today have little to fear about in those regards, however the future is uncertain. Very few people (like those who are detained in places such as concentration camps or prisons who have restrictions already placed on their FoM) are likely to have experienced worsened enjoyments of their rights due to AI enhanced surveillance. In places like Xinjiang China or Gaza, AI enhanced surveillance is used to extreme damaging lengths.

While AI enhanced surveillance is to play a huge role on the issues of actual FoM in the future, there is a more immediate problem at hand that we are obliged to discuss. One more closely linked to AI surveillance and the internet. This issue being the rights to freedom of assembly and association (FoAA). In recent years it has been the focus of academia and subsequent literature on the issue of FoM online, and the interconnectedness that there subsequently is between FoM and FoAA both online/offline and AI enhanced surveillance models. As stated, most people particularly in the West won't experience (for now) things like the infamous Chinese social credit system (SCS). And those living in lesser economically developed countries LEDCs (even those with autocratic governments) often won't have the state funding available to implement projects on that scale like those that have been seen across China and in its smart cities. Even though it is becoming cheaper and cheaper to do so. While things like these are becoming more and more widespread, we must look at both sides of the coin (online and offline) with equal importance. What AI and its many different forms of surveillance will have an impact on is how we use the internet and most importantly how we use social media. The use of AI to analyse harnessed data and its implications to push or use specific algorithms greatly impacts the extent to which we are free to use social medias as we choose. And as a result, enjoy our FoAAs, arguably the most valuable form of FoM.

We must emphasise the indivisibility of human rights, that for one human right to be fully enjoyed there must be a collective realisation of all human rights. FoAAs cannot be enjoyed in the absence of FoM and vice versa. Our FoM must be protected and enshrined for future generations in the face of an increasingly smart AI and to do this significant work is due!

FoM and FoAA online

The rights of FoAA are fundamental rights guaranteed in article 20 of the UDHR. Two separate human rights commonly grouped together, freedom of association enables individuals to come together and collectively to express, promote, pursue, and even defend common interests. While freedom of assembly refers to the intentional and temporary presence of a number of individuals in a public place for a common expressive purpose. This is echoed in articles 21 and 22 of the International Covenant on Civil and Political Rights (ICCPR), ratified by 172 countries, further emphasised in many member states constitutional documents. They are essential to the establishment and functioning of a democracy and ensure that all individuals and groups can peacefully come together to pursue their common goals. These, among other human rights, are under threat day in day out from the development and widespread deployment of AI enhanced surveillance systems on the internet.

Given the importance of AI for the inner workings of social media and the broader internet, FoAA online will be dependent upon how AI is used. And by extent how surveillance can be facilitated through further AI usage. By determining or influencing what content we see or what content exists, AI shapes how and why people assemble online. Allowing some groups to exercise their rights fully while discouraging or banning others outright. Or furthermore, encouraging some to join groups that they wouldn't have done so naturally, these ‘echo chambers’ harden views and increase polarization. The former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye states: ‘Artificial intelligence-driven personalisation may also minimise exposure to diverse views, interfering with individual agency to seek and share ideas and opinions across ideological, political or societal divisions.’ It can be added that AI-driven personalisation may minimise how and where individuals assemble online, what types of associations can be formed and the extent to which the rights to both assembly and association are respected.

Additionally former UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai, affirms that assembly and association do exist online stating that ‘… the rights to freedom of peaceful assembly and of association can be exercised through new technologies, including through the Internet.’ If we think about the most recent large movements of people out of their homes and onto the streets in the last twenty years in acts of protest it would be hard to come up with an example that didn’t use social media to organize it. Take the 2009 Iranian Green Movement coined the ‘Twitter Revolution.’ It became the first major world event worldwide to be almost entirely broadcast on social media. If people aren't free to move around the internet and use it in their desired way, then they are likely to be censored. Be it self-censorship (believing they are part of an insignificant minority and fearful of retribution) or deliberate intent from AI run algorithms to hide or remove content. Both result in people being less likely to exercise their civil liberties and freedoms, such as protest, unionisation and political engagement and FoM.

Internet censorship and additionally internet shutdowns also represent ways in which FoAAs online can be restricted. The UN Human Rights Council (HRC) resolution A/HRC/RES/38/11 affirms the importance of a basic internet access as a core element of assembly and association, being concerned

with ‘undue restrictions preventing Internet users from having access to or disseminating information at key political moments, with an impact on the ability to organize and conduct assemblies.’ Beyond internet access, the UN HRC have supported and affirmed that FoAA also applies once an individual has access to the internet. In multiple UNHRC resolutions (resolutions 20/8, 26/13, 32/13, 38/7) ‘the promotion, protection, and enjoyment of human rights on the Internet’ have been explicitly highlighted such as in A/HRC/RES/24/5.

Furthermore, in 2018, UN HRC resolution A/HRC/RES/38/11 stressed ‘that although an assembly has generally been understood as a physical gathering of people, human rights protections, including for the rights to freedom of peaceful assembly, of expression may apply to analogous interactions taking place online.’ Finally, UN General Assembly resolution A/RES/73/173 in 2018 called upon ‘States to ensure that the same rights that individuals have offline, including the rights to freedom of expression, of peaceful assembly and of association, are also fully protected online’ and further, to grant ‘respect to all individuals exercising their rights to freedom of peaceful assembly, of expression and of association, online and offline, in cases of threat, harassment, violence, discrimination, racism and other violations and abuses committed against them’.

The opportunities for dictators and autocrats to take advantage of new cutting-edge technology to influence social media and bend it to their advantage is simply frightening. Never before has there been so much data poured onto the internet, unregulated, unmonitored and uncontrolled with little to no third-party oversight. Social media and more specifically data have proven to be an unknown domain. As things like dataveillance and the leverage of big data become more frequent, algorithms and AI run programmes become more and more effective every day. These programmes can be used in many ways such as predictive policing and counter terrorism models. While they are very effective at reducing crime rates and minimizing the chances of terrorist attacks, these programmes place significant moral dilemmas at the hands of governments, companies and lawmakers alike.

Post COVID 19 many governments and businesses still have huge swathes of biometric data harnessed from things like tracking apps that were used to monitor the spread of the COVID 19 disease. While these proved effective at the time, significant issues now lie with how the data might be repurposed or sold on in the future and for what it could be used for. As the demand for these systems increases the immediate need to use available data to train them will increase. Resulting in data being used that was likely collected by another system for a different purpose. Data often becomes an independent entity, i.e. it can be copied, multiplied, manipulated and repurposed. If in the wrong hands this data (such as biometrics) coupled with facial recognition technology (FRT) and smart CCTV cameras can be used effectively to stop dissent and public disorder or wipe human rights supporters, journalists and critics. Silencing freedom or liberation movements worldwide, blurring the lines between privacy and freedom, entering into territories of ubiquitous surveillance. Many people living under the iron fist of violent and oppressive regimes will be more afraid to protest or fight back (exercising their FoM and FoAA) for fear of enhanced surveillance and the increased likelihood of violent life-threatening

punishment.

FoM and FoAA offline

While the impacts on AI enhanced surveillance models online are enormous and present an unprecedented threat to the foundations of modern democracy. It would be abysmal of any UN committee to overlook the real-world impact that surveillance tech would have, and the subsequent creep towards an Orwellian reality is a very real threat. At least 75 of the world's 176 countries, according to the Global Surveillance Index (GSI), are already actively investing in and deploying AI enhanced intelligence systems for surveillance purposes, primarily in smart cities using facial recognition, and smart policing. With around 3 billion photos available to the US Federal Bureau of Investigations and local law enforcement having been used to 'search by face' to identify and arrest criminals in 2020 alone. However, many have already taken steps towards stopping this Orwellian reality from materializing. The EU Artificial Intelligence Act (Regulation 2021/0106) bans the use of "'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement", strictly for necessary purposes like the search for victims of crime, the prevention of a threat to life, physical safety or terrorist attacks. Additionally, for the search of a perpetrator or suspect of a criminal offence. The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) go a step further prohibiting the use of such systems in public spaces, calling for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces. Including faces, fingerprints, DNA, voice and other biometric or behavioural signals, in any context at all. It's clear that significant legal work has already been initiated in the Western world, but more help is needed to introduce robust international regulations.

The main effects of these technologies are best explained in specific examples however, there are some common themes. AI enhanced facial recognition CCTV surveillance and the use of pre gathered biometric data are the most common. The best example of these are in places like China where 'smart cities' which are filled with tech (mainly sold by companies like Huawei) where ubiquitous surveillance is a common theme excused under the guise of safety and security. And it's true, some of these technologies can be employed with incredible efficiency, to deny that would simply be wrong. Huawei even marketing that the implementation of their 'smart cities' could 'eradicate extremism' from the middle east. As mentioned in the previous subsection, AI enhanced systems are used to gather, sort and assess data which can be used in predictive policing etc. While these things might be good in the short run, they pose serious threats to the future of human rights as the legal restrictions and what can be done with the data once it has been gathered are slim and often inconsistent.

Issues like these are new and countries often don't intend on causing future human rights violations, but they can unknowingly set down the groundwork for doing just that. Take the individual

COVID tracing systems used in Norway and in Singapore, both used to help track and stop the spread of the disease. In Norway (renowned for its democracy and high standards of living) their app revolved around a live feed on the location of each user's whereabouts, which were then uploaded into a centralized system, posing huge risks for privacy and GDPR. The government then removed the system upon recommendations from NGOs. On the other hand, the system used in Singapore 'Trace Together' worked by uploading individual location points forming chains of movements (acting as a 'breadcrumb trail') not as a live feed. If a person had tested positive only the people, whose trails overlapped would be notified or analysed at all. Also, the data would be completely erased after 21 days. While the Norwegian system was far more effective, the one employed in Singapore was far safer, from a data protection point of view. Norway was just one example however imagine the movements of millions of people traced over an extended period. Think about how many interested third parties would buy that data! The need for protection and regulation is clear.

We only need to look to places like Xinjiang where Uyghur Muslims from the ages of 12 are made to give over biometric data like fingerprints and DNA samples among others. Allowing the Chinese government to keep tabs on them essentially for the rest of their adult lives. This is particularly bad as China has implemented its social credits system (SCS), a political idea many never thought would materialize. Under this system the way that people conduct their lives is tracked and measured. Everything from the people they meet and talk to, the posts they like, what they buy, where they go and who they agree or do not agree with are recorded. Basically, this system allows the government to gauge how much of a threat their citizens are to the control of the communist and the status quo. Punishing and excluding those who disrupt them healthcare and social welfare etc. On the other hand, those who are 'good citizens' are rewarded with fast-track access to services. In worst cases the freedom of movement of the 'bad citizens' is removed altogether. Similarly in Israel many have said that the government had been using enhanced AI surveillance systems to engage in AI assisted or 'autonomous' apartheid. Not to mention the creation of Pegasus software often used to tap and track the phones of journalists and human rights activists like that of Jamal Khashoggi.

As of the early 2000s the EU has made strides to further incorporate the use of biometrics as a form of identification for migrants entering the Schengen zone without proper documentation. Many of these systems enhanced by AI. In 2000 Biometric registration of asylum-seekers was implemented establishing the Eurodac database to store asylum-seekers' fingerprints intended to aid in determining the state responsible for processing asylum applications, with the full biometric data base coming into play in 2011. 2017 seeing the Entry/Exit System (EES) legislation introduced. With the EES monitoring cross-border movements of temporary visitors to the Schengen area, aiming to replace manual passport stamping with a centralized database containing biometric and biographic data. All these systems depend on AI and complex computer systems to operate fully and connect with the individual security systems of each member state.

Another common form of AI enhanced surveillance is smart CCTV systems, whose accuracy remains dubious. While the systems themselves may be fully functioning and the programming behind them sound. Often the data uploaded into the systems is not of use or bad quality. This 'bad' or 'dirty' data can be particularly damaging to minority groups such as people of colour often reinforcing existing prejudice into already biased policing. Minorities are far more likely to be over surveyed and subject to stops and investigation because of the enhanced technologies, when they might not have committed any crime at all. Such an example could be seen in predominantly black communities in New York and across the USA in light of the Black Live Matter (BLM) movements.

Major Countries and Organizations Involved

China: China remains the leader in world class ubiquitous surveillance of their citizens, gathering data from them via osmosis at their every turn. China benefits and pushes greatly in the advancement of such technology as it greatly benefits the maintenance of the status quo. The modern Chinese power system depends on bolstering the ethnic majority (Han) and trying to lessen the gap between different types of Chinese people and promote cultural hegemony. It does this mainly by suppressing language and creating a standardised secular culture heavily reinforced through social and educational norms. In many extreme cases like that of the Muslim Uyghurs in Xinjiang it turns to violent methods to suppress the local populations. China also seeks to benefit from the expansion of such AI systems as it gives them a 'foot in the door' when it comes to winning favour in developing LEDCs and competing against the USA for global relevance.

The EU: The EU has arguably made the biggest advancements when it comes to protecting its citizens from AI surveillance alongside general data protection. The EU will seek to improve the use of AI to help deal with the migrant crisis among others. The further use of AI enhanced surveillance is very much a double-edged sword in the eyes of European management. It could be used as a great tool to help with migrants as mentioned above but also used to squash far right movements online and tackle extremism. However, with the rise of the far right throughout Europe AI enhanced surveillance poses a real threat to democracy as we know it and could lead to possible human rights abuses and suppression of free media, particularly those who support women's and gay rights. Centrist politicians and European moderates will seek increased restriction and oversight from major institutions to help mitigate possible risks. The European Union has advanced considerably in AI regulation with the AI Act, aiming to harmonize innovation with human rights safeguards by imposing stringent criteria for high-risk AI systems and limiting real-time biometric monitoring to major offenses. Nonetheless, the Act has been criticized for not prohibiting public mass surveillance and for permitting the use of AI in migration management, which raises worries about effects on marginalized communities. Although the AI Act establishes an international benchmark for regulating AI, continual assessment is required to tackle human rights risks associated with surveillance, including dangers to personal mobility and FoM.

Amnesty International: Amnesty International has done substantial work in shining light upon the risks of possible human rights violations and current ones that stem from AI enhanced surveillance not only on FoM but on human rights in general. Having released and created specific software that can be used for free to detect things like Pegasus spy software, Amnesty International proves to be a valuable group bringing attention to topics normally not touched on by state media. In December 2024, they disclosed the Serbian government's employment of spyware to track activists and journalists, underscoring the abuse of technology to stifle civil society.In May 2024, they recorded how AI technologies at border crossings often worsen inequalities and violate the human rights of migrants. Moreover, Amnesty condemned the EU's choice to avoid prohibiting public mass surveillance in the AI Act, cautioning that it establishes a harmful global standard. These initiatives highlight Amnesty International's dedication to examining and opposing the use of AI in surveillance situations that endanger human rights.

LEDCs: Many LEDCs seek to expand the use of AI enhanced surveillance technologies active in their nations as a tool to curb instability. Many young countries struggle with turbulence, economically and socially. Many LEDCs don't have the same hegemonic culture as European nation states do, resulting in conflict between ethnic groups. Many leaders from one ethnic group will seek to use these technologies to gain and maintain the upper hand over other cultural groups, often restricting and violating human rights in the process. Many of these LEDCs will turn to China for access to cheap AI enhanced surveillance tech. In the same way many African nations turned to the US after WWII for self-determination and financial support through capitalist models moving away from previous colonial models of the Europeans. Many of these countries are now frustrated that the American dream of democracy and capitalism never materialised in their home countries resulting in exploitation and worsened inequality. Some now encourage swapping allies and moving to the BRICS axis and China for support through means of surveillance technology contracts. China loves this as it allows them to expand their network of influence across the globe, worsening proxy war between them and their western counterparts.

Timeline of Events

Date	Description of event
1945	Alan Touring invents the computer
1960	First CCTV cameras rolled out in Britain
1983	The internet was made
2000	The EU implements biometric data gathering in immigration processes
2018	Huawei launches digital platform for smart cities at world Expo conference
2022	ChatGPT released
2024	general assembly adopts landmark resolution on AI

Previous Attempts to solve the Issue

Little attempts have been made by perpetrating powers to address the issue as autocrats seek no desire to turn away from new technological possibilities that would allow them to increase their control. Collective attempts have been made by groups such as the EU to implement general legislation to protect the rights of its citizens, yet more is needed. The UN has reached consensus on the severity of the issue and the need to enshrine rights both online and offline, and they hold equal importance. Yet the need for member states to come together and implement sweeping measures to tighten the regulation on data collection and management is due.

Possible Solutions

In summary, incorporating AI into surveillance systems presents substantial opportunities for improving security, yet it needs to be thoughtfully regulated to safeguard individuals' FoM. To achieve this balance, it is essential to create clear and transparent regulations that outline the scope and purpose of surveillance, guaranteeing it is utilized responsibly and solely for specific, essential purposes. These regulations must be legally binding and implemented on a global scale, consistent across all countries. Technologies that enhance privacy, like data anonymization and edge computing among others, can reduce the effects on individual privacy. Moreover, human supervision and consistent bias evaluations are crucial to avoid discriminatory actions and guarantee responsibility in AI decision-making. Consistent third party independent oversight is needed for both governments and companies alike. Restricting surveillance to designated times and locations, offering consent and opt-out options, and establishing robust protections against data misuse, like encryption, are essential measures to reduce risks. Public involvement and contributions from civil society can additionally guarantee that surveillance methods uphold individuals' rights. Ultimately, examining options beyond AI surveillance and promoting global standards will aid in creating a worldwide framework that respects privacy while ensuring security, guaranteeing that AI does not compromise the essential freedoms it aims to defend.

Methods like these can only be effective and robust if they are implemented on a global level to ensure there are no loopholes that can be bypassed. Delegates need to focus on legal framework and cooperation to enshrine rights of Fom and FoAA online and offline. Human rights should be at the centre of resolution creation, focusing on key beliefs held by all member states, ensuring consensus is reached. The UN shouldn’t rule out these technologies and advancements that they will bring for fear of complications, however regulations are needed to ensure they are used for their proper purposes only. These are complicated issues and little legal precedent has been set, making this a challenging topic for delegates. key principles such as cooperation, legal framework creation, communication and investment will be paramount to effective resolutions and fruitful debate.

Bibliography

Kaskina Rasma, Cvetovska Angelina ‘Artificial intelligence (AI) and human rights: Using AI as a weapon of

repression and its impact on human rights,' The European Parliament, June 2024 https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450(SUM01)_EN.pdf accessed Sunday December1

Donnelly Drews, 'China Social Credit System Explained – What is it & How Does it Work?' Horizons, February 11 2024 https://joinhorizons.com/china-social-credit-system-explained/#:~:text=The%20China%20social%20credit%20system%20rates%20individuals%20based%20on%20the,grade%20(usually%20from%20A%2DD accessed Sunday December1

Amnesty International 'USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research' February 15, 2022 https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/ accessed Sunday December1

Amnesty International 'India: Hyderabad 'on the brink of becoming a total surveillance city' November 9, 2021 https://www.amnesty.org/en/latest/news/2021/11/india-hyderabad-on-the-brink-of-becoming-a-total-surveillance-city/ accessed Sunday December1

Amnesty International 'Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT' May 2 2023 https://www.amnesty.org/en/documents/mde15/6701/2023/en/ accessed Sunday December1

Amnesty International 'Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally' July 19 2021 https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project-2/ accessed Sunday December 1

Fontes Catarina, Hohma Ellen, Corrigan Caitlin .C, Lütge Christoph, 'AI-powered public surveillance systems: why we (might) need them and how we want them,' Technology in Society, Volume 71, 2022, https://doi.org/10.1016/j.techsoc.2022.102137 accessed Sunday December 1

EuroMed Rights, 'AI in Border Control and Surveillance, Current and Future implications' https://euromedrights.org/wp-content/uploads/2023/11/230929_SlideshowXAI.pdf accessed Sunday December 1

Baweeja Sahajveer, 'Singh Swapnil Beginning of Artificial Intelligence, End of Human Rights,' July 16 2020 https://blogs.lse.ac.uk/humanrights/2020/07/16/beginning-of-artificial-intelligence-end-of-human-rights/ accessed Sunday December 1

Saheb, T. "Ethically contentious aspects of artificial intelligence surveillance: a social science perspective". AI Ethics 3, 369–379 (2023). https://doi.org/10.1007/s43681-022-00196-y accessed Sunday December 1

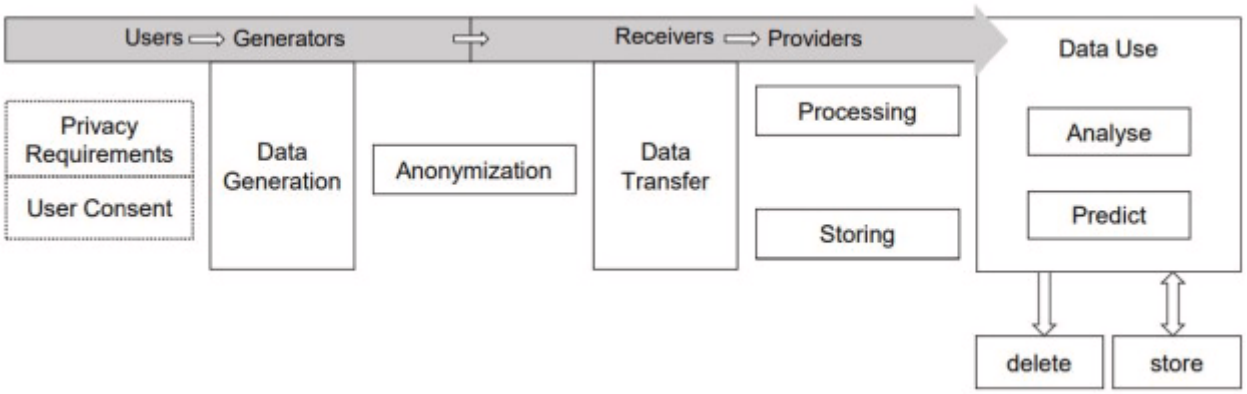
Ashraf, C. (2020). 'Artificial intelligence and the rights to assembly and association. Journal of Cyber Policy', 5(2), 163–179. https://doi.org/10.1080/23738871.2020.1778760 accessed Sunday December 1

McKendrick Kathleen 'Artificial Intelligence Prediction and Counterterrorism' August 2019, Catham House, https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf accessed Sunday December 1

Article 19, 'Rights to anonymity online, policy brief' June 2015, https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf accessed Sunday December 1

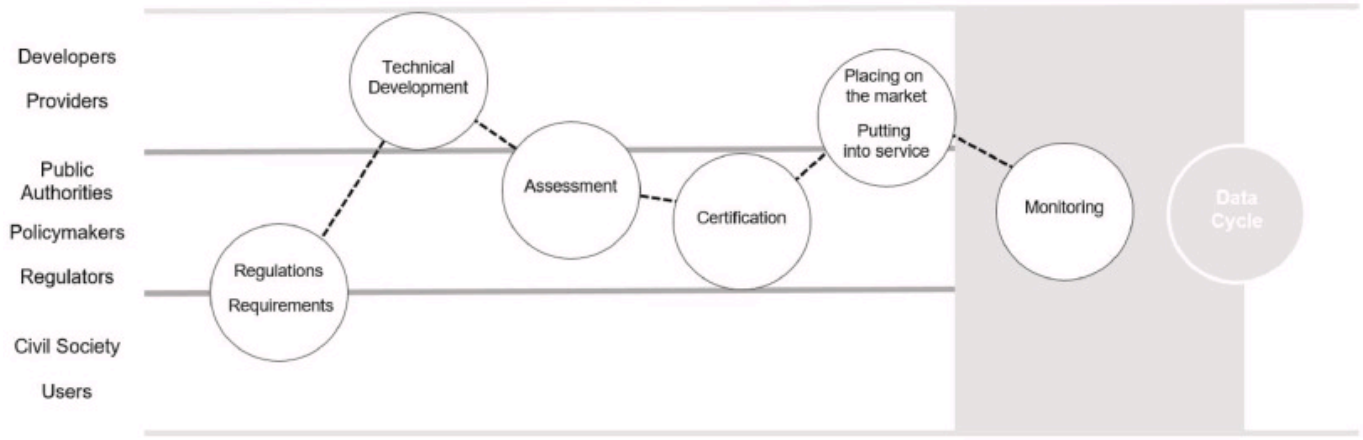
Vermuelen Mathias, 'Surveillance: Ethical issues, legal limitations, and efficiency' The European commission 2012, https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D4.7-The-scope-of-the-right-to-privacy-in-public-places.pdf accessed Sunday December 1

Appendix or Appendices



Example of a possible data cycle[1]

[1] Catarina Fontes, Ellen Hohma, Caitlin C. Corrigan, Christoph Lütge,
AI-powered public surveillance systems: why we (might) need them and how we want them,
Technology in Society,
Volume 71,
2022,
102137,
ISSN 0160-791X,
https://doi.org/10.1016/j.techsoc.2022.102137.



AI governance framework. Identifying stakeholders and grading responsibility in an AI system lifecycle.[2]

Useful Materials

I. The Dangers of Video Surveillance and A.I.
II. https://time.com/7202584/gaza-ukraine-ai-warfare/
III. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics
IV. https://www.oecd.org/en/topics/sub-issues/ai-principles.html
V. https://www.amnesty.org/en/latest/news/2024/05/global-new-technology-and-ai-used-at-borders-increases-inequalities-and-undermines-human-rights-of-migrants/
VI. https://doi.org/10.1093/jhuman/huad020
VII. https://www.lawfaremedia.org/article/assessing-impacts-of-ai-on-human-rights-it-s-not-solely-about-privacy-and-nondiscrimination
VIII. https://www.amnesty.org/en/latest/campaigns/2024/01/the-urgent-but-difficult-task-of-regulating-artificial-intelligence/
IX. https://www.ohchr.org/en/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner

[2] same source for both diagrams