2024

MUNUC – SFLS Conference

上海外国语大学附属外国语学校
芝加哥大学国际模拟联合国大会

Social, Humanitarian, and Cultural Committee (SOCHUM)

Social, Humanitarian, and Cultural Committee

SOCHUM

MUNUC SFLS

Model United Nations of the University of Chicago

TABLE OF CONTENTS

HISTORY OF COMMITTEE

The General Assembly of the United Nations was established in 1945, and it currently consists of 193 Member States.[1] Alongside the Disarmament and International Security, Economic and Financial, Special Political and Decolonization, Administrative and Budgetary, and Legal Committee, the Social, Humanitarian, and Cultural Committee is delegated tasks from the United Nations General Assembly to address.[2] Known as the Third Committee, or SOCHUM, it is responsible for a wide array of issues concerning social, humanitarian, and human rights issues. Notably, the need to promote human rights worldwide has been a focus for SOCHUM, as it is a predominant goal for the United Nations as a whole to uphold human rights.[3] And while many of the General Assembly's resolutions pass with much consensus amongst member-states, there have been noted disagreements among members on the issue of human rights.[4] As this committee deliberates on how to best address the topic of Migrant Labor Rights or the implications of Artificial Intelligence, not only does SOCHUM's focus on human rights need to be maintained, but also, SOCHUM must continue to work towards developing inclusive and engaging solutions that allow for equitable humanitarian advancement.

[1] "About Us". United Nations. https://www.un.org/en/about-us.

[2] "United Nations General Assembly". https://www.britannica.com/topic/United-Nations-General-Assembly.

[3] "Secretary-General's Call to Action for Human Rights". United Nations. https://www.un.org/en/content/action-forhuman-rights/index.shtml.

TOPIC A: IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

Statement of the Problem

Artificial Intelligence (AI) seems to be one of the most promising frontiers of modern-day technology. Yet the social and cultural implications of the increasing integration of AI into our lives must be considered and accounted for, not only by those writing the code behind self-driving cars, or by those writing laws on consumer privacy, but also by our society as a whole. Artificial intelligence touches our lives in numerous ways. AI is at work every time you enter a google search, every time you shop online, and every time you unlock your phone with FaceID, use Siri, or a "Smart" appliance like an Amazon Echo speaker. AI can undoubtedly be beneficial—or just innocuous—but it can also be harmful.

In fact, the impact of AI may be beneficial, innocuous, and harmful, all at once. For instance, when it comes to the impact of AI on the job market, jobs will be both created, unaffected, and lost. AI could reduce low-skill labor positions as tasks are automated. On the other hand, AI is expected to create jobs both in fields like information technology. It can also indirectly benefit job seekers by helping people find jobs and by boosting business growth, thus creating more jobs.[4] So as AI results in a general "upskilling" or "reskilling" of jobs, how can the benefits be maximized while the harms are minimized? It may be useful to consider how access to education and economic opportunities across regions may contribute to financial stratification that is only exacerbated by the growth of AI. For some populations, AI may only bring fears of job loss and a descent into a dystopian society. How can these fears be addressed?

[4] "The Impact of Artificial Intelligence on Unemployment". Technology.org: Science and Technology News. 17 December 2019. https://www.technology.org/2019/12/17/the-impact-of-artificial-intelligence-on-unemployment/.

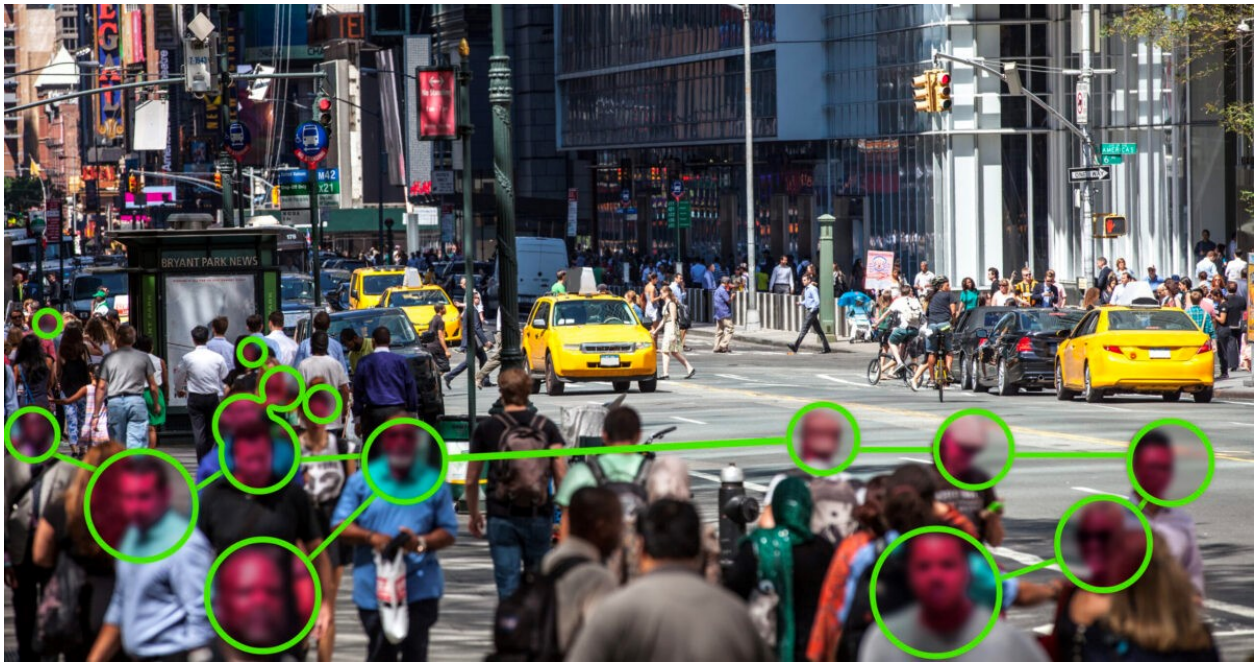
Automation in a car factory. [5]

Moreover, as AI continues to grow and develop, it is crucial that steps are taken to address bias in artificial intelligence. Also known as algorithmic bias, Machine Learning (ML), a subdomain of AI, often takes on the cognitive biases of the humans creating the Artificial Intelligence products. One example of bias in Artificial Intelligence is the presence of racial discrimination in facial recognition technology. A study known as the Gender Shades project by researchers at MIT and Microsoft Research found that while top facial recognition algorithms boasted an accuracy above 90%, the top five AI software all had the lowest accuracy for darker-skinned females and the highest accuracy for lighter-skinned males.[6] This example has serious implications for law enforcement as well as the criminal justice system. An article in 2020 from Harvard expressed concern over bias in facial recognition software not only for the ability for misclassification to harm in a criminal justice setting but also psychologically as certain populations are over-surveilled. For instance, a study of the 2016 Project Green Light in Detroit found that there was a higher presence of cameras in majority-black

[5] Julia.Roesler. 2020. "English: Volkswagen´S First New Generation Electric Car Being Built with Siemens Automation Technology." Wikimedia Commons. February 19, 2020. https://commons.wikimedia.org/wiki/File:Siemens_automation_in_volkswagen_factory.jpg.

[6] Buolamwini, Joy and Gebru, Timmit. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification". 2018. https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

areas and that this unevenly distributed surveillance was associated with a diversion of public health benefits as well as the criminalization of communities.[7][8]



Facial recognition software.[8]

More broadly, regardless of AI's impact on the criminal justice system, healthcare system, or in the everyday lives of consumers, there are many shared considerations stretching across fields of application. One such consideration is data privacy and consent. It is estimated that law enforcement agencies possess photos of 50% of adults within their facial recognition networks, and, more importantly, that there may not have been informed consent or even basic awareness of this participation.[9] How can legislators encourage proper ethics and transparency in data collection, which is an integral part of AI? Further, in data collection for the development of machine learning algorithms, how can data quality be improved to represent all populations while the reflection of

[7] Urban, Yesh-Brochstein, Raleigh, and Petty. "A Critical Summary of Detroit's Project Green Light and its Greater Context: Detroit Community Technology Project". 9 June 2019. https://detroitcommunitytech.org/system/tdf/librarypdfs/DCTP_PGL_Report.pdf?file=1&type=node&id=77&force=.
[8] "EPIC Comments Re: New Jersey Regulating Law Enforcement's Use of Facial Recognition Technology." n.d. EPIC - Electronic Privacy Information Center. https://epic.org/documents/epic-comments-renew-jersey-regulating-law-enforcements-use-of-facial-recognition-technology/.
[9] Najibi, Alex. "Racial Discrimination in Face Recognition Technology". Harvard University: The Graduate School of Arts. 24 October 2020. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

human cognitive biases is lessened? Secondly, the applications of AI and its impact on marginalized communities should not be ignored. While the development of AI may be a rich man's game, with economic inequality predicted to increase as the rich get richer from investing in AI, it can affect everyone, directly and indirectly.

AI's economic impact isn't only limited to investment; one huge category of AI is automation. Machines don't get tired, and can even perform surgery, all without the fatigue and human error present in blood-and-bone surgeons. But as AI can replicate the tasks formerly performed by humans, again, what does this mean for job loss and unemployment?

In healthcare, AI has the potential to spread medical knowledge, and thus, increase access to specialized care. This may especially benefit areas where there is a physician shortage, such as in rural areas and developing countries.[10] It can also reduce the workload of healthcare providers, who often suffer from burnout. Ophthalmology and radiology are two areas where imaging analysis AI holds great promise of allowing general practitioners to perform diagnoses previously reliant on specialists.[11] But it is important to realize that AI algorithms rely on health records and information from consumers—they need to be trained on data before becoming capable of making predictions or any type of suggested diagnosis. As more and more data is collected from pharmacies, insurance companies, and even fitness trackers, to what extent should consumer privacy be maintained?

As cybersecurity becomes more important than ever, governments and international bodies have begun developing global standards for AI, not only in terms of facilitating technological cooperation but also in this crucial dimension of policy and ethics. There are guidelines for responsible, trustworthy AI, as well as transparency and accountability pushed by studies such as the ProPublica study on COMPAS (a tool used to predict recidivism rates) or the Gender Shades study on facial recognition software. Nevertheless, the problems of bias in development, risks in application, and

[10] "Arguing the Pros and Cons of Artificial Intelligence in Healthcare". Health IT Analytics. 2 March 2022. https://healthitanalytics.com/news/arguing-the-pros-and-cons-of-artificial-intelligence-in-healthcare.
[11] Price, Nicholson W. "Risks and remedies for artificial intelligence in health". Brookings. 14 November 2019. https://www.brookings.edu/research/risks-and-remedies-for-artificial-intelligence-in-healthcare/#:~:text=While%20AI%20offers%20a%20number,health%2Dcare%20problems%20may%20result.

costs to our society remain. As future work is done to address the wide array of implications of this technology, a wide range of perspectives must be considered, with concern not only for the social and cultural dimensions of our society, but realistically, also for the institutions that hold up our societies, such as economies, justice systems, and human health.

History of the Problem

The prospect of artificial beings replicating human intelligence has been an idea explored for thousands of years in philosophy, fiction, and myth. During the 20th century, advancements in technology resulted in the first explorations into the field of artificial intelligence, branching off from machine learning and computer science in the 1950s. Over the past decade, we have observed the gradual integration of AI technology into everyday life, most notably through smartphone technology. In September 2017, Apple announced Face ID during the unveiling of the iPhone X, marking the beginning of widely marketed facial recognition-based security systems to consumers across the globe. The rapid proliferation of facial recognition software has resulted in its adoption by companies, law enforcement, universities, and individuals for a variety of purposes. Often, these purposes require the storage of personal information without valid consent. The lack of consistent application of privacy regulations on this front has resulted in a widely recognized need to rethink pre-digital notions of personal privacy. While companies and governments have been perfecting AI technology and storing data for years, international policy has lagged behind the rapid advancements. As a result, many existing regulations have failed to consider how areas such as privacy, security, policing, and armed conflict have been reshaped by breakthroughs in AI software.

Some of the most recent literature on the issue of AI regulation has come from the European Union and Organization for Economic Co-operation and Development (OECD). In April 2019, the European Commission presented Ethics Guidelines for Trustworthy Artificial Intelligence listing 7 key requirements that AI systems should meet.[12]

Human Agency and Oversight

The intention of all AI systems is to aid humans in performing tasks. However, this requirement specifies that AI should be used in ways that empower users. People should still have the ability to make informed decisions on the ways a specific AI system is being used. To that end, humans should

[12] "Ethics Guidelines for Trustworthy AI." Shaping Europe's Digital Future, European Commission, 26 Apr. 2022, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

have oversight over AI systems, mostly to ensure the continual ethical use of the system. AI should not infringe on basic human rights and human oversight is the best way to ensure that goal. This level of oversight has many approaches, the two most common being human-in-the-loop and human-on-the-loop. The first approach uses a human who starts and stops an AI system when performing tasks. In other words, the AI only works after receiving a cue from its human user. On the other hand, human-on-the-loop does not require a human user to initiate the functioning of an AI. A tangible way to think about these two concepts is with AI assistants like Siri. If an AI assistant is constantly listening for the cue (i.e. "Hey Siri"), then that system would be using human-in-the-loop. However, if a voice assistant were to simply be listening to a conversation you might be having and give you a search result based on something you said, that would be human-on-the-loop.[13] In this scenario, the assistant isn't waiting for a cue and may instead act as soon as it believes that you need assistance with any task.

Technical Robustness and Safety

AI systems must be safe for users and non-users. This requirement is best understood through AI for use in automation. If an AI system is being used to automate a task or an assembly line, in the event of an accident or emergency, the system must have back-up plans to deal with these emergencies. Whether that takes the form of human operators or programming that can be initiated, AI systems must be developed with safety in mind.

Privacy and Data Governance

This requirement is concerned with keeping the data of users of AI systems confidential according to the laws of a country. Users whose data is being interpreted or otherwise used by an AI system must have peace-of-mind knowing that the data they submit is confidential.[14] This is particularly prescient to AI in healthcare, but also applies to other areas. Data should be kept confidential from operators of AI systems, but these systems should also be resilient to hacks and other malicious attacks intended to steal confidential data. Whether that takes the form of anonymizing patient information

[13] *Ibid.*
[14] *Ibid.*

to human operators or other means it is imperative that privacy of users is upheld. Beyond this, developers of AI systems should take good care to ensure that data being used by AI is of high quality and taken with integrity. Otherwise, AI systems will be susceptible to malfunctioning.

Transparency

AI, from the development stage through the real-world application of technologies, should be transparent. At all levels of development and implementation, users and non-users must be aware of how this AI system is being used and what data it is collecting. Furthermore, AI systems should be able to "explain" their decisions to a human, whether an operator or a patient.[15] If an AI system determines a diagnosis or recommends a particular product, that AI must have some way of explaining how it came to that decision. Particularly for human-on-the-loop AI systems, if an AI begins performing operations, it should be able to explain why taking action was necessary. AI systems must also be transparent when interacting with users who may not be aware that they are interacting with an AI. Not only should users be informed that they are, for example, talking with a chatbot AI but also the features and limitations of that system.

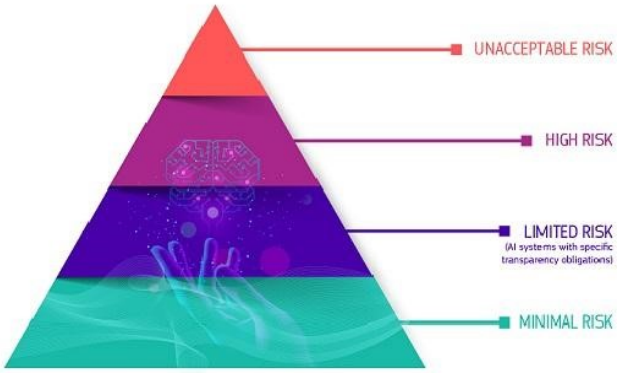
Diversity, Non-Discrimination, and Fairness

The next requirement for AI systems is that unfair biases must be mitigated and eliminated. This usually applies to the development and implementation of AI systems. If AI systems use biased datasets, they will only serve to perpetuate further discrimination and biases from the data that they were fed for training. Therefore, it is imperative that AI systems are not used to marginalize vulnerable groups, discriminate, or otherwise exacerbate prejudices of developers and real-world institutions.[16] AI must also be used to foster diversity and be made accessible to as many people as possible.

[15] *Ibid.*
[16] *Ibid.*

Accountability

The final requirement of sustainable AI involves making AI accountable to humans. This goes beyond the transparency requirement as AI must have mechanisms to take responsibility for actions and decisions made by AI. Typically, this means AI systems must undergo routine audits of algorithms, datasets, and design principles. If AI systems lack auditability, then there is no way for human users to know that the AI has a human's best interest in mind. It is not enough for the AI to undergo these audits after finishing the development process. Like any working machine, AI systems should be checked and the regularity of these inspections may need to be overseen or at least monitored by governments.[17] Most governments do not have regulations for AI and as these systems propagate checks must be put in place.



European Commission Framework for AI Risk.[18]

Towards the implementation of these guidelines, The European Commission has developed a regulatory framework with the purpose of ensuring fundamental rights for people and businesses. This framework defines four levels of risk regarding AI.[19]

[17] *Ibid.*

[18] "Regulatory Framework Proposal on artificial intelligence." Shaping Europe's Digital Future, European Commission, 26 Apr. 2022, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

[19] *Ibid.*

Unacceptable Risk

This tier includes AI systems that would be considered a threat to the safety, livelihoods, and rights of people. These systems should not be explored nor researched. If such technologies were to exist, they should be banned. Examples of AI use that would fall under this category would include voice assistants which promote self-destructive behavior or governmental social scoring schemes. Regulations for these sorts of AI systems are rooted in prohibiting the research of these technologies.[20] By prohibiting their research, it is the hope that these technologies never reach operational capabilities. If they were to, immediate intervention is necessary.

High Risk

AI systems used in infrastructure, education, law enforcement, and border control management among others must be subject to strict obligations before being allowed on the market. High-risk AI systems must be checked for the quality and accuracy of datasets, documentation providing information on the system, and human oversight measures among other regulations. Furthermore, all biometric identification systems such as facial recognition software are considered high risk and are prohibited with narrow exceptions such as searching for a missing child, terrorist threats, or identifying a perpetrator or suspect of a serious criminal offense. Even in these instances, the AI system should be trained using unbiased datasets to reduce the chance of a false conviction or misleading results.[2161] These AI systems are perhaps the most challenging to regulate because their applications are beneficial but have the potential for exploitation. Therefore, it is critical that these systems are carefully monitored.

Limited Risk

Limited Risk AI systems require specific transparency obligations. These systems are not necessarily harmful to humans, but there are still applications for these technologies which could be used for manipulation or exploitation. Chatbots, for example, would belong in this category as it is essential

[20] *Ibid.*
[21] *Ibid.*

that humans know they are communicating with an AI and not a human. Some technologies which are currently limited risk have the potential to—and are likely to—advance into High Risk AI systems.[22] However, technology and a greater understanding of AI would be necessary to cause this increased risk level. Systems currently considered limited risk must be regulated to ensure ongoing research and development is focused on beneficial uses while limiting the manipulation of these technologies for nefarious purposes.

Minimal/No Risk

Minimal-risk AI can be used freely. Some examples include video games and spam filters. These encompass the vast majority of AI systems, especially ones that we interact with on a regular basis. These systems pose little harm to humans and are often freely available on the Internet.[23] Regulation of these systems is still necessary to avoid the exploitation of users. However, due to these systems being widely available many are aware of any potential dangers these may pose.

AI and Consumer Safety

Tim Berners-Lee, an English computer scientist, is credited with inventing the World Wide Web through the introduction of hypertext software to the Internet in 1991. This allowed people to access pages from hyperlinks, ushering in the modern era of networked communication including blogs, email services, and list servers. Social networking services such as GeoCities, Classmates.com, and SixDegress.com were introduced in the late 1990s under what was later classified as "Web 2.0." An information architecture consultant named Darcy DiNucci coined the term "Web 2.0" to describe websites that emphasize user-generated content such as Wikipedia, Facebook, and Twitter. As of 2020, there were as many as 4.08 billion social media users worldwide. Despite the widespread use of social networking over the past decade, safety and security standards for consumers have only recently entered public discourse.

[22] *Ibid.*
[23] *Ibid.*

The largest case to date regarding social media privacy was on April 10, 2018, when a hearing was held in response to revelations of data harvesting by Cambridge Analytica, a political consulting firm that harvested data of 87 million Facebook users to profile voters during the 2016 election.

In November 2021, former US Secretary of State Henry Kissinger published a joint statement along with former Google CEO, Eric Schmidt and MIT professor Daniel Huttenlocher entitled "Being Human in an Age of AI." The article calls for the creation of a government commission dedicated to the regulation of AI, recognizing the importance of AI technology in areas such as law enforcement, healthcare, economics, national security, and international law.[24] AI regulation should go beyond which technologies should and should not be allowed to monitor citizens, but also focus on addressing the role automation plays in society. As automation decreases the number of workers needed to, for example, operate a factory, governments must be prepared to deal with these real-world problems too.

Facial Recognition

The Indian government is introducing an automated facial recognition system across the country which is one of the largest widespread efforts at utilizing facial recognition software to date. The Indian government says that this system will bolster security, prevent crime, and help find missing persons. Digital rights organizations have criticized this effort saying that there is little evidence that this technology will reduce crime. Furthermore, facial recognition software often fails to identify women and darker-skinned persons accurately and its use is problematic in the absence of a data protection law in India. "The technology is being rolled out at a very fast pace in India, on the premise that 24/7 surveillance is necessary and good for us. It is important to challenge this notion, and a court case such as this will also help raise public awareness - most people are not even aware they are being surveilled," said Anushka Jain from the Delhi-based digital rights group Internet Freedom Foundation (IFF).[25]

---

[24] Huttenlocher, Henry Kissinger, Eric Schmidt and Daniel. 2021. "Opinion | the Challenge of Being Human in the Age of AI." Wall Street Journal, November 1, 2021, sec. Opinion. https://www.wsj.com/articles/being-human-artificalintelligence-ai-chess-antibiotic-philosophy-ethics-bill-of-rights-11635795271.

[25] Al Jazeera. "Facial Recognition Taken to Court in India's Surveillance Hotspot." Privacy News | Al Jazeera, Al Jazeera, 21 Jan. 2022, https://www.aljazeera.com/news/2022/1/20/india-surveillance-hotspot-telangana-facial-recognition-courtlawsuit-privacy.

Surveillance warning in Delhi.[26]

Other developed nations such as Australia have seen controversies over the utilization of facial recognition technology for security purposes. In 2016 Australia's Department of Home Affairs began building a national facial recognition database. This database was put to use in 2020 to facilitate COVID-19 containment procedures. Australia was one of several democracies which used facial recognition technology for this purpose. The Australian Human Rights Commission called for a moratorium on the technology until Australia has a specific law to regulate its use.[27] This call highlights one of the most concerning trends regarding the implementation of facial recognition software across the globe—it has expanded without any regulation. While data privacy laws are

.

[26] "File:Delhi Metro (44376702752).Jpg - Wikimedia Commons." 2015. Wikimedia.org. November 7, 2015. https://commons.m.wikimedia.org/wiki/File:Delhi_metro_%2844376702752%29.jpg.
[27] Hendry, Justin. "Human Rights Commission Calls for Temporary Ban on 'High-Risk' Govt Facial Recognition," iT News, 28 May, 2021. https://www.itnews.com.au/news/human-rights-commission-calls-for-temporary-ban-on-high-risk-govtfacial-recognition-565173

being introduced in a growing number of countries, very little attention has been brought to the invasive data-collecting facial recognition databases that have expanded in number in recent years.

The most prominent facial recognition technology provider, US company Clearview AI provides software to companies, law enforcement, universities, and individuals and matches faces to a database of more than 20 billion images from the internet and social media. Clearview has created a searchable database of 20 billion facial images. It has amassed such a large database by scraping photos from social media without users' consent or knowledge. Australian CEO and founder Hoan Ton-That has said the company will not work with authoritarian governments such as North Korea and Iran. However, it has encountered problems in some countries, having already been banned in Canada and Australia.[28] On 24 May, the UK's Information Commissioner's Office (ICO) fined it more than £7.5M (US$9.1M), following a joint investigation with the Office of the Australian Information Commissioner.[29] Ton-That disagrees with the criticisms of Clearview AI's business model maintaining that facial recognition technology has great potential for crime prevention.

Concerns regarding the regulation of AI technology are not only an issue that the international community must contend with in the public sector but in the private sector as well. The utilization of AI by internationally recognized brands has raised questions about whether companies should be able to store users' facial recognition information. In early 2015, Facebook introduced DeepFace, a software that alerts individuals when their face appears in any photo posted on Facebook. When they receive this notification, they can remove their face from the photo. DeepFace software became the subject of several lawsuits under the 2008 Biometric Information Privacy Act with claims that Facebook had been collecting and storing face recognition data of its users without obtaining consent. In response, Meta announced that it plans to shut down Facebook's facial recognition

[28] Mudditt, Jessica. n.d. "The Nation Where Your 'Faceprint' Is Already Being Tracked." Www.bbc.com. https://www.bbc.com/future/article/20220616-the-nation-where-your-faceprint-is-already-being-tracked

[29] "ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted," Information Commissioner's Office, 23 May 2022. https://ico.org.uk/about-the-ico/media-centre/news-andblogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/.

system.[30] Tiktok agreed to a $92 million settlement to a US lawsuit which alleged that the app had used facial recognition in both user videos and its algorithm to identify age, gender, and ethnicity.[31]

[30] Herra, Dana. "Judge Tosses Illinois Privacy Law Class Action vs Facebook over Photo Tagging; California Cases Still Pending." Cook County Record, 27 Jan. 2016, https://cookcountyrecord.com/stories/510660138-judge-tosses-illinoisprivacy-law-class-action-vs-facebook-over-photo-tagging-california-cases-still-pending.
[31] BBC News. "Tiktok Agrees Legal Payout over Facial Recognition." BBC News, BBC News, 26 Feb. 2021, https://web.archive.org/web/20210226160803/https://www.bbc.com/news/technology-56210052.

Past Actions

Due to widespread calls for the regulation of AI development, several nations announced plans for an International Panel on Artificial Intelligence in December 2018, which was quickly renamed the Global Partnership on AI. In June 2020 the Global Partnership on AI was launched in a joint effort by Australia, Canada, the European Union, France, Germany, India, Italy, Japan, Rep. Korea, Mexico, New Zealand, Singapore, Slovenia, the USA, and the UK. Recently, other United Nations entities have begun promoting AI regulation such as the UNICRI Centre for AI and Robotics through reports including *AI and Robotics for Law Enforcement*, a joint effort by the UNICRI and the International Criminal Police Organization (INTERPOL).[32]

On 24 November 2021, the Recommendation on the Ethics of Artificial Intelligence was adopted by UNESCO's General Conference at its 41st session marking the first-ever global agreement on the ethics of AI.[33] While these actions have begun the global discussion on AI technology, they are only just beginning to discuss resolutions regarding the issues at hand. However, the field is new and emerging so little action has been taken to coordinate an international approach to the issue. This gives hope that international cooperation may be easier to coordinate collective action in order to create a normative international standard regarding AI technologies between UN member states.

[32] "High-Level Event: Artificial Intelligence and Robotics - Reshaping the Future of Crime, Terrorism and Security." UNICRI, https://unicri.it/news/article/AI_Robotics_Crime_Terrorism_Security.
[33] "Recommendation on the Ethics of Artificial Intelligence." UNESCO, 5 May 2022. https://en.unesco.org/artificialintelligence/ethics.

Possible Solutions

Consumer Sorting

It is evident that facial recognition technology is imperfect in many ways. As a result, its use in policing and marketing is problematic as it can widen pre-existing inequalities. Facial recognition empowers law enforcement systems around the world, many of which have a long history of racist or anti-activist surveillance.[34] IBM and Microsoft have announced steps to reduce bias by modifying testing cohorts and improving data collection on specific demographics. While this is an important step towards reducing the problems in AI technology, it is not sufficient to rely on companies to regulate themselves.

It is up to this committee to develop a framework that regulates "big data" corporations. Algorithmic audits are a useful tool to identify the shortcomings of facial recognition technology. However, this committee must consider how the UN's unique position also makes it difficult to take actionable steps. Simply put, the UN cannot be the sole body responsible for monitoring facial recognition data across the globe—member states must take action within their borders. Considerations should be made to incentivize member states to regulate public and private collections of user data. Especially for governmental use of facial recognition technologies, the UN must find an effective enforcement mechanism to ensure compliance by all member states.

Coordinated research efforts have become an actionable step to investigate bias in AI. A Gender Shades audit confirmed a decrease in error rates on Black females and investigated Amazon's Rekognition, which also showed a 31% error in gender classification for darker-skinned women.[35] Amazon has alleged issues with auditors' methodology rather than addressing racial biases. It is important that pressure is put on companies that market this type of technology to law enforcement

[34] Bedoya, Alvaro, Privacy as Civil Right (May 12, 2020). New Mexico Law Review, Vol. 50, No. 3, 2020, Available at SSRN: https://ssrn.com/abstract=3599201.

[35] Buolamwini, Joy. "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products." MIT Media Lab, https://www.media.mit.edu/publications/actionable-auditing-investigatingthe-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products.

such as Amazon in order to ensure equitable and unbiased use of AI in the future. Beyond these steps, more must be done to address bias in machine learning across all industries.

Consumer Privacy and Safety

One of the major reasons that consumer privacy continues to be an issue is that market incentives can work against consumer privacy. Dina Florêncio and Cormac Herley (2010) examined the password policy of seventy-five websites and found that password strength is *weaker* for some of the largest, most attacked sites that should have greater incentives to protect their valuable database.[36] One possible explanation is that websites adopt weaker password requirements to avoid decreasing traffic on the site. Evidently, security may compete with a consumer's demand for convenience and low prices. This theory might explain why relatively few firms adopt multi-factor authentication despite its significant security benefits. Incentivizing corporations to increase security protocols or creating regulations to ensure consumer privacy in the face of these opposing market forces can be important steps toward bolstering privacy for consumers and users of heavily trafficked sites. On the other hand, consumers must be educated about the necessity for these strengthened online security protocols which they may see as a barrier to a website's ease of use. Particularly for important websites where sensitive financial and consumer-identifying information is kept, consumers and corporations should be prepared to give up the ease of use in exchange for greater security.

Data Markets

Well-worded privacy policies at the time of the transaction can increase transparency between data buyers and sellers. Particular limitations can be set to ensure that future uses of data are limited. This can be effective in preventing the misuse of personal data as well as increase competition in data markets resulting in efficient market outcomes. Promoting education on privacy and cautioning consumers about the uncertainty of selling personal data can have a similar effect. Identity and payment information are often made crucial for completing transactions for the purpose of data

[36] "Artificial Intelligence and Consumer Privacy." 2019. The Economics of Artificial Intelligence, 439–62. https://doi.org/10.7208/chicago/9780226613475.003.0018.

mining. E-commerce sites such as Amazon and AliBaba often use private information (e.g., age, nationality, gender), personal financial information, personal identity information (e.g., username, gender, occupation, address) together with online shopping behavior (e.g., browsing history, browsing time, shopping habits), etc. to make decisions about advertising. Increasing regulations on what companies can ask will prevent them from gathering information that isn't strictly necessary for transactions.

Automation

Automation is perhaps the most tangible effect AI will have on our everyday lives. Improvements in engineering, electronics, and related fields have brought about innovative machines which can perform many tasks that were once thought impossible by machines. Automation is moving beyond the factory line conveyor belt into fields such as medicine, literature, and banking. As such, countries must take a proactive approach to the issue. However, what sorts of action should be taken? Should advances in technology be stopped in order to avoid a catastrophic revolution in industries that can already be largely automated? Or should we allow the forward momentum of automation to reduce the number of workers needed in particular industries? These are questions governments, industry leaders, and other stakeholders are asking themselves around the world. It is up to policymakers to find ways to address the social and cultural effects stemming from automation.

While it will take many decades before society is fully automated, the experiences of, for example, the automobile manufacturing industry, show the potentially disastrous consequences automation has on local economies. The OECD has identified driving, food service, and cleaning as industries that are currently most susceptible to automation, among many others.[37] How can workers in these fields, some of whom have spent their entire working life in their position, be integrated into other sectors? Governments must create actionable plans to address the economic and social needs of people working in industries that are most susceptible to automation. Finding ways to integrate these people into other sectors with dignity will be essential to the success of workers who lose their jobs due to automation. Beyond this, governments must prepare to grapple with labor markets that

[37] Kiersz, Andy. 2019. "These Are the Industries Most Likely to Be Taken over by Robots." World Economic Forum. April 25, 2019. https://www.weforum.org/agenda/2019/04/these-are-the-industries-most-likely-to-be-taken-over-by-robots.

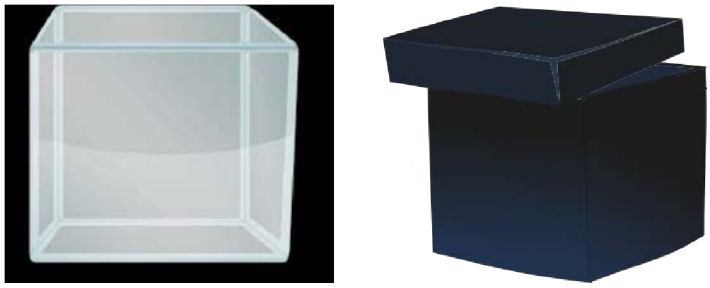
deal with major flows of people from automated industries to other non-automated sectors. This will only intensify job search pressures and could lead to large sectors of unemployed persons.

Beyond all these dilemmas is addressing the way AI is at-large by groups in society. This phenomenon is best understood by considering the implications of AI in healthcare. While the jury is still out on the accuracy between human and algorithmic interpretations of medical data, lawmakers must also consider how patients will handle results given to them by a human versus a robot. Some may find greater relief in having MRI images viewed by a human while other patients may believe an AI interpretation of the results will be more accurate. Either way, society must be prepared to deal with both consumer preferences. Beyond transparency in the interpretation of, for example, medical results, policymakers must consider the extent to which companies must report their use of AI algorithms for other operations. In the aforementioned medical example, a potential patient would theoretically have the option to choose between a doctor they know will have a human specialist examine the photos or a doctor who they know will use AI to examine the photos. However, some industries, such as transportation, would not afford customers that same choice. Particularly in cities and countries with robust public transportation systems, governments would have to choose whether to save on costs by replacing workers with AI or keeping human operators. Consumers, on the other hand, may feel more or less safe knowing their bus or train did not have an operator ready to address any unexpected problems. These are all considerations governments must take into account as they make decisions on the use of AI in automation.

Bloc Positions

In exploring the many nuances that this topic has to offer, blocs may choose to formulate positions based on some of the following considerations. As blocs take on these considerations, amongst others, they must analyze numerous trade-offs as priorities for developing AI are decided. Think about the state of AI in your country and the needs of your country, and then consider the following questions.

What lies within the Black Box? The Concern of Explainability and Interpretability



There are two boxes in front of you. One is transparent, and you can see the mechanisms going on inside it. Another is dark, and you can't see the mechanisms going on inside it. The clear box may produce a worse output than the dark box, but you understand how it came to arrive at the output. Which one would you choose?

Artificial Intelligence is often similar to a black box, as we don't know what's going on inside it. Inputs go in this mysterious black box that is an AI algorithm, and outputs come out. Black box algorithms are born directly from data, making it such that exactly how variables are combined to make predictions is uncertain, even for creators of the algorithm.[38] Historically, this may be because machine learning was first used for more "low-stakes decisions such as online advertising and web search," in which case "individual decisions do not deeply affect human lives."[39] Thus, it was less

[38] Rudin, Cynthia and Radin, Joanna. "Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From an Explainable AI Competition". Harvard Data Science Review. 22 November 2019. https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/7.
[39] *Ibid.*

important for humans to understand how data was being processed behind-the-scenes in AI algorithms. Because machine learning has evolved to have bigger implications on human lives, some argue that interpretable models must be prioritized as a more ethical alternative to black-box models. The more interpretable a model is, the clearer it is how each piece of information fits together to yield the output prediction. While it may seem obvious that interpretability is key, it may come at the expense of a less accurate model.

So what should be prioritized? Explainability or accuracy? The Harvard Data Science Review claims that "the belief that accuracy must be sacrificed for interpretability is inaccurate." Others in the AI community see a trade-off between predictive accuracy and explainability. More complex Machine Learning algorithms such as Neural Networks or Ensemble Methods are known for being worse in terms of explainability while performing better than simpler models such as Linear or Logistic Regression. More specifically, one study investigating this trade-off in predictive silico modeling found that transparent methods generally had lower accuracies. However, this study suggests the trade-off may not be very severe, stating that when adopting a transparent method, the loss in predictive accuracy may be "quite limited."[40] So while a sacrifice is made for a model's decision making to be more understandable by humans, the sacrifice may only be a small one.

Furthermore, the needs for accuracy versus interpretability may vary depending on the context in which AI is used. A 2021 study in the UK on a citizen jury's opinion on AI found that while jurors preferred accuracy over interpretability in situations relating to healthcare, they valued interpretability equally or more so in non-healthcare situations.[41] Therefore, the concern of explainability and interpretability may not be simply a question of which one should be prioritized, but also under which contexts. And the context for which AI is used may not be limited to what field it is applied in. Intention on the part of the creator is also important. Some may believe that by creating complicated models, creators are able "to profit without considering harmful

[40] Johansson, et al. "Trade-off between accuracy and interpretability for predictive in silico modeling". 3 April 2011. https://pubmed.ncbi.nlm.nih.gov/21554073/.
[41] Van der Veer, et al. "Trading off accuracy and explainability in AI decision-making: findings from 2 citizens' juries". 1 August 2021. https://academic.oup.com/jamia/article/28/10/2128/6333351.

consequences."[42] In those cases, creators may not be the most intentional in crafting a product that minimizes harmful effects on people.

In this accuracy-interpretability trade-off, it may be obvious why accuracy matters, but why does interpretability even matter? Assessing the fairness of a complicated model may be difficult. A few years ago, an AI-based technology to predict recidivism rates (the chance someone will commit another crime) known as the Correctional Offender Management Profiling for Alternative Sanctions tool, or COMPAS for short, was engaged in controversy. The Atlantic labeled it "A Popular Algorithm…No Better at Predicting Crimes than Random People," and ProPublica said it was "biased against blacks."[43] Because of trade secret laws, the COMPAS algorithm was essentially "immune from third-party scrutiny," making it difficult for not only courts using COMPAS to understand what goes on within the algorithm's code, but also for those trying to hold AI to ethical standards such as fairness.[44] This case also brings up another important question: how does one define fairness? And how does one police what is "fair" and "unfair"?

What it means to be fair varies somewhat across disciplines and even within disciplines. In the COMPAS debacle, the company behind the algorithm, Northpointe, argued that its algorithm was fair because COMPAS predicted the same likelihood of recidivism across all groups; the investigative journalism nonprofit, ProPublica, did find that the algorithm accurately predicted recidivism for Black and white people at the same rate.[45] But, in the cases when the algorithm was wrong, "Black arrestees who would not be rearrested in a 2-year horizon scored as high risk at twice the rate of white arrestees not subsequently arrested."[46] So while across groups, there was an equal likelihood of recidivism, when the algorithm was wrong, it failed to achieve fairness. Since fairness can be framed in different ways, how can AI be held accountable to ethical standards across all dimensions?

---

[42] Rudin, Cynthia and Radin, Joanna. "Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From an Explainable AI Competition". Harvard Data Science Review. 22 November 2019. https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/7.

[43] Corbett-Davies, et al. "A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear.". 17 October 2016. https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/canan-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/.

[44] Lee Park, Andrew. "Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing". 19 February 2019. https://www.uclalawreview.org/injustice-ex-machina-predictive-algorithms-in-criminal-sentencing/.

[45] "What does 'fairness' mean for machine learning systems?". Berkeley Haas. https://haas.berkeley.edu/wpcontent/uploads/What-is-fairness_-EGAL2.pdf.

[46] *Ibid.*

Is this up to the private sector or public sector? How may quantitative and qualitative tools for fairness be employed? Not only could fairness mean different things to different people, but also how important fairness is could be a question. Prioritizing constraints for fairness may also come at the cost of lower accuracy.[47]

Data Collection: Consumer Privacy and Representation in Data

Remember the garbage-in, garbage-out principle of Machine Learning? A good Artificial Intelligence algorithm relies on large amounts of high-quality data. But is information something consumers want to give up?

Not only is consumer privacy a large concern in data collection, but how people are represented in data also matters. Since machine learning relies heavily on the quality, objectivity, and size of the training data upon which software is developed, it is pivotal that AI algorithms are trained on data representative of all populations. The question then becomes "how data representative of all populations" should be defined. Currently, some countries not only have a greater capacity to develop AI but also have a greater capacity to collect data. As the world becomes increasingly globally integrated, how can data collection be truly representative on an international level? Consider how international cooperation and competition play a role in the domestic and international uses of AI. Should data collection be localized if the current application in mind is only subject to a local scale, or should data collection be more globalized with the expansion of such technology in mind?

Or at a more fundamental level, should our society even allow for more information to be collected on consumers' every move? Sites and services may offer long, small-texted disclaimers that few people read, but is this enough for data collection to be ethical? These days, the extent to which consumers' private lives are kept private is up for debate. Technology is ingrained into many processes surrounding sensitive information like finances and medical history. Legally, politically,

[47] *Ibid*.

socially…how should our society operate when it comes to data ownership over consumer information?

The questions surrounding the relationship between consumer information and AI stretch far beyond collection and usage. The implications of AI on human lives begin with setting the proper intentions before data collection even begins. It encompasses data storage and destruction. Which leads to the question: who or what is responsible for data governance?

Cooperation or Competition?

Is it up to individual countries to decide for themselves how to develop Artificial Intelligence, and in turn, how to address the implications of Artificial Intelligence. In order to advance technological progress, some may believe that competition will push frontiers, while some may believe that cooperation is best. How much or to what extent should AI even be regulated and standardized on an international level?

Bibliography

Al Jazeera. "Facial Recognition Taken to Court in India's Surveillance Hotspot." Privacy News | Al Jazeera, Al Jazeera, 21 Jan. 2022, https://www.aljazeera.com/news/2022/1/20/indiasurveillance-hotspot-telangana-facial-recognition-court-lawsuit-privacy.

"Arguing the Pros and Cons of Artificial Intelligence in Healthcare". Health IT Analytics. 2 March 2022. https://healthitanalytics.com/news/arguing-the-pros-and-cons-of-artificialintelligence-in-healthcare.

"Artificial Intelligence and Consumer Privacy." 2019. The Economics of Artificial Intelligence, 439–62. https://doi.org/10.7208/chicago/9780226613475.003.0018.

BBC News. "Tiktok Agrees Legal Payout over Facial Recognition." BBC News, BBC News, 26 Feb. 2021, https://web.archive.org/web/20210226160803/https://www.bbc.com/news/technology56210052.

Buolamwini, Joy. "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products." MIT Media Lab, https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-ofpublicly-naming-biased-performance-results-of-commercial-ai-products.

Buolamwini, Joy and Gebru, Timmit. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification". 2018. https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

Corbett-Davies, et al. "A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear."17 October 2016. https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-beracist-our-analysis-is-more-cautious-than-propublicas/.

"EPIC Comments Re: New Jersey Regulating Law Enforcement's Use of Facial Recognition Technology." n.d. EPIC - Electronic Privacy Information Center. https://epic.org/documents/epic-comments-re-new-jersey-regulating-lawenforcements-use-of-facial-recognition-technology/.

"Ethics Guidelines for Trustworthy Ai." Shaping Europe's Digital Future, European Commission, 26 Apr. 2022, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

"File:Delhi Metro (44376702752).Jpg - Wikimedia Commons." 2015. Wikimedia.org. November 7, 2015. https://commons.m.wikimedia.org/wiki/File:Delhi_metro_%2844376702752%29.jpg.

Hendry, Justin. "Human Rights Commission Calls for Temporary Ban on 'High-Risk' Govt Facial Recognition," iT News, 28 May, 2021. https://www.itnews.com.au/news/human-rightscommission-calls-for-temporary-ban-on-high-risk-govt-facial-recognition-565173.

Herra, Dana. "Judge Tosses Illinois Privacy Law Class Action vs Facebook over Photo Tagging; California Cases Still Pending." Cook County Record, 27 Jan. 2016, https://cookcountyrecord.com/stories/510660138-judge-tosses-illinois-privacy-law-classaction-vs-facebook-over-photo-tagging-california-cases-still-pending.

"High-Level Event: Artificial Intelligence and Robotics - Reshaping the Future of Crime, Terrorism and Security." UNICRI, https://unicri.it/news/article/AI_Robotics_Crime_Terrorism_Security.

Huttenlocher, Henry Kissinger, Eric Schmidt and Daniel. 2021. "Opinion | the Challenge of Being Human in the Age of AI." Wall Street Journal, November 1, 2021, sec. Opinion. https://www.wsj.com/articles/being-human-artifical-intelligence-ai-chess-antibioticphilosophy-ethics-bill-of-rights-11635795271.

Johansson, et al. "Trade-off between accuracy and interpretability for predictive in silico modeling". 3 April 2011. https://pubmed.ncbi.nlm.nih.gov/21554073/.

Julia.Roesler. 2020. "English: Volkswagen´S First New Generation Electric Car Being Built with Siemens Automation Technology." Wikimedia Commons. February 19, 2020. https://commons.wikimedia.org/wiki/File:Siemens_automation_in_volkswagen_factory.jpg.

Kiersz, Andy. 2019. "These Are the Industries Most Likely to Be Taken over by Robots." World Economic Forum. April 25, 2019. https://www.weforum.org/agenda/2019/04/these-are-theindustries-most-likely-to-be-taken-over-by-robots.

Lee Park, Andrew. "Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing". 19 February 2019. https://www.uclalawreview.org/injustice-ex-machina-predictive-algorithms-incriminal-sentencing/.

Mudditt, Jessica. n.d. "The Nation Where Your 'Faceprint' Is Already Being Tracked." Www.bbc.com. https://www.bbc.com/future/article/20220616-the-nation-where-your-faceprint-is-alreadybeing-tracked.

Najibi, Alex. "Racial Discrimination in Face Recognition Technology". Harvard University: The Graduate School of Arts. 24 October 2020. https://sitn.hms.harvard.edu/flash/2020/racialdiscrimination-in-face-recognition-technology/.

Price, Nicholson W. "Risks and remedies for artificial intelligence in health". Brookings. 14 November 2019. https://www.brookings.edu/research/risks-and-remedies-for-artificialintelligence-in-health-care/#:~:text=While%20AI%20offers%20a%20number,health%2Dcare%20problems%20may%20result.

"Recommendation on the Ethics of Artificial Intelligence." UNESCO, 5 May 2022. https://en.unesco.org/artificial-intelligence/ethics.

"Regulatory Framework Proposal on artificial intelligence." Shaping Europe's Digital Future, European Commission, 26 Apr. 2022, https://digitalstrategy.ec.europa.eu/en/policies/regulatory-framework-ai.

Rudin, Cynthia and Radin, Joanna. "Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From an Explainable AI Competition". Harvard Data Science Review. 22 November 2019. https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/7.

"The Impact of Artificial Intelligence on Unemployment". Technology.org: Science and Technology News. 17 December 2019. https://www.technology.org/2019/12/17/the-impact-of-artificialintelligence-on-unemployment/.

Urban, Yesh-Brochstein, Raleigh, and Petty. "A Critical Summary of Detroit's Project Green Light and its Greater Context: Detroit Community Technology Project". 9 June 2019. https://detroitcommunitytech.org/system/tdf/librarypdfs/DCTP_PGL_Report.pdf?file=1&type=node&id=77&force=.

Van der Veer, et al. "Trading off accuracy and explainability in AI decision-making: findings from 2 citizens' juries". 1 August 2021. https://academic.oup.com/jamia/article/28/10/2128/6333351.

"What does 'fairness' mean for machine learning systems?". Berkeley Haas. https://haas.berkeley.edu/wp-content/uploads/What-is-fairness_-EGAL2.pdf.