On AI Governance

Keith D Foote

Abstract

The concept of AI governance has been developed to promote responsible behavior in the use of artificial intelligence. Artificial intelligence can be used for the betterment of mankind, and has proven itself to be very useful in completing a large number of tasks both quickly and efficiently. Sadly, AI can also be used in support of criminal behavior, ranging from the creation and distribution of misinformation to audio and video impersonations. AI governance can be described as a philosophy developed to minimize the misuse of artificial intelligence for unethical and criminal behavior.

Contents

Introduction

The concept of AI governance has been developed to promote responsible behavior in the use of artificial intelligence. Artificial intelligence can be used for the betterment of mankind, and has proven itself to be very useful in completing a large number of tasks both quickly and efficiently. Sadly, AI can also be used in support of criminal behavior, ranging from the creation and distribution of misinformation to audio and video impersonations.

AI governance can be described as a philosophy developed to minimize the misuse of artificial intelligence for unethical and criminal behavior.

Recent improvements in artificial intelligence — the use of large language models, generative AI, ChatGPT — have prompted both government and industry leaders into discussing the need for a system of ethical guidelines, regulations, and laws when using it. Fears of artificial intelligence replacing workers have also been expressed.

Concerns About the Potential Dangers of AI

Efforts to develop AI governance programs, guidelines, and regulations, are reflections of real concerns about the potential dangers of artificial intelligence. Writers, for instance, have expressed their concerns about artificial intelligence taking their jobs, and went on strike for both increased wages "and" severe restrictions on using AI for writing purposes. There are a number of articles on the internet describing how "you" can train ChatGPT to imitate "your" writing style. (On a personal note, I believe this is a deceptive practice.) The downside of this training process is that ChatGPT can be trained to imitate "other" writers. While certainly unethical, this practice is not illegal.

Artificial intelligence can be a remarkably useful tool in assisting with fraud.

Another significant concern is the ability of modern AI to create life-like images, referred to as "deepfakes". Generative AI can create deep fake videos of individuals saying anything the person in control of the AI wants them to say. Deepfakes have also become a serious concern because of their potential for creating child pornography, or pornography with the AI generated celebrities. As the technology becomes more readily available, revenge porn is also becoming a concern.

The use of generative AI has also become a concern for politicians and political organizations.

Another way generative AI has been used in criminal activities is by imitating voices. Ransom demands have been presented after the re-creation of a daughter's voice on the phone, sobbing and telling a parent she's been kidnapped.

AI governance deals with a variety of critical issues, such as privacy, built-in biases, impersonation, theft, and fraud. It is unfortunate that laws and regulations are necessary to protect individuals within the general population from individuals with weak or no ethics. Businesses should make a point of staying updated on emerging laws and regulations and ensure compliance of their AI systems' creations and deployment, as well as developing their own ethical codes.

Organizations can navigate the ethical concerns raised by the use of artificial intelligence by adhering to a system of AI governance best practices, in turn promoting its responsible use for the betterment of humankind.

Ethics vs the Law

Ethics are moral values that an individual (and the culture they live in) establishes for personal behavior. Laws are structured rules that are based on enforcing commonly agreed upon ethics, and typically include a punishment for breaking those laws. New laws are created when people are being harmed by new circumstances, such as new technology, where an ethical code has not yet been developed, or when ethical norms are ignored, typically to make a dishonest profit.

While the law cannot force people to be honest, empathic, or fair, it can restrict the criminal behavior of people who want to avoid punishment. For example, deliberate deceit, or the betrayal of a confidence, may not be illegal, but does qualify as unethical.

While it is not illegal to provide misinformation to the general public, it is illegal to deceive people for purposes of short term profit (fraud). There are laws against knowingly making false statements to federal government agents (primarily to prevent fraud). This has been extended to lying to FBI agents when they are investigating crimes. (A program of long-term misinformation, such as the one oil companies used to confuse the general population about global warming. Yes, I use the term global warming — climate change deals with specific locations, while global warming covers the entire planet.)

There are no laws protecting the general population from misinformation.

Human Rights and Artificial Intelligence

Human rights are created by humans as the optimal way of dealing with other humans from a societal perspective. The concept of human rights can be considered part of mankind's societal evolution. The protection of an individual’s privacy is considered a human right. Unfortunately, protection against fraud and deceit is not yet considered a human right. Additionally, we have not yet evolved to the point where the right to work is considered a human right.

In the United States, the First Amendment in the *Bill of Rights* deals with freedom of speech: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

The Fourth Amendment deals with privacy: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Some of these rights were designed and created, in part, to deal with specific issues that were serious concerns during the 1760s. Freedom of religion and speech were obviously concerns (that was why they moved to America), but so was privacy. In 1760, a number of British officials were issued writs of assistance, giving them the right to enter people’s homes on a whim to search for smuggled products, and to take anything they wanted. This went on for over a decade, until the revolution in 1776.

In 1781, the Articles of Confederation were approved to create the Congress of the Confederation. The Confederation continued until 1789, but was then replaced with the U.S. Constitution and our current form of government.

To better understand the forefather’s feelings about privacy during the 1760s and early 70s, imagine a policeman coming to your home with a permanent search warrant that gives them the right to enter and search any home they want, whenever they want, and to take people’s possessions without concern.

in Paris, on December 10th, 1948 (after World War II, and with the United States' financial support, the United Nations presented the *Universal Declaration of Human Rights*. Article 14 of this document supports privacy, stating, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." However, the *Universal Declaration of Human Rights* are "guidelines" for countries, not laws or a guarantee of personal freedoms.

What is the Truth?

Protection against fraud is not formally considered a human right. This is primarily because fraud was not mentioned in the U.S.constitution. And then, there's the conflict of freedom of speech versus the freedom to lie and deceive. In the United States, the two have become confused. It is difficult to restrict freedom of speech without restricting creativity and change. The situation becomes confusing, and makes it difficult to create any laws that restrict misinformation.

Do we restrict new ideas, new art, or alternative viewpoints under the guise of "enforcing the truth?"

To gain insight into the dilemma faced by the U.S. government, consider the situation faced by supporters of an alternative physics model (the *Ultra-Space Field Theory*) that uses a field theory paradigm in interpreting the evidence, and finds fault with the currently popular *Standard Model*, which uses mathematical equations as hard supporting evidence and is based on a particle theory paradigm. The *Ultra-Space Field Theory* promotes understanding, while the *Standard Model* promotes the use of mathematical equations (no understanding required).

The conservative physics community considers "any" alternative models to be misinformation. Should the *Ultra-Space Field Theory* be banned?

Current Government Efforts to Protect Human Rights

There is no single law regulating online privacy. Instead, the U.S, is currently relying on a patchwork of state and federal laws.

In order to develop a system that protects both individuals from misinformation, and support the freedom to be innovative, governments must take certain steps. The first step involves developing an understanding of the problems resulting from the unethical use of artificial intelligence. In the United States, this was initiated by the Senate when they asked several high tech CEOs to attend nine sessions, with the first taking place on September 13, 2023, to discuss the CEO's concerns about AI. (It is unclear if the remaining eight sessions ever took place.)

On October 30, 2023, President Biden issued an executive order regarding AI concerns. With the exception of a mandate that requires the "developers of the most powerful AI systems share their safety test results and other critical information with the U.S. government," the executive order deals with "developing" standards and guidance. At this time, the United States has not developed any laws controlling or limiting the behavior of artificial intelligence.

Significant problems causing paralysis in the United States government are the ages of the members of congress combined with a significant amount of bribery. Because of their age, many members of congress have lacked a cultural indoctrination of the criminal and unethical behaviors supported by computers and the internet. These threatening behaviors have become amplified with the evolution of artificial intelligence.

With the passage of time, this blind spot in government representatives has become smaller, but bribery continues, and the more recent chaos in the House of Representatives, with some members of congress deliberately blocking the passage of laws and project funding for a variety of self-serving reasons, also blocks the passage of bills and protections against computer based crimes.

The European Union (EU) was one of the first governmental organizations to decide they needed AI-focused regulations. The final text of their proposed legislation, the EU AI act, is still being developed following an agreement on December 8, 2023. They chose to develop a series of risk levels, with Unacceptable Risk AI Systems described as a threat to people (these "risks" will be banned). Unacceptable risks include:

- The cognitive, deliberate, behavioral manipulation of humans or specific vulnerable groups. An example would be voice-activated toys which encourage children to perform dangerous behavior.
- Social scoring, the process of classifying people using their socio-economic status, behavior, or personal characteristics.
- The use of real-time and remote biometric identification systems.

China does not have the same free speech considerations democratic governments support. As a consequence, their AI priorities are different. *The Interim Administrative Measures for Generative Artificial Intelligence Services* was implemented on August 15, 2023. These AI control regulations require businesses offering generative AI services complete a security assessment and a filing of algorithms. They also require providers to make efforts to improve the accuracy, objectivity, authenticity, reliability, and demand oversight of generated content.

Generally speaking, those countries that are concerned with AI governance are still in the process of developing appropriate laws and regulations to protect their citizens.

Large Tech and Regulatory Capture

Regulatory capture describes a form of corruption when politicians and regulatory agencies are manipulated into serving the interests of large corporations and wealthy individuals. Rather than protecting the public from their abuses, these regulatory agencies support and mask the abuses they are supposed to be protecting the public from. Regulatory agencies and politicians become the tools of large corporations and rich individuals. (The National Rifle Association provides an excellent example of regulatory capture.)

Currently, regulatory capture is being put in place to control the development of laws and regulatory agencies that should restrict and regulate the artificial intelligence industry. In this case, a group of Silicon Valley billionaires have created at least two organizations designed to manipulate and control the government's impact on their AI businesses, Open Philanthropy and the Center for AI Safety.

The extreme theme of artificial intelligence destroying or taking over humanity has become shared by "philanthropic" organizations. (It is my personal belief that their focus on the concern of AI destroying humanity is a distraction designed to promote the monopolization within the AI industry and maximize the profits of the largest AI corporations. A form of gaslighting.) The owners of large businesses supplying artificial intelligence can use this exaggerated fear as a rationalization for restricting and "licensing" AI research.

Consider that U.S. Senators Richard Blumenthal (D-CT) and Josh Hawley (R-MO) have announced legislation to establish restrictions for artificial intelligence. One of their goals is to establish a law titled, *Licensing Regime Administered by an Independent Oversight Body*. Their proposed law states: Companies developing sophisticated general purpose

AI models (e.g.,GPT-4) or models used in high risk situations (e.g., facial recognition) should be required to register with an independent oversight body, which would have the authority to audit companies seeking licenses and cooperating with other enforcers such as state Attorneys General. The entity should also monitor and report on technological developments and economic impacts of AI.

Given the current circumstances, it is predictable the Independent Oversight Body will be made up of a small number of representatives from the most profitable AI organizations. These businesses will promote laws that work to their advantage, resulting in a monopoly of the AI industry.

AI fellows, with salaries paid for by Open Philanthropy, are currently working for the the Department of Homeland Security, the Department of Defense, and the State Department. They are also working in the Senate Commerce Committee and House Science Committee, two groups crucial in developing rules for artificial intelligence. These AI fellows have also been installed in key think tanks that help in shaping AI policy, such as Georgetown University's 'Center for Security and Emerging Technology' and the RAND Corporation.

Dr Andrew Rogoyski, of the Institute for People-Centred AI at the University of Surrey, stated, "I have grave concerns that governments have ceded leadership in AI to the private sector, probably irrecoverably. It's such a powerful technology, with great potential for good and ill, that it needs independent oversight that will represent people, economies and societies, which will be impacted by AI in the future."

Problems Caused by the Unethical Use of AI

While artificial intelligence does have the potential to revolutionize commerce and research, it can, unfortunately, also be used unethically and illegally. There are many potentially negative consequences that can take place through the unethical use of artificial intelligence. These consequences include biases and discrimination, the replacement of workers (in effect, stealing their jobs), outright fraud, and violations of human rights and privacy, and unintended harm.

Bias and Discrimination- Because it has been shown that human prejudices can be transferred to artificial intelligence, biases and discrimination have become significant concerns. If the data used for training artificial intelligence contains inherent biases, those biases are used in the AI system's decision making process. Those biases were first discovered in the banking industry, and more recently, have been discovered when

For example, an AI system used by a hiring company may discriminate against certain job candidates based on their gender, race, or ethnicity. And simply because the data used to train the system contained biased patterns. This can perpetuate existing societal inequalities and harm marginalized groups.

Privacy Violations– Another concern is the violation of privacy and human rights. AI can be used to gather and process vast amounts of personal data, often without individuals' consent or knowledge. This can lead to privacy violations and the misuse of sensitive information. For example, governments and law enforcement agencies can use facial recognition technology to identify and track individuals without their consent. And this can infringe on individuals' right to privacy and freedom of movement.

Unintended harm– Another potential consequence of unethical AI use is unintended harm. This can occur when an AI system is not designed or tested properly, resulting in unintended consequences that can harm individuals or society as a whole. For example, an AI system used in a medical setting that makes incorrect diagnosis or treatment recommendations can harm patients, and put the patient's life at risk.

As AI technology is still developing and has limitations, it is important to involve human judgment in decision-making processes. This can help ensure that ethical considerations are taken into account, and can stop the artificial intelligence from making decisions which could be biased or harmful. By including humans in the decision making process, it helps ensure artificial intelligence is used responsibly and ethically.

As artificial intelligence evolves, ethical considerations become more important than ever, and "laws must be put in place to guide and restrain AI developers and providers," and ensure that AI technology is used responsibly and ethically.

The Creation of Laws

The creation of a law, in a democracy, is time consuming, particularly if the laws involve protecting the public from corporations using unethical practices to increase their profits. For example, Facebook sold information about their customers. This was, and is, still not considered a crime, but does qualify as a tort, allowing a person, or a group of people, to sue for damages, but only after the fact. (Meta – Facebook's owner – paid $725 million to the users of its Facebook platform.)

Torts do not have the same preventative strength that laws do.

A 2018 lawsuit accused Facebook (and Mark Zuckerberg) of misrepresenting organizational policies regarding third-party data access and compromising their user's privacy with sloppy and lax protections. The office of the attorney general has alleged Facebook violated the U.S. Consumer Protection Procedures Act and seeks civil damages for the offense.

Developing AI Governance Best Practices Within a Business

Business managers should consider the impact of AI on their customers and employees, and implement policies that minimize risks and avoid doing harm. By developing a system of AI governance best practices — which include ethics, businesses can support the responsible use of artificial intelligence for the advancement of humankind.

1. Identify AI Generated Materials: Many governments are discussing the required use of watermarks as a way of distinguishing AI generated art. For organizations that are honest and responsible, a watermark provides an easy way of communicating the art was created by AI, and not a human. The problem with watermarks is that they can be removed quite easily, and to increase the potential for confusion and misinformation, watermarks can be added to art created by humans.

Honest and responsible organizations should include a watermark on any AI generated art. Articles that are written by AI should place "AI generated" in the spot where the author's name is normally located, regardless of whether the person who initiated the article wants to claim authorship. (To do otherwise is simply misleading and deceitful.)

2. Dealing with Algorithmic Biases: Unintentional (or secretly planted) biases and prejudices that are built into an AI's algorithms can have an impact on an organization's hiring practices and customer service by using demographics, such as race or gender.

To determine if an AI is biased, give it a test run. Test it several times for biases. Excel has developed What-If analysis tools (Goal Seek and Scenario Manager) that will perform these tests. These tools are designed to promote equity and fairness in AI systems. They ensure the AI operates without discrimination.

3. Customer Security: There are two basic types of customer information that businesses gather. The first is supplied directly by the customer, and includes such things as their home address and phone number, possibly a birth date, etcetera. Everyone agrees this information should be secure and protected.

Artificial intelligence can be combined with data governance to support data privacy and security laws. By developing an AI supported data governance program and security rules, a business can significantly reduce the risks of stolen and exploited data.

The second form of customer information is purchased from other organizations and includes data ranging from online shopping patterns to social media activity. This type of information (referred to as third party data) is collected with the intention of manipulating a human into making a purchase.

Most people don’t like the idea of their personal preferences and needs being observed and exploited. Honest and responsible businesses should not support the use of artificial intelligence in manipulating humans, nor third party data in general.

4. Develop a Philosophy of “Do No Harm” when using Artificial Intelligence: There are businesses whose only goal is short term profits. Deceit is fine, so long as it brings in a profit. But would you do business with them more than once? In the continuous pursuit of profits, it can be easy to lose sight of the big picture.

When ethics are included in the business model, a philosophy of do no harm develops. Honest, accurate information rarely damages a business’s customer base, but deceit or theft typically results in the loss of any future business with that customer. Additionally, accurate information streamlines the efficiency and flow of the larger society, in turn promoting the advancement of humankind. The introduction of misinformation can result in chaos and confusion.

Artificial intelligence can be used to promote chaos and confusion, or it can be used for purposes of good communication.

5. Develop a Code of Ethics for Both the Organization “and” the AI: An AI governance code of ethics should outline the organization's desire and commitment to ethical behavior. This code of ethics may include a commitment to “use artificial intelligence to provide accurate information” and “artificial intelligence shall not be used to create or distribute misinformation.”

Creating an AI governance code of ethics helps an organization to establish clear standards of behavior. If made available to the public, a business's code of ethics can help in developing the trust of customers and stakeholders, mitigating legal risks, and demonstrating social responsibility.

6. The Data Steward and AI Ethics Reports: An AI governance program should include a series of policies and procedures that support ethical concerns. One of these policies should require regularly scheduled ethics reports, and the data steward seems to be an appropriate person to assign this responsibility to. By creating a reporting mechanism on the ethical use of the organization's artificial intelligence, senior leadership can ensure accountability. Routine audits can also help to identify potential legal issues and promote compliance.

These measures collectively strengthen the implementation of an AI governance program and promote responsible AI practices throughout the organization.

7. Educate Management and Staff: Creating a comprehensive AI governance program requires that all staff and management have an understanding of the organization's code of ethics and long term goals. The education process ensures that all staff are working to achieve the same goals, and that no one on staff is misguidedly working against those goals.

The Use of Algorithms in AI Governance

Should we, as humans, find a way to separate and identify accurate information from misinformation, we "might" be able to develop algorithms that prevent artificial intelligence from performing criminal acts and distributing misinformation.

As artificial intelligence continues to evolve, the need for ethical codes supporting long-term behavior patterns for AI, that support healthy human cultures, becomes more and more important. These ethical codes should be built into the algorithms of artificial intelligence.