Ethical Concerns Caused by the 3rd Wave of AI and Legal Countermeasures

Mu Lei

Abstract
The fast rise of the third wave of artificial intelligence (AI) brings about concerns to the human society. Ethically, there are concerns about how to prevent AI from deviating from human values, how to avoid the alienation of AI and make sure that human beings will not be enslaved by the machines, how to deal with the relationship between the personal information security and freedom, and how to handle the moral conflicts caused by AI. The countermeasures should focus on protecting individual privacy, ensuring code security, and embedding the moral programs into AI, thus equipping AI with the ability to make ethical and moral judgments. In response to the broken window effects resulted from AI, a law-based AI management system should be put in place to elevate the industrial threshold and standardize the AI algorithms.

Keywords: artificial intelligence; ethics; privacy; free will; legal norms

1. Introduction
Along with the progress of the big data technologies and deep algorithms, the European and American countries have made breakthroughs with AI, accelerating the third wave of the AI boom. AI serves beyond the sectors where the tasks are easy and repetitive. Despite the great convenience, AI as new technologies and phenomena poses security, ethical and legal challenges in the new forms for human society. In 2014, Elon Musk, founder of Tesla, warned, “We should be cautious with AI. National and international supervision should be introduced to prevent human beings from doing something stupid.” The public and scientists show the same concerns. What ethical issues will AI bring about? How to standardize its application? Extensive and inspiring discussions are made on this topic. On November 24, 2018, at an AI-themed meeting, the members of the Standing Committee of the National People’s Congress agreed that General Secretary Xi Jinping made instructions on the legal issues related to AI at the 9th collective studying session of the Political Bureau of the Central Committee of the CPC. Xi called for further explorations on the legal, ethical and social issues related to AI, and suggested to perfect the laws, regulations, systems, institutions, ethics and morals to ensure the healthy development of AI. By analyzing the concerns, doubts and controversies triggered by AI, this paper aims to draw the countermeasures in response to the ethical implications and to build the new system of legal norms, thus removing the concerns on AI and providing guidance on the safe, reliable and orderly development of AI.

2. Ethical concerns on the development of AI
(I) How to prevent AI from deviating from human values
Deep learning is the most distinctive feature of AI. To some extent, AI “excels in independent thinking”. Learning makes AI smarter, or evil. In the game against Lee Se-dol, AlphaGo lost one round after making a series of rookie mistakes. Some doubt that AlphaGo lost the game on purpose to attract more attention. If the doubt proves to be true, then AI has “acquired” the human thinking and leverages it to compete against human beings, which can be
unsettling. Not all human thoughts and behaviors are “kind”. If AI learns to be deceptive, bullying and manipulative, then it would be a disaster. Back in the 1940s, the sci-fi writer Asimov proposed three ethical rules on AI study: (I) the robots should not hurt the human beings; (II) the robots must obey the human orders; (III) the robots must be able to protect themselves without violating the first two rules. The rules are still insightful today.

Some scholars hold, “According to the modern political institutions, religions shall be subject to reasons. Similarly, the development of AI should be regulated by human minds and intelligence. Otherwise, the prophecy that the world would be ruled by intelligent men could become a reality.”

James R. Clapper, director of National Intelligence, warned about the evil use of AI technologies. In the annual security report, he cautioned that the weaknesses in cyberspace would be augmented by AI, although the AI systems may make our life easier. AI is the creation of human beings, but it may surpass human beings after “learning”. Under this context, some argue, “We don’t want AI to break the balance between technology and ethics. But we are not even satisfied with what we have achieved on the ethical building. If our society is unfair, manipulative, disharmonious and out of order, then AI robots would make things worse.” Stephen Cave, executive director of Leverhume Centre for the Future of Intelligence at Cambridge University, believes, “Excessive AI use is risky.”

(II) How to avoid AI alienation

With a Latin origin of alienalio, the word “alienation” is used by Marx to explain the labor alienation phenomena in the political economy, i.e. the products of human labor are objectified into the aliens that enslave and control the human beings. In other words, the fruits of the subjects’ labor grow into the alien forces that dominate and enslave the subjects. On January 7, 2017, Alibaba held the 2nd New Think Tank and New Economy Conference themed on Vision 2046. At the round table talk under the theme of Opportunities and Risks of AI, Duan Yongchao, CSO of SEEC and chief adviser to ZenCoo noted, “At the AI era, we are tamed by the machines while we tame them.”

There are scholars believing, “If the machines are allowed to develop without restrictions, then the human beings will be enslaved by them in future.” In late May 2017, the 1st Global Artificial Intelligence Summit was held. At the Summit, Stuart Russel, co-author of Artificial Intelligence: A Modern Approach, warned about AI abuse, because the killer machines could be invented. To justify the benefits of AI, the robots must fulfill the humans’ wishes as much as possible. In other words, the machines are supposed to satisfy, rather than discomfort, human beings.

Therefore, there is a risk that AI might be alienated. Human beings as the designer, developer and user of the AI applications would lose control over AI when they are over-reliant on it and then be controlled and enslaved by AI. The progress of AI would surely free human beings from brainwork and physical labor and improve the living quality of human beings. But the human brains may become less intelligent as human beings become over-dependent on AI. The capacity to think independently and to solve the problems would degenerate consequently. According to the report Preparing for the Future of Artificial Intelligence released by the White House, the recent machines do a better job than human beings when implementing certain tasks. If AI is self-aware and has the ambition to control the human beings, the humans would “be weaker and more powerless than the Indians who were in face of the firelocks of the white race, and get controlled by AI”.

(III) How to deal with the relationship between the personal information security and freedom

Big data is the basis of AI and advances the third wave of AI. It provides unlimited space for the “deep learning” of AI. Without bit data, AI will get nowhere. However, “The ubiquitous sensors and AI enable the businesses to collect personal information not only when the users are using digital devices, but when

1 Yu Xingzhong. When law meets AI [N]. Legal Daily, 2016-3-28 (007).
3 Guan Xianshi. Why are we worrying about AI? [N]. Guangxi Daily, 2016-3-16 (002).
they travel between the public space and private space.” 10 When the private space is completely exposed to AI, personal life would get severe disruption. It is reported that “Google’s London-based subsidiary Deep Mind has acquired the medical data of over 1.6 million patients from three hospitals run by the Royal Free London NHS Foundation Trust.” 11 The IEEE Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems (1st Edition) released in 2016 notes, “Data asymmetry is a moral dilemma for personal information protection. In the age of algorithms, AI uses more and more personal data. To address the issue of asymmetry, the policies on personal information protection should be formulated. The autonomous and intelligent systems should be designed and applied based on the respect for the integrity of personal data.” 12

In addition, AI brings about an adverse impact on the freedom and political rights of the citizens. According to the American tech media The Verge, in 2015, the police in Baltimore identified and arrested the protesters with Geofeedia, a facial recognition application that analyses the photos that the Instagram, Facebook and Twitter users shared. Geofeedia is a social medial monitoring company in Chicago. It captures massive user information from the social networks and provides it for hundreds of law-enforcement organs, which use the information to monitor and track the activities of the social organizations and the citizens. 13 Some scholars hold, “The AI applications will soon become creepy. We all should be nervous about the consequence of building a country of supervision.” 14 The scientific rules should be put in place to handle the relationship between privacy protection, information security and AI development.

(IV) How to handle the moral conflicts caused by AI

At the beginning of the third wave, AI has been widely used in industrial production, auto-driving, medical diagnostics, housekeeping services and aviation services, making people’s life and work easier. Despite the benefits, AI can be confusing sometimes. In July 2015, a robot under debugging at VW’s manufacturing plant “attacked” a worker and rolled over him on the metal plate, causing his death. On March 23, 2016, Microsoft launched the AI ChatBot Tay, which was quite popular because it can “learn” things. But soon Tay was trained by some netizens to “talk” aggressive and discriminatory words against different groups. Tay was removed from the application stores 16 hours after its launch. In the same year, Google’s autonomous vehicle under test in California collided with a bus. Luckily, no life was claimed. The accident poses a question: in case of an emergency, should the autonomous vehicle prioritize to protect its passengers or the pedestrians? Mercedes-Benz’ answer to this question is the passengers. This tricky moral question is discussed by the legislators, the ethical experts and the lawyers. For the management of Mercedes-Benz’ driver assistant, active safety and evaluation system, the answer is uncertain. 15

In face of the “moral dilemma”, some pointed out that “no one would buy a car that avoids running over the pedestrians at the cost of his or her own life.” This point of view makes sense morally. “The auto vehicles have more control over the passengers. It is the best that the vehicles save the passengers rather than the pedestrians. People may also argue that Mercedes-Benz has made the moral commitment to the passengers, who leave their lives and safety to the AI systems.” 16 These accidents cause reflections and discussions about AI: how to determine the responsibilities of the fabricated AI systems when they cause damages to others? Who should be held accountable for the ChatBot Tay’s

discrimination against the minorities, the females and the disabled: the developers or Google? Is Tay that can “learn” the subject of liability? Is the robot’s “killing” a murder or an accident? If a murder, is it caused by the flawed design of AI or the “acquired” initiative? If an accident, who should be held accountable? The designer? The manufacturer? The user? Or just AI? The responsibility ethics caused by AI goes far beyond the governance scope of social ethics and laws today. The AI-caused legal and ethical issues must be taken seriously.

3. Legal norms in response to the ethical issues caused by AI

(i) Uphold data justice and protect individual privacy

In the age of AI, people have to “sacrifice privacy, personal life and critical mind in exchange for predictability, safety and prolonged life”. Living in a world where the monitoring cameras are everywhere, people can hardly protect themselves from not being monitored by the cameras. The price bias based on big data is denounced by the public. It refers to the varied pricing policies for the same product among different users. The systems estimate the users’ need urgency for an item by analyzing the location, search items and search frequency of the users, and then adjust the prices accordingly. This, in essence, is the abuse of user data. The data includes the users’ privacy, i.e. the users’ preferences for goods and services and the traveling patterns. However, “as the generator and user of the data, the citizens are involved in the ‘basic cycle of big data’, but have no control over the information and technology infrastructures.”

When fed with sufficient data, AI would quantify the “value” of each person, which is definitely an infringement of the basic human rights of the citizens.

“To prevent the concentration of value and power, we must balance the benefits and risks of the digital platforms (including the industrial platforms), make sure they are open, and create opportunities for collaborative innovation.” To some extent, people in the AI age would get more “transparent”. But authorization must be obtained before any institution or individual collects and uses personal information. To be specific, the privacy agreement should be concise; the platforms should not collect the users’ personal information irrelevant to the services it provides; the individual data collected by any institution is used to provide better services only, and the data collectors shall ensure data security and avoid data leakage.

(ii) Protect code security and prevent and monitor risks

In the AI age, “code is law”. AI functions based on the codes programmed by human beings and affects every aspect of human life. Codes function as the new rules of the world. “In cyberspace, the internal and external power is centralized by the hardware and software designers.” The transparency and legitimacy of codes therefore attract increasing attention. It is true that only a few excel in coding. Most of the users are in a passive position. To make profits and avoid censorship, most intelligent systems are not transparent. “Some designers choose not to make the source codes public. The users don’t know the rules behind it. They cannot come up with a different idea or participate in the decision-making process. They just have to take the results.”

With advanced codes, many private companies have collected massive data, which makes them valuable partners in terms of “information sharing”. The governments may work with these companies in exchange for their “client information”. Code as a new medium blurs the boundary between the market and the state. Empowered by codes, the public power expands and the “monitoring state” comes into being, which goes against the public intention to restrict the public power with

21 Yu Sinan. AI should not develop at the cost of privacy. People’s Daily, 2017-10-27(020).
technologies. At the same time, intellectual properties and trade secrets enable private companies to expand their businesses in an unprecedented way. With codes, these companies gain “private forces”. Both the expanding public power and the private forces are shocking the social order of justice. Like the previous technological revolutions, AI cannot benefit all classes and groups equally. But it should not be used as a means of monopoly and social monitoring. “The fight for open-source codes is no less important than the fight for democracy and the fight against the abused of the state power.” The open-source codes are the “basis of an open society”. Therefore, codes should be secure and transparent throughout development, production and maintenance.

(iii) Embed moral codes and stick to the original functions of algorithms

The developers should embed the moral codes into the algorithms of AI products so that the products make correct choices in specific conditions. To this end, the moral codes should be a simple copy of human morals, which can be extremely complicated because different individuals make varied choices in face of the same situation. If such complexity is transplanted into AI, then the executive force of AI would be undermined and chaos may take place. In addition, moral codes should be free from individual or group preferences. Driven by profits, the companies may add secret rules to the algorithms. For instance, Google Map entices the users to visit the places that the advertisers want them to go. Such soft constraints go against people’s expectations for AI. Lastly, the moral codes must be customized based on specific situations, respecting the local and individual conditions.

Moreover, the moral codes should be designed in the bottom-up approach, which holds that moral habits are self-fostered and acquired in the cooperation and sharing with others. If the moral codes are created in an up-down approach, then it may arouse the misunderstanding that the public are ruled by privileged. For example, the American fin-tech company Zest developed the AI credit evaluation platform ZAML, which determines the users’ credit based on their online behaviors, rather than on the actual credit records. ZAML “examines the users’ applications”, checks the spelling and grammar mistakes in the applications, and then determines the users’ “compliance” tendency based on the examination and checking results. The immigrants who are non-native English speakers would get negative results. In fact, grammar and spelling reflect one’s literacy rather than his or her moralities. This grave mistake was made because the platform was designed in the top-down approach and the public voice was not taken into consideration at all.

4. Legal countermeasures against the shock of AI

(i) Elevate the threshold of the AI industry

AI is a blue ocean for capital, taken as the lifeline by all tech businesses. Just like Pandora’s Box, AI is magical and appealing. The reasonable call for proper control over AI has been overlooked since 2017. AI evolves in an overwhelming way. The AI products that cover the key areas of the citizens’ individual life must be used in accordance with the laws.

1. Individual biological features

Many AI products are used to test the data like fingerprints, pupils, speeches and DNA. They make testing tasks easier and efficient. The data tested is the most valuable passwords for individuals. But in the virtual world, such information is merely codes, which turn a human into a system. “Online information covers every step of your life, from birth to death. As the personal data accumulates, the life journey of a human unfolds in the computer database.” When all individual data is stored in the virtual space, one may concern about the existence of another copy of him or her in the virtual world and the possible harm brought about to the real “he or she” by the virtual “he or she”. This is by no means exaggeration. According to Kayne McGladrey, IEEE member and director of the Information Security Department in Integral Partners, “Theoretically, a fingerprint mold that can be recognized by the sensors can be manufactured as long as the resolution of the scanned fingerprints is high. And this could take place in a completely unknowing

way.” The fake fingerprints can be used to unlock mobile phones and to steal personal property and private data.

Speeches and videos can be forged by Al technologies as well. Adobe’s software Project Voco could transcribe and edit the speeches and then generate new speeches with identical tone and pitch. Researchers at Washington University have developed the AI technologies that “could produce the fake videos” and match the speakers’ mouth shapes with the sounds from the audio clips. The laws on preventing the abuse of individual biological data lag behind. For instance, the celebrities suffer much from the obscene videos generated by the AI-empowered face-swapping applications. Laws must be put in place to restrict the application of AI applications. On one hand, data such as the fingerprints should only be exported one-way once input into the systems. The exported data shall not be used by any AI applications. On the other hand, the user shall not get the authorization from the AI applications when he or she tries to match his or her biological data with another person.

2. Destructive weapons

Many AI products have hidden and uncontrollable destructive forces. An adequate risk alarm system should be established before these products bring about a shocking impact on human society. In 2017, Google worked with the US Department of Defense on Project Maven, which provided AI technologies for the military to analyze the videos collected by UAVs. This project was opposed by several Google employees and over 1,000 famous scientists. Google claimed that it played a small part in the project, only providing the open-source machine learning software for the Department of Defense. At the same time, the company needed the massive video samples collected by the military UAVs and used the samples to train the machine learning models. But public concerns remain. What the public are afraid of the most is not the expansion of Google into a business empire, but the dominance of AI over human society.

It would be much more secure if the core technologies are made known to only a limited few. The codes, based on which the AI weapons of mass destruction are developed, should be secure and transparent with no value preferences. The governance, author and controller over the author of the codes are key to ensuring justice in practices. If some of the code developers hold value preferences and make the AI weapons more aggressive and the military, without knowing the existence of such preferences, brings about worse consequences than expected, then who should be held accountable? If the military authorizes the authors to tamper the codes without notifying the company, then should the company be held accountable for the legal consequences? Or if the aggressive codes are jointly written by the company and the military, how should the liabilities be distributed?

To avoid and solve these challenging issues, companies should be banned from developing and manufacturing destructive weapons. Compared to public institutions, companies are often run in an invisible way. Over-intervention over the companies would hinder innovation while indulgence may bring about the devastating consequences. The contract society is built to protect the security of the public. No armed deterrent forces should be developed in the disguise of trade secrets. In the film Lord of War, the weapon dealers sell conventional weapons worldwide, causing countless bloody incidents. The technical and operative forces of destruction of the AI weapons are far more powerful than that of the conventional ones, enabling the individual criminals to launch the attacks that require teamwork in the past. In addition, the criminals have more means of reconnaissance because the AI weapons can be operated in distance. These products should be developed and circulated in a restricted area to avoid any uncontrollable threats to human society.

(Ii) Standardize the operation permissions of Al products

It is depressing that no law makes it implicit that technological progress should benefit all individuals in society. Technology in itself does not necessarily make the society just. In the previous technological revolutions, it is the law the makes the society fair. But unlike the previous revolutions, the social imbalance caused by AI is more elusive, making the relationship between the producers and the capital more complicated. Take the autonomous vehicles as an example. By now, no company is able to develop a product that runs perfectly on the roads by itself. The AI products are often designed and improved based on big data, which is generated by the users’ behavior. In other words, if data use is excessively restricted, then it will make the upgrade of AI products difficult; but if the AI products are allowed to collect the users’ information without constraints, then every user will be transparent. From the perspective of public power, it is challenging to strike the balance between data protection and
technological progress. This is not supposed to be part of the paternalism of the law.

Therefore, the public power, particularly the law, should not go into details when governing the AI products. Instead, it should only set out the general operating rules. To specific, the laws should respect and safeguard the citizens’ autonomy when they use AI products. Many AI products, once being installed, coerce the users to grant permission to access the users’ Contact, Microphone and Camera; otherwise, the users will not be able to use the products. This is the infringement on the users’ privacy. When all companies that develop the like products follow suit, the users will be in the passive position. Many AI products adopt the agree-authorization mode, i.e. the principle of informed consent, which is a king clause in the area of personal information. The clause is intended to enrich the connotation of autonomy. But in practice, it has been abused. The user agreements of AI products are lengthy. The users often have no patience to read through before accepting the agreements, which is deemed as the strong acceptance by the companies.

With the strong acceptance in place, the users should not stop the AI products from collecting personal information when they use the products; otherwise, the products cannot be used. To address this issue, the consent pattern of the users should be put into better protections. The conventional consent pattern is composed of “full notification + express consent + legal handling”,30 which fails to well respect individual willingness. Actually, most individuals do not well understand how personal information will be used. It’s like one remains confused even if he or she reads through a series of mathematical formulas. He or she cannot fully understand the formulas unless putting them into actual use. Therefore, a flexible exit mechanism should be designed, allowing users to ban AI products from accessing personal information in specific conditions. For example, if the user who has allowed an AI product to access his or her Microphone decides to withdraw the permission out of privacy concerns, then the AI product must respect the user’s decision and make sure that the product can be normally used as before.

(III) Prohibit to preset the algorithms that transcend the human morals

In the general sense, moral algorithms should be set in response to the possible harm created by AI products. And these algorithms should be used under strict restrictions. The human morals spiral as a result of natural selection. Today, the transhumanism is shaking the traditional moral system that has been exercised in human society for thousands of years. Transhumanism originated after the Enlightenment in the 17th Century. Constrained by the technical factors, it failed to boom then. The recent surge of AI technologies contributes to the revival of transhumanism, which contends that human beings should continue to evolve to overcome their born flaws. This idea is dangerous in that it blurs the essence of human beings. For instance, it calls for a stronger constitution and a longer life, which, though seemingly attractive, are tearing down the human society.

If the algorithms that transcend human morals are preset in the AI products to make life better, then neo-Darwinism would be inevitable. If the moral standards of society are set as high as those followed by the sages, then the public would find it hard to survive. The transhumanist morals cannot be put into practice unless the individuals are free from the material pressures; otherwise, they could not be ready to help whenever needed. The transhumanist moral algorithms imply that the technologies are not within the complete control of human beings. They standardize human behaviors from a divine perspective. Technologies are tools rather than guides. It is imperative to standardize the application of AI with laws and prohibit the preset transhumanist moral algorithms, thus preventing the AI technologies from overstepping the boundaries and overturning the morals and ethics of the human society.