Translation

The following document, issued just prior to the opening of the World Artificial Intelligence Conference (WAIC) in Shanghai in late August 2019, consists of proposed legal guidelines related to AI security. The guidelines—apparently issued only in Chinese, without named authors—put forward legal means to ameliorate a wide variety of potential dangers posed by the rise of AI technology, such as bugs, hackers, algorithmic bias, and structural unemployment.

Title
WAIC Artificial Intelligence Security and Rule of Law Guidelines (2019)
WAIC人工智能安全与法治导则（2019）

Author
2019 World Artificial Intelligence Conference (WAIC; 2019世界人工智能大会)

Source
This document was published on August 30, 2019 as an embedded image file in an article about WAIC 2019 on *Guangming Wang* (光明网), a web portal associated with *Guangming Daily* (光明日报), an official newspaper of the Communist Party of China (CPC) Central Committee aimed at an intellectual audience.

The Chinese source text of the 2019 WAIC guidelines is available online at:
https://imgtech.gmw.cn/attachement/jpg/site2/20190830/005056a56a1b1ed33d9820.jpg
The Guangming Wang *article to which the WAIC guidelines are attached is available online at:*
http://tech.gmw.cn/2019-08/30/content_33123802.htm?s=gmwreco2

Translation Date	Translator	Editor
15 January 2020	Etcetera Language Group, Inc.	Ben Murphy, CSET Translation Lead

Artificial intelligence (AI) is a disruptive technology that is ushering in a new wave of technological revolution and industry transformation, and while it is creating enormous benefits for humankind, it is also giving rise to a variety of entirely new security risks. These AI Security and Rule of Law Guidelines have been proposed in order to scientifically anticipate and control the security risks of AI development, with governance focusing on a number of key issues each year in accordance with the principles of step-by-step progress and differentiated (分类) policy implementation. The focus in 2019 is on algorithm security, data security, intellectual property rights (IPR), social and employment issues, and legal liability issues.

I. AI Algorithm Security

(i) Risks and challenges

AI algorithm security risk refers to various kinds of security risks caused due to AI algorithm design and the running of programs. It mainly includes technical flaws, design bias, and black box algorithms.

1. Technical flaws. Technical flaws in algorithm models make AI systems unable to run normally or vulnerable to network attacks or malicious sample intrusion, generating unexpected or even harmful results and resulting in losses to personnel or property.

2. Design bias. Value biases on the part of algorithm designers themselves make algorithms unable to achieve the well-intentioned goals established by the designers, generating unexpected and harmful social results, such as algorithmic bias.

3. Black box algorithms. The trend in AI technology is toward self-learning and continuous evolution. Not only is it difficult for external users to understand the logic of algorithm operations, but it is also increasingly difficult for developers themselves to fully explain the decision-making mechanisms of their algorithms, and this algorithmic "black box" tendency will lead to a loss of control over technology and other harmful results.

(ii) Rule of law response

1. Carry out technical assessment of algorithm security. Through policy and legal guidance, encourage R&D of AI security technology, build an AI software quality assessment system, and carry out assessment testing of key AI applications.

2. Promote the technologically ethical introduction of algorithms. Laws must strengthen the design of algorithm models based on human ethical norms, require that AI developers design explainable intelligent systems, and encourage the continuous calibration of intelligent algorithm logic with the values and norms of human society.

3. Strengthen the transparent supervision of intelligent algorithms. Create new algorithm regulatory models and establish a multi-layered regulatory system. Governments must regulate AI products and services according to law, and AI corporations and the industry must establish corresponding algorithm supervision systems, and maintain regulatory collaboration with governments.

II. AI Data Security

(i) Risks and challenges

AI data security risk refers to the various kinds of security risks generated in the process of data acquisition, analysis, and transmission by AI systems, and mainly includes data privacy, data protection, and data quality risks.

1. Data privacy. Data privacy risks include the automated obtaining of users' sensitive information during the acquisition phase, using intelligent mining of users' non-sensitive data during the analysis phase to derive sensitive personal information and then utilizing it, and, during the transmission phase, transmitting user data without permission to third-party institutions or other countries (regions).

2. Data protection. Data protection risk refers to where AI system data resources are subject to attacks, theft, tampering, etc., causing data breaches to occur or systems to become unusable or even out of control. Data are the foundation for the normal and stable operation of AI products, and as they involve user privacy, trade secrets, and even state secrets, data protection challenges are particularly daunting.

3. Data quality. AI R&D and applications are highly dependent on data quality. Data quality deficiencies give rise to significant risk, which mainly includes security risks due to insufficient data set size and diversity, as well as data set contamination.

(ii) Rule of law response

1. Strengthen data security legislation and law enforcement. Carry out systematic legislation and strict law enforcement for personal data and important data, and formulate a differentiated, level-by-level management system and standards incorporating key AI application scenarios. AI corporations/industries must strengthen legal and administrative supervision of the acquisition and use of sensitive personal data.

2. Augment AI technology development pathways. The mainstream technology pathway for AI at present is based on deep learning from vast quantities of data (海量数据). In the future, it will be necessary to use policy measures to support diversified development of AI technology, such as AI algorithm technology based on smaller data sets.

3. Improve the level of AI data resource management. Promote data resource sharing and exchange between the public and private sectors, build AI quality training databases by individual industry sectors, lower AI data acquisition costs, and improve AI industry data quality.

III. AI Intellectual Property Rights

(i) Risks and challenges

AI IPR issues refers to the intellectual property issues that are generated from using AI to create literary, artistic, and other works. These mainly include the risks and challenges associated with algorithm IPR, data IPR, and creative works IPR.

1. Algorithm IPR. AI systems are characterized by automated learning and automatic coding and by being unexplainable. The passive protection model of existing software copyright has deficiencies, as infringers can use code representation forms that easily bypass algorithms in order to simulate or even surpass their functions, while the existing patent protection model is often unable to meet the demands of AI business innovation due the relatively high thresholds and long periods involved.

2. Data IPR. AI systems handle different kinds of data resources mainly through automated methods, while copyright protection uses a database's content selection or arrangement to reflect its "originality," and AI data resource acquisition and processing methods cause data IPR definitions to have great uncertainty.

3. Creative works IPR. For creative works, the development of AI is making the definition of "originality" ever vaguer, and the traditional copyright protection model centered on human intellectual labor faces difficulties, giving rise to problems identifying infringement among AI systems and between AI systems and human creative works.

(ii) Rule of law response

1. Strengthen AI algorithm patent protection. Broaden the scope of protection under patent law for AI algorithms, formulate a supporting system for AI algorithm patent applications, use technical means to improve the examination of AI algorithm patents, and improve the efficiency of AI algorithm patent reviews.

2. Encourage protection of AI data openness. Clarify ownership of AI data, undertake identification of intellectual property rights for corporate data resources and, on that basis, encourage corporations to strengthen the circulation and sharing of AI data resources, and push them to build AI datasets.

3. Encourage conversion of AI works into intellectual property. Undertake scientific identification of "originality" in AI creative works based on the Copyright Law, etc., with IPR protection to be granted to qualified creative works, and deconstruct the AI creation process to further confirm intellectual property ownership and the distribution of rights and benefits.

IV. AI Social and Employment Issues

(i) Risks and challenges

AI technology development poses risks and challenges for society's existing production structure and distribution system. These mainly include such issues as structural unemployment and increased income inequality.

1. Structural unemployment. The widespread application of AI technology will lead to the restructuring and fusing of traditional industries. Numerous traditional occupations will inevitably be replaced by AI, and those do not just include simple repetitive and streamlined labor jobs; they also include some professional and skilled knowledge work jobs.

2. Emerging labor shortages. At the same time that AI technology replaces traditional occupations, it is also creating a series of brand new jobs, and in particular places greater demands on the innovation, creativity, and entrepreneurial abilities of the workforce. The existing labor force structure and education system are still ill-equipped to adapt to this transformation, and emerging occupations face labor shortages.

3. Increased income inequality. As AI technology drives a leap in productivity for the society as a whole, the society's wealth will be accumulated by a minority of industries and corporations that possess AI technology advantages. This will constitute a major influence on the distributive relationships of different industries, different corporations, and different jobs. Income distribution disparities among workers will also grow as a result.

(ii) Rule of law response

1. Strengthen supervision of AI workforce substitution. Strengthen assessment of the employment risks of AI technology applications, issue legal regulations, carry out supervision and assistance for industries and occupations facing AI technology substitution, safeguard the job opportunities and rights of workers, especially those in low and middle income brackets, and promote orderly AI workforce substitution and career pivoting, so as to protect against the danger of large-scale unemployment in society.

2. Accelerate cultivation of the emerging workforce for AI. With an orientation toward AI development trends, scientifically plan the basic education and vocational education systems, ramp up cultivation of various kinds of AI talent, strengthen establishment of AI programs and labs in basic education, and support development of social institutions for AI career pivoting.

3. Carry out income adjustment oriented toward AI. Taking both efficiency and fairness into account, and while encouraging corporation to earn large profits through AI innovation, strengthen adjustment of society's distribution of income in the AI era, provide protection and assistance to the workforces of traditional industries hit hard by artificial intelligence, and increase the rationality and accuracy of secondary distribution (二次分配) [government programs to reduce income inequality] in society.

V. AI Product Legal Liability Issues

(i) Risks and challenges

AI product legal liability refers to problems concerning the identification and bearing of legal liability after acts of infringement or criminal acts are initiated in the process of using AI products or services. They mainly include: ambiguous AI legal entities, and the complexity involved in delimiting responsibility for AI.

1. Multiplicity and ambiguity of AI product legal entities. Multiple legal entities are involved in AI products, including AI product designers, producers, operators, and users. AI product legal entities are difficult to determine.

2. Complexity of AI product infringement liability. This includes: AI infringement caused due to improper use by AI controllers and users; intentional use of AI by AI controllers and users to engage in infringing behavior; infringement resulting from hacking and other external technological intrusions; and infringing behavior resulting from AI systems in the future possessing "self-learning" and "self-awareness" (自主意识).

(ii) Rule of law response

1. Clarify responsible entities. In this age of weak artificial intelligence, AI products themselves do not qualify as independent legal entities. AI products are positioned as "tools," and AI designers, producers, operators, and users bear the legal entity responsibilities.

2. Scientifically allocate legal liability for AI infringement. Based on the principle of liability for fault, where the fault is on the part of product designers, producers, operators, or users, liability is to be shared according to the degree of fault; where the infringement is caused by external technological intrusion, the technological intruders shall be held accountable. For infringement consequences that result from hazards that were impossible to predict at the early stages of AI product development owing to technological limitations, mechanisms such as insurance should be introduced to effect the sharing of liability.

2019 World Artificial Intelligence Security Summit (高端对话)
2019 World Artificial Intelligence Conference, Rule of Law Forum
August 30, 2019