Research on Legal Challenges Brought by the Development of Internet of Things

LI Meixiang
School of Law, Shandong University of Technology, Shandong, China

Abstract

The promotion and application of Internet of Things has brought earth-shaking changes to our lives. It has also spawned many legal problems□such as the protection of citizens' privacy rights, enterprises' intellectual property strategy, and national network information security, etc. In this context, we need to carry out rational analysis and prediction of these problems, and put forward targeted suggestions for legal improvement, which can better prevent the legal risks brought by the development of Internet of things.

Keywords

Internet of things; Privacy; Intellectual Property; Information Security

I. Introduction

In recent years, Internet of Things (referred to as IoT) has developed rapidly in various aspects such as city management, industrial production, health care, and family life, etc. It is estimated that by the end of 2020, the scale of China's IoT industry will reach 1.5 trillion yuan. However, China only focuses on the development of IoT technologies, and ignores its legal challenges. In 2009, Commission of the European Communities released *Internet of Things-An action plan for Europe*. This act provides guidance on such legal issues as the right to silence of the chips, information security, standards mandate, and standard authorization, etc. In the same year, the US Congress passed *American Recovery and Reinvestment Act*. The bill specifically states that IoT involves patents and personal privacy. We should analyze the legal problems arising from the development of IoT, and use legal means to promote the development of science and technology.

II. The Challenge of Internet of Things to Citizens' Privacy

The right of privacy is an important right in the private life of citizens, which is closely related to the life and work of citizens. The privacy of citizens in the context of IoT mainly refers to information privacy and scope privacy. Information privacy is about privacy such as personal identity, individual characteristics, and credit status, etc. Scope privacy is the privacy of a person's daily location and surrounding environment. By embedding RFID chips into various commodities and connecting sensors, laser scanners and other information sensing devices, the information privacy and scope privacy of citizens can be easily known by others through IoT technology. Citizens' consumption preferences, credit status, etc., can be easily analyzed and inferred, and their whereabouts can be easily tracked. Once these information is leaked or spread on the Internet, it will have a great impact on citizens' lives and work. In August 2017, police in Zhejiang Province, China, cracked a criminal gang that produced and distributed hacking software for home cameras online. In this case, the suspects cracked nearly ten thousand IP addresses of home cameras and obtained a large number of personal life images, photos and even private personal information. On February 28, 2017, Troy hunt, a security expert, exposed that the user data of the Cloud Pets Teddy Bear, an Internet filled intelligent toy, was stored in a public database without any password or firewall protection. More than two million recordings of children and more than 800,000 email addresses and passwords were exposed.

Therefore, the law should balance the development of technological with the protection of citizens' right of privacy and right to know, and coordinate the relationship between them. The law should be amended in time to stipulate the right to silence of the chips. Citizens can decide whether or not to disconnect the network environment of electronic tags. When selling a product, the retailer should clearly inform the consumer whether an electronic tag is embedded in the product, and make a prompt in writing to ensure that anyone who contacts the product can understand the existence of the electronic tag. After purchasing goods, consumers have the right to decide whether to remove RFID chips to protect their privacy.

RFID chips can be embedded not only in products, but also in the human body. In 2006, a private video surveillance company called CityWatcher.com in Cincinnati, Ohio, USA, implanted electronic chips in the right arm of two voluntary employees. This is the first time that a US company has implanted electronic chips into its employees to identify them. Sweden is the country with the largest use of implanted chips. By the end of 2018, about 4000 people had been implanted with RFID chips in Sweden. When RFID chips are implanted in a patient's body, doctors can read the medical records recorded by the RFID chips through remote servers and conduct real-time health monitoring. It will be of great significance to reduce the public medical costs and realize the sharing of medical resources. But at the same time it will seriously reduce the scope of personal privacy. Once a citizen's medical information is leaked, he may face the risk of unemployment. Because if an employee suffers from a disease that requires high medical expenses, it means that the employee's working ability and position are limited, and the enterprise may have to pay higher insurance premiums or even be rejected by insurance companies. In this regard, California of the United States has enacted laws prohibiting such acts of companies that may damage human rights and privacy. The European Commission intends to develop a new regulatory framework that seeks to balance civil liberties with the risks posed by IoT. China should also pay close attention to the protection of citizens' privacy brought by IoT, and improve its civil laws by drawing on the legislation of other countries,

III. The Challenge of Internet of Things to Patent Law

On February 5, 2013, the State Council issued the *"Guiding Opinions of the State Council on Promoting the Orderly and Healthy Development of the Internet of Things"*. The guidance proposed to strengthen the protection of intellectual property rights, actively carry out intellectual property rights analysis and evaluation of IoT-related technologies, and accelerate the promotion of IoT-related patents. The core technologies of IoT mainly include RFID technology, sensor technology and wireless network technology.

IV. The challenge of RFID technology to patent law

RFID (Radio Frequency Identification) technology is the most critical technology of IoT. The author uses SooPat patent search engine to search and analyze the domestic RFID patents. As of December 31, 2019, 3,615 RFID patents have been authorized in China, including 1,260 invention patents, 2,274 utility model patents, and 81 design patents. Among the authorized RFID patents, invention patents account for 35%, and utility model and design patents account for 65%. Due to the highest innovative requirements of invention patents, it can be inferred that China's innovation ability in RFID technology is at a low level, and there is still a big gap with developed countries. Developed countries attach great importance to the global layout of RFID patents. South Korea's Samsung, which has the highest number of patent applications in the world, and Qualcomm of the United States, which ranks the second, have patent layout in many countries and regions. Patent rights have regional characteristics. If a technology is not patented abroad, it is very easy to have patent disputes in international trade.

V. The Challenges of sensor technology to patent law

Compared with RFID technology, China's sensor technology started earlier and the amount of patent authorization is huge. The author uses SooPat to search and analyze the sensor patents. As of December 31, 2019, 160966 patents have been authorized in China, including 43248 invention patents. The current problem is that the patentee is scattered and the patent conversion rate is low. Chery Automobile Co., Ltd. has the largest number of sensor patents, but only has 280 invention patents. In addition, many universities and research institutes have sensor patents, but most of these patents have not entered the industrial application. The United States, Germany, Japan have mastered a large number of original sensor technologies. Measurement Specialties Inc(MEAS), Honeywell International Inc, Emerson Electric Co., WIKA Group, SIEMENS AG FWB, TDK Electronics AG, YOKOGAWA and Fuji Electric Co., etc., are all leaders in the sensor industry. Their annual production capacity reaches more than tens of millions. Foreign companies or joint ventures have almost monopolized the market for cutting-edge sensors. By contrast, the application range of sensors in China is narrow, and the annual output value of the largest sensor companies is only 55000.

VI. The challenge of wireless access technology to patent law

Wireless access technology is a technology that connects objects and objects with people to realize high-speed data transmission. From the perspective of China's technological development, before 2000, there were few patent applications for wireless access technology, and the period from 2000 to 2010 was a period of slow growth. In 2011, the Ministry of Industry and Information Technology issued the "*12th Five-Year Development Plan of the Internet of Things*". Since then, the applications for wireless access technology patents have increased significantly. The author used SooPat to search for domestic wireless network technology patents. As of December 31, 2019, 10077 patents have been authorized. Among them, there are 7440 invention patents, which accounting for nearly 74%. According to this analysis, in terms of wireless access technology, Chinese companies have strong innovation capabilities. However, it should also be noted that in China, the third and tenth place in sensor patent ownership are foreign companies, respectively Qualcomm and Intel in the United States. Over 30% of the patents of these two companies were applied for and authorized before 2009, and some core patents have become industry standards. Most of China's wireless access technologies are peripheral technologies, and there is still a big gap compared with the core technologies in foreign countries.

From the above analysis, it can be seen that the biggest problem faced by China's IoT industry is the low innovation ability and few core technologies. Once Chinese enterprises adopt foreign patented technology, they will have to pay for intellectual property for a long time and will subject to foreign restrictions. Therefore, China should establish an industry early warning system, pay attention to the patent layout of foreign companies, and avoid the risk of patent infringement. At the same time, it is necessary to promote sound communication between enterprises, avoid technology homogenization, encourage enterprises to carry out technology development and innovation, break foreign technology monopoly, incorporate intellectual property protection and industry standard formulation into national strategy, and attach the use of legal means to protect technological innovation.

VII. The Challenge of Internet of Things to Network Information Security

Internet of things is the internet of everything. In 2018, Gartner's survey report showed that there were 8.4 billion devices connected to IoT in 2017, and the number is expected to reach 14.2 billion in 2019 and 25 billion in 2021. IoT has large equipment base, wide distribution, and high network bandwidth. Once the IoT loophole occurs, a large number of devices will be charged to form a botnet, and a distributed denial-of-service attack will be launched on the network infrastructure, which will cause network congestion and even network paralysis.

In recent years, global cybersecurity incidents have occurred frequently. The information security of IoT is not only related to individual privacy and company operation, but also related to the orderly operation of national economy, social security and even political stability. By using ransomware and IoT, hackers can take over and manipulate IoT devices, control vehicles, cut off power, leak sensitive information, and even stop production lines. On October 21, 2016, Dyn, a US domain name service provider, suffered a DDos attack with 620G traffic from a botnet consisting of tens of thousands of webcams and digital video recorder. The incident led to a large-scale disconnection of the US east coast and hundreds of important websites such as Twitter, Amazon and the Wall Street Journal could not be accessed. In the same year, Deutsche Telekom suffered a network attack. More than 900000 routers In Germany could not be connected to the Internet. This network disconnection accident lasted for several hours and resulted in Deutsche Telekom being unable to provide normal network services to users. Also in the same year, hackers remotely connected to the Ukrainian Power Grid and resulted in power outages for 1.4 million homes. In 2017, the ransomware known as WannaCry shocked the world with its widespread attack. More than 230,000 Windows PCs in 150 countries were infected in one day, and many of them belonging to government agencies and hospitals.

Many IoT devices are manufactured and installed without industry specifications, and there will be more and more loopholes in IoT. When the world is interconnected into a super system, system security will directly threaten national security. In the global cybersecurity market, the United States has a market share of 44.2%, and China has a very small proportion, only 5.9%. The urgent task is to improve China's network information security legislation, strengthen the network security awareness of citizens, enterprises and government departments, reduce the dependence on foreign technology, and ensure the orderly and safe development of IoT.

References

[1]. Guo Min, Zhang Shaobo, Li Xiangdong, Wang Guojun, "Research on Location Privacy Technology in IoT", Journal of Chinese Computer Systems, Vol.38, pp1961-1965, Sep2017.

[2]. Yang Jie, Zhuang Chunsheng, Zhang Hongmin "Research on Internet Information Security and Privacy Protection", Digital Technology and Application, Vol.32, pp196-197, Dec2017.

[3]. Ding Xiaodong, "Personal Information Legislation in the Age of Big Data and Artificial Intelligence: Challenges of New Technology to Information Privacy", Journal of Beijing University of Aeronautics and Astronautics(Social Sciences Edition), Vol.33, pp8-16, May2020.

[4]. Yu Yangjian, "Internet of Things Device's Own Flaws Challenge Privacy Security", Wireless Internet Technology, Vol.39, pp27-28, Jan2019.

[5]. Zhou Taoyi, "Protection against Location Privacy of Users on Internet of Things Based on Anonymous Trajectory and Time Obfuscation Technology", Journal of Shandong Agricultural University(Natural Sciences Edition), Vol.50, pp270-273, Feb2019.

[6]. Feng Shiduo, Cao Heng, Gao Jingjie, "The Trend of IoT Equipments Safety Supervision and its Enlightment from the 'SB-327 Information Privacy: Connected Devices'", Information and Communications Technology and Policy, vol.26, pp. 78-80, Jul 2019.

[7]. Du Xiaojiang, Wu Longfei, "Towards Smart Home Security and Privacy: a Survey ", Journal of Guangzhou University(Natural Sciences Edition) , vol.18, pp.40-51, Jun2019.