DOI 10.15302/J-SSCAE-2016.06.007

The Obligation of Decryption Assistance by the Internet Service Providers: Suggestions on the Amendment of Article 27 of the Cybersecurity Law (the Second Review of Draft)

Cui Congcong[1], Li Yuxiao[2], Han Song[1]

1. Institute of Internet Governance and Law, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Cyber Security Association of China, Beijing 100010, China

Abstract: The obligation of decryption assistance by the Internet service providers reflects the conflict between public powers (such as investigatory power) and private rights (such as the right of communication privacy and the right of privacy). Data under encryption by users should be gathered by the Internet service providers on the basis of the principle of controllability and traceability, the principle of proportionality, and the principle of necessity. Providers should fulfill the obligations of decryption assistance supervised by strict procedure. Thus, the overall utility of social governance control, the tranquility of private life, and the business interests of Internet service providers can be maximized. Severe violations of private rights and disorderly situations due to governmental failure can be avoided if these suggestions are carried out.
Keywords: obligation of decryption assistance; principle of necessity; principle of proportionality; principle of controllability and traceability; remedy measures

1 Introduction

Crime is becoming more international, organized, covert, and high-tech in this Internet age. In recent years, encryption and storage technologies of communication have been used by terrorists to disseminate fear of violence, accept foreign command, and plot terrorist attacks, thus becoming a severe threat to national security and public safety. Widely used cryptographic techniques objectively obstruct judicial criminal investigations. Thus, the use of cryptographic techniques makes a lot of legal cases of endangering national security and public safety difficult to be found, deterred, and punished in time. For the purposes of safeguarding national security, maintaining social order, and so on, during the investigation of criminal cases, investigatory organizations have sometimes had to ask Internet service providers to facilitate their access to personal information in an encrypted national. It is necessary for the law to demonstrate the boundaries of Internet service providers' obligation to assist law enforcement.

2 Apple Inc. versus the FBI: conflicts in decryption assistance

2.1 Focus of controversy and the results

Conflicts between the use of technology and the needs of law enforcement have been continual since the initial development of cryptographic techniques [1]. The original intention behind

Received date: 12 October 2016; **revised date:** 18 October 2016
Corresponding author: Cui Congcong, Beijing University of Posts and Telecommunications, Associate Professor. Major research field is cyber law. E-mail: cuicongcong@bupt.edu.cn.
Funding Program: CAE Major Advisory Project "Research on Cyberspace Security Strategy " (2015-ZD-10)
Chinese version: Strategic Study of CAE 2016, 18 (6): 034–038
Cited item: Cui Congcong et al. The Obligation of Decryption Assistance by the Internet Service Providers: Suggestions on the Amendment of Article 27 of the Cybersecurity Law Draft (Second Review Draft). *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.007

using cryptographic techniques was to achieve confidentiality of information, thus providing technical support for citizens' right of communication privacy. However, offenders can also use cryptographic techniques to conceal facts and evidence regarding crimes, so it is a continuous and unavoidable problem. On February 16, 2016, the Federal Bureau of Investigation (FBI) acquired a search warrant issued by the court of California requiring Apple Inc. to assist law enforcement agencies in investigating an iPhone that had been seized in the Syed Rizwan Farook assault case in San Bernardino. Apple CEO Tim Cook refused the order that the FBI had asked Apple Inc. to build a "backdoor" in the iPhone, and responded publicly the next day. In his statement, Cook said: "we fear that this demand would undermine the very freedoms and liberty our government is meant to protect;" he believed that the FBI's request would threaten users' information security. On February 28, the New York District Court accepted Apple Inc.'s lawsuit. Judge James Orenstein believed that the US government's interpretation of the All Writs Act is too broad, and that this practice is contrary to the spirit of the US Constitution. On March 7, the US Department of Justice requested the judge to withdraw previous judgment and ordered Apple Inc. to assist with decryption. On March 22, the FBI decrypted the iPhone with the help of the Israeli company Cellebrite.

In this case, since the suspects were gunned down by police, the police investigation was facing a dead end. Compared with a situation that telecom operators were requested to provide users' text messages that were stored in the operators' servers to law enforcement agencies, in this case, the Internet service provider's obligation to assist law enforcement is extended to decrypt the encrypted users' information, and to take the initiative to break the user agreement regarding decryption. This situation will undoubtedly lead to user concerns regarding personal privacy and information security. In fact, both sets of acts—the All Writs Act that was cited by the FBI and the Second and Fifth Amendment of the US Constitution that were cited by Apple Inc.—are the law of the industrial age. The FBI requires Internet service providers to assist law enforcement, and these obligations extend to decrypting and providing users' files. However, the information provided cannot simply be a metaphor for physical folders or safes [2]. If the current situation regarding the obligation of Internet service providers to assist law enforcement remains, for pragmatic purposes regarding general provisions, Internet service providers will be forced to provide whatever investigative powers require. This situation will soon be out of control. Without procedural safeguards, law enforcement agencies and Internet service providers can easily abuse their power and violate personal privacy and personal information security.

2.2 Conflict between the powers and rights involved in decryption assistance

Criminal investigations related to safeguarding national security and combating terrorism have always involved intense collision between national powers and individual rights [3]. Decryption assistance that relies on the Internet service providers is a nation's essential method to punish crimes and maintain social order, and is an inevitable choice between protecting individual freedom and controlling crime for the common good. However, it is undeniable that decryption assistance results in obvious tension between national powers and the freedom of business, protection of personal dignity, personal freedom of communication, and other individual fundamental interests. Seen from the surface, Apple Inc.'s motivation in declining the FBI's requirement about decryption assistance is to protect its commercial interests. However, hidden beneath the surface are other interests regarding the "medium" of conflict between public power and private rights. These hidden interests are a value judgment that is based on a comprehensive consideration of the interests of and impacts on all parties involved. Although decryption assistance is an effective method of preventing and controlling crime, it can easily violate individual rights and have spillover effects. Thus, it is not easy to find a balancing point—That is, it is becoming increasingly difficult to find the right balance between the legitimate needs of law enforcement, and the freedom of business and personal privacy.

3 China's legislation and judicial practice

3.1 Legislation

Law enforcement assistance is an important part of the Internet service providers' obligation to ensure the cyberspace security. As problems with online investigations and evidence accumulate, Internet service providers, as the important participants in network activities, should actively perform their duties to assist law enforcement. This duty requires Internet service providers to devote effort to law enforcement in the form of necessary assistance and technical support. This duty also includes communication monitoring, reasonable interception, decryption assistance, and so forth. Furthermore, Internet service providers must keep the information they seek during law enforcement assistance secret for reasons of information security [4].

Article 77 in the National Security Law of the People's Republic of China requires citizens and organizations to perform their obligations regarding safeguarding national security and to provide necessary support and assistance to national security agencies, public security organizations, and the relevant military agencies. Article 18 in the Counterterrorism Law of the People's Republic of China requires telecommunication business operators and Internet service providers to provide technical interfaces and decryption, and other technical support and assistance for the prevention and investigation of terrorist activities as conducted by public security organizations and national

security agencies in accordance with the law. However, the present law makes no provision for decryption assistance to be applied in other criminal cases. Article 27 of the Cybersecurity Law of the People's Republic of China (the Second Review of Draft) requires network operators to provide technical support and assistance for the protection of national security and for the investigation of criminal activities conducted by public security organizations and national security agencies in accordance with the law. It is a vital problem to ascertain the content and legal procedure for law enforcement assistance. However, there are no clearly stipulations on the range and procedural safeguards of technical support and assistance, as well as the remedy measures of citizens' rights in the Cybersecurity Law of the People's Republic of China (the Second Review of Draft).

3.2 Judicial practice

Compared with American investigations operating under the restrictions of court writ, China's legislation makes the boundary of public power unclear and relies too heavily on judiciary authorities' self-discipline. The current problems are that the judiciary authorities have requested law enforcement assistance too frequently, and that required conditions for law enforcement assistance are too loose. In addition, it is common for the judiciary authorities to require telecommunications business operators to provide criminal suspects' calls and short messaging service (SMS) records [5]. Based on the outdated principle of visible investigation regarding the sending of plain-text messages [6], the judiciary authorities had the power to obtain information for relevant cases directly from the servers of the Internet service providers. Now, most means of telecommunication and Internet use include measures to send messages as ciphered text. As a result, Internet service providers must decrypt users' information in order to meet the requirements of the national authorities.

4 Suggestions for the amendment of Article 27 of the Cybersecurity Law of the People's Republic of China (the Second Review of Draft)

In prosecuting crime, countries that require Internet service providers to assist with decryption will violate and restrict the personal right of privacy. Although individuals should have a certain degree of tolerance for such situations, it does not follow that the national power in a technical investigation should be unrestricted. For special investigatory measures that are directly related to human rights, the internationally common practice is to prevent the unlimited expansion and abuse of power through legal control. To fulfill this aim, Article 27 of the Cybersecurity Law of the People's Republic of China (the Second Review of Draft) should define the applicable case types, applicable premise, and applicable objects of decryption-assistance measures.

4.1 Applicable case types

Personal rights include all relevant rights, such as the right of privacy and personal information control, and the right of communication privacy. Based on the requirement to protect the basic rights of citizens, the applicable scope of cases that can legally request decryption-assistance measures is limited to major criminal cases, including the crime of endangering national security, terrorist crimes, mafia-organized crimes, serious drug-related crimes, serious crimes of corruption and bribery, as well as the major criminal cases involving serious violation of citizens' rights by using their functions and powers, cases of hunting wanted criminals, cases involving fugitive suspects or defendants, and other criminal cases involving serious harm to society that may result in sentencing of 10 years imprisonment, life imprisonment, or the death penalty. The category of "serious crimes" reflects the importance of the violated right; for the crimes described above, requiring Internet service providers to provide decryption assistance is important enough to offset the negative impact of the resulting violation of the right to privacy, right of communication privacy, and the freedom of business. Because crimes of bribery are often hidden, an investigation using only general investigatory measures often has little effect. If we do not permit Internet service providers to assist in decryption, it will be difficult for law enforcement agencies to find such crimes, or to investigate and punish offenders.

4.2 Applicable premise

Assisted decryption must be excluded from general investigatory measures. It could not be applied until common investigatory measures fail or other measures may require a great deal of manpower, material resources, and time and may cause great damage to personal rights and public interests. Another meaning of the principle of necessity is that only when judicial agencies have a high degree of reasonable doubt about individual behavior that may cause serious social harm can they require Internet service providers to assist in decryption; that is, if there is substantial evidence that individual behavior would cause a considerable level of social harm, the judicial agencies can be able to ask a Internet service provider to provide decryption assistance in a particular case. In this situation, the investigatory power can take a higher priority over the personal right of privacy and the right of communication privacy, thereby making the authorized decryption assistance legal.

4.3 Applicable objects

In decryption-assistance process, the information that the authorities want to obtain mainly falls into the following two categories: ① the identity information of criminal suspects, and ② the communication content of criminal suspects. If decryp-

tion assistance is made specific to a suspect, it is bound to lead to cases in which a lack of a suspect's identity information results in legal enforcement agencies being unable to ask Internet service providers to provide decryption assistance. However, if there is no limit on applicable objects, the investigatory organizations will have too sufficient motivation and power to obtain information from the Internet service providers, with the intention of screening out the objective evidence from the mass of information provided. In consideration of the relationship between efficiency of investigation and protection of human rights, we believe that the applicable objects of decryption assistance should be clear and limited, and should be directly related to specific communication lines and/or electronic equipment; however, the identity of the object does not need to be fully clear [7]. In addition, decryption assistance, as a supplementary investigatory measure, can only be applied upon individuals that are closely related to the very suspect of the crime in the case of necessity.

Thus, Article 27 should be amended so that it requires Internet service providers to provide necessary technical support and assistance to the public security organizations and the national security agencies in order to safeguard national security and detect major crimes according to the law.

5 Security measures and remedy measures

From the legislative point of view, the Cybersecurity Law of the People's Republic of China should be the basic law of cyberspace security, with decryption assistance as only a small component. Security measures and remedy measures in the process of decryption assistance should be regulated in the implementation details.

5.1 Security measures

Decryption assistance not only comes down to the privacy of the parties involved, it may also involve business secrets or national secrets. Thus, investigators and Internet service providers who lay hands on national secrets, commercial secrets, and personal privacy in the process of an investigation must act in a strictly confidential manner, and must not disclose or sell information, or make it illegally available to others. They must destroy material that is unrelated to the case in a timely fashion. To avoid affecting the detection and investigation of cases, Internet service providers must assist with maintaining confidentiality during decryption, and they are not allowed to inform the user during the investigation, without the law enforcement agencies' approval.

5.2 Remedy measures

5.2.1 The remedy for Internet service providers

Although Internet service providers have an obligation to assist with decryption, they also have the right to appeal to the law enforcement agencies or their higher authorities, so that they can protect their rights and interests. In addition, the decryption-assistance process may carry costs, which Internet service providers can ask for compensation from law enforcement agencies. Of course, such costs must be reasonable and directly related to the decryption-assistance activities.

5.2.2 The remedy for interested parties

Remedies for interested parties are mainly to protect their rights, including the right to know, objection right, and right to claim damage compensation. First, after a decryption-assistance activity, the law enforcement agencies should inform interested parties about the decryption-assistance situation. This will allow the interested parties to check whether or not the situation corresponds with reality, so that they can raise an objection or apply to exclude illegal evidence. Second, if interested parties consider that the decryption-assistance activity is illegal, or that decryption-assistance measures violate the principles of necessity and proportionality, they can apply to law enforcement agencies for reconsideration. Furthermore, interested parties can apply for national compensation if their legal rights have been damaged in a case of illegal decryption assistance.

6 Conclusions

Internet service providers always face a dilemma when they assist with decryption: the "practical necessity" of national security protection and the maintenance of public interests versus the "practical risk" of threatening citizens' rights of privacy and the freedom of business. In cases where law enforcement agencies lack the ability to decrypt, ordering Internet service providers to assist with decryption is a relatively low-cost method. To minimize the spillover effect, relevant legislation must clearly state applicable case types, applicable objects, and applicable principles, and must define the security measures that are necessary to empower interested parties the rights, including their rights to know, rights of appeal, and rights to apply for national compensation. The legislation must strictly limit applications in substantive and procedural aspects to make citizens have ability to predicate national policy, thereby ensuring a dynamic balance between crime control and human rights protection for criminal investigation activities.

References

[1] Ma M H, Guo Y, Ma N. Legal Issues regarding the self-decryption obligation and its application in China [J]. Journal of Soochow University (Philosophy & Social Science Edition), 2016 (1): 89–94. Chinese.

[2] Kiok J. Missing the metaphor: Compulsory decryption and the fifth amendment [J]. Boston University Public Interest Law Journal, 2015, 24 (1): 53–79.

[3] Xie D K. On the protection of right of privacy in technical investigation [J]. Legal Forum, 2016, 31 (3): 32–40. Chinese.

[4] Huo Y K, Feng X S. The analysis of network operators' safety guarantee obligation based on the theory of the social role [J]. Journal of Xi'an Jiaotong University (Social Sciences), 2016, 36 (1): 62–68. Chinese.

[5] Tang Z M. Two issues of the freedom of correspondence and protection of correspondence secrets [J]. Law Science, 2007 (12): 13–17. Chinese.

[6] Gao R L. Unlicensed search and evidence exclusion rule of electronic data evidence in the USA [J]. Journal of Shanghai University of Political Science & Law (The Rule of Law Forum), 2015, 30 (5): 72–81. Chinese.

[7] Hu M. Technical detection by procedure regulation in United Kingdom, France, Germany, Netherlands and Italy [J]. Global Law Review, 2013 (4): 6–18. Chinese.