2017 2(2) 8-11 Submission: 2017/11/30, Peer review: 2017/12/10, Accepted: 2017/12/25, Published: 2017/12/30

International journal of terrorism & national security

Publication state: Japan
ISSN: 2423-8376

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: camus200@naver.com

Peer reviewer
E-mail: terrorismstudies@naver.com

http://dx.doi.org/10.22471/terrorism.2017.2.2.08

Comparative Study of Communication Restrictions on Crime of TERRORISM

Lim Yoo-seok

Gunsan University, Gunsan, Republic of Korea

Abstract

In recent years, the world has been emphasizing the role of intelligence agencies in the field of telecommunications aimed at strengthening the response to acts that threaten national security, such as the threat of international terrorism.

In particular, crimes against national security such as espionage or terrorism are committed by the criminals who have been trained outside domestic territory, observing their own strict security regulations. For these reasons, investigations on communications conducted by criminals who attempt and direct is essential to investigation crime against national security.

Considering legislations on telecommunication restrictions in some advanced countries, the United Kingdoms has enacted the Investigatory Powers Act(IPA 2016) to counter threats to national security and serious crimes, allowing investigative agencies, security and intelligence agencies to monitor a large scale of surveillance.

The United States has implemented the CALEA, the Patriot Act, the FISA, and the ECPA, which are legally enforced by law.

It is necessary to revise the important part of the domestic communication confidentiality protection law against the crimes which threatens the national security by referring to the matters concerning the communication restriction law of major countries.

In the context of IoT communication, individuals, society, and the nation are linked to one fate community through the transmission and reception of packet data over the Internet. Also, telecommunications infrastructures are subject to territorial domination as tangible goods, it is necessary to understand national security as "the safekeeping of the nation as a whole".

[Keywords] ***National Security, Terrorism, Investigations in Telecommunication, Investigatory Agency, Intelligence Agency***

1. Introduction

Recently, criminals are becoming more advanced and intelligent due to the development of information and communication science and technology. In particular, crimes against national security such as espionage or terrorism are committed by the criminals who have been trained outside domestic territory, observing their own strict security regulations. In addition, the methods of crime by taking advantage of advanced science and telecommunication technology have been rapidly developed.

On the other hand, the collection of legitimate evidence by investigative agencies is becoming increasingly difficult, but investigations on communications conducted by criminals who attempt and direct is essential to investigation crime against national security.

It is also important in terms of protection of personal information in domestic laws and regulations. Furthermore, it provides the basis of legitimate and proper investigation on communication to ensure national security and public safety by intelligence and investigation agencies.

Hereinafter, the legal system for proactive and preventive measures against transnational crime threatening national security will be discussed. To this end, this article will compare relevant legal system in the United Kingdoms and the United States and suggest the recommendations for amendment of law on communication restrictions.

2. Review on Comparative Law

2.1. United kingdoms

The United Kingdoms enacted the Investigatory Powers Act 2016, which allows a large-scale surveillance on communications by investigative agencies, security and intelligence agencies to counter threats to national security and major crimes[1], and the Queen expressed her consent to enact the law as of November 29th, 2016[2]. Moreover, the Act became in force by various dates starting on December 30th, 2016[3], establishing and restricting the electronic surveillance powers by the intelligence community in the UK, such as law enforcement agencies and police. It has also influenced data related national security, and technical communications. In addition to this, it has introduced new supervisory systems for managing the use of investigatory powers by law enforcement agencies, security and intelligence agencies and its monitoring, and for strengthening its safeguard in the United Kingdoms.

IPA 2016 provides investigation authorities, security and intelligence agencies with legal right to retain all the information on the telecommunication history, such as infiltration into computers, smart phones, tablets, storage devices, and so forth, to enhance the investigatory powers by the national agencies. It provides legal safeguards to define its scope of power as well.

Still, the law raised some issues in the course of legislation by the Parliament. It was because of the broad authority that technology and telecommunications operators in the UK and abroad provide with governmental agencies to keep their personal information. The authority is regulated in relation to bulk warrant allowing the request for potential support the law enforcement agencies in the United Kingdoms as a form of close access to telecommunication[4].

2.2. United states

Along with European countries, the United States has four major laws relating to legitimate interception: the Communications Assistance for Law Enforcement(CALEA), the PATRIOT Act of 2001, Foreign Intelligence Surveillance Act(FISA, 1978) and the Electronic Communications Privacy Act(ECPA). The Foreign Intelligence Surveillance Act is a legislation that considers that the object of surveillance and interception could be foreigner(s) who does not hold American citizenship. In 1994, the US Congress clarified CALEA more clearly, requiring operators to maintain a network infrastructure for legitimate eavesdropping bodies based on law. In particular, after the September 11 terrorist attacks, Congress increased its electronic surveillance by the PATRIOT Act. This law extends FISA, which was already implemented for surveillance on foreign citizen[5].

The Telecommunications Privacy Act(ECPA) distinguishes the definition of communication interception in the following three categories: (i) wire communications through the telephone line as an auditory transmission related to a conversation involving human upbringing; (ii) oral communications where one party of the conversation does not intend to interfere; (iii) electronic communications that transmit all or part of symbols, signals, and visual material, excluding telephone calls and voice conversations, by using telephone lines, radio waves, or other media[6].

Interception of national security crimes is permitted by the Foreign Intelligence Surveillance Act(FISA). The object to be audited by FISA is related to overseas information activities: i) the content of the communication is foreign confidential information, ii) the application for interception shall be filed with the Foreign Intelligence Surveillance Court(FISC), a special court established by FISA.

The Law on mutual legal assistance(CALEA) is a complement to ECPA and FISA for effective interception. Under the Act, a telecommunications operator shall have telecommunications facilities and equipment capable of intercepting the subscriber's communications within the scope of the provision of services and providing the information to the information and investigation agencies pursuant to a court order or related regulation. If a telecommunication operator or manufacturer does not have the necessary equipment for interception or does not provide interception services, the court may order the establishment of eavesdropping facilities and provide the communication contents in accordance with the Act. The telecommunication operator shall provide the investigation agency with a communication history of the alleged offender by the court.

3. Suggestions for Revision of Domestic Telecommunication Protection Act

3.1. Necessity and legitimacy of the Internet interception

If the conventional communication means is aimed at voice conversation via a telephone line, contemporary communication means is not limited to voice by means of the Internet, but is converted into digital data such as letters, pictures, expressions and commands for various electronic devices including various websites. All possible information is targeted. In addition, since these digital data transmitted and received on a packet-by-packet basis are easily distinguished from the evidence of crime in the real space because of the infinite copying, modification and deletion, it is possible to prevent the crime by capturing the crime in advance[7].

3.2. Provisions of exceptional grounds for wiretapping against national security threat crimes

The Internet line data is not only easy to deleted, changed, and encrypted, but also makes it difficult to detect if the dark web is used. Even if it detects, it cannot be expected to prevent damage. Especially, it is obvious that there is a need to provide an exception clause for the Internet wiretapping.

3.3. Base station investigation through tracking location information

Base station investigations that identify location information are a necessary investigation method for tracking offenders of specific crimes or other crimes that threaten national security. In many cases, the communication confirmation data is used at the early stage of the intervention or investigation and it is often difficult to specify the person 's personal information. It is necessary to re-investigate the personal information of the subscriber(s) separately before requesting the communication confirmation data, and if the result of the investigation cannot be grasped, the investigation cannot proceed any longer. Therefore, considering the risks and urgency of crimes that threaten national security, base station investigation that grasps real - time location information is an area that is actively necessary for suppressing the crime.

4. Conclusions

It is not arguable that public interest and crime prevention are traditionally regarded as critical issues. In order to strengthen the response to acts threatening national security, such as threats of international terrorism or provocations by North Korea, information on communications held by telecommunications providers is essential to in-

vestigative agencies or intelligence agencies[8]. In addition, there may be various discussions on the concept of national security or national security.

However, in the context of IoT communication, individuals, society, and the nation are linked to one fate community through the transmission and reception of packet data over the Internet. Also, telecommunications infrastructures are subject to territorial domination as tangible goods, it is necessary to understand national security as "the safekeeping of the nation as a whole".

Author
Lim Yoo-seok / Gunsan University Professor
B.A. Dongguk University
M.A. Dongguk University
Ph.D. Dongguk University

Research field
- Implication and Role of Intelligence for Counterterrorism Activity in U.S.A, Korean Journal of Public Security Administration, 10(3) (2013).
- The Role of Maritime Police for Maritime Sovereignty, Review on Police Administration, 11(2) (2016).

Major career
- 2008~present. Korean Association of Terrorism Studies, Board Member.
- 2015~present. Korean Association of Security and Criminal Law, Board Member.

5. References

5.1. Journal articles

[7] Jung JH. Legal Study on the Necessity and Legitimacy of the Interception of Packets Over Internet Communication. *Hong-Ick Law Review*, 18(1), 505-529 (2017).
[8] Choi CS. The United States Legislation for Investigative and Information Authorities Right to Collect Information on Use of Telecommunications and the Implications - Focused on Review of the USA Freedom Act of 2015. *Informedia Law Review*, 20(1), 113-140 (2016).

5.3. Additional references

[1] httt://www.computerweekly.com (2016).
[2] Alan Travis Home Affairs. "'Snooper's charter' Bill becomes Law, Extending UK State Surveillance". The Guardian. Retrieved (2016).
[3] Investigatory Powers Act goes into Force, Putting UK Citizens under Intense New Spying Regime Published by The Independent (2016).
[4] https://www.mi5.gov.uk (2017).
[5] Cable Television Laboratories: Packet Cable Electronic Surveillance Specification, PKT-SP-ES-DCI-101-060914 (2006).
[6] U.S. v. Herring, 993 F.2d 784, 787 (1993).