Website blocking as Legal Measures to control Online Gambling: A comparative analysis of Thai, U.S. and Singapore laws

Kanathip Thongraweewong[1]

Abstract

In Thailand, gambling is generally prohibited by the specific law, The Gambling Act, but this law does not stipulate clearly and comprehensively on the measure to control online gambling especially technical measures such as website blocking. However, computer crime Act B.E. 2560 provides certain mechanisms that can be applied to block online gambling websites such as notice takedown in section 15 and blocking from court order in section 20. Nevertheless, those principles still have limitations in scope and elements as well as interpretation problems in application to online gambling websites This research will conduct comparative analysis of website blocking measures in Thai laws with foreign laws, i.e. Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) of the U.S., Remote Gambling Act 2014 (RGA) of Singapore. In addition, the negative impact of these measures, both technical and legal aspects such as freedom of expression will be discussed.

Keywords: Website blocking, Computer law, Online gambling law, Freedom of expression, Cybercrime law.

[1]Associate Professor of law, Director of Digital law Institute
KasamBunditUniversity 1761 Patanakarn Road, SuanLuang, Bangkok 10250
E-mail: kanathip@yahoo.com

Introduction

The regulations of online gambling vary from country to country. In some countries, online gambling is legal while it is illegal in some certain countries (Nikkinen, 2014). The main reason for prohibiting online gambling is to protect children from health related problems (Messerlian et al, 2005). In Thailand, gambling is generally prohibited by specific law, The Gambling Act, but this law does not cover website blocking. However, computer crime Act B.E. 2560 as recently amended provides certain mechanisms that can be applied to block online gambling websites. This paper will examine this Act especially section 20. Then, comparative analysis of Thai and selected foreign laws, i.e. the U.S. and Singapore, will be conducted. The negative impact of those laws on several aspects including the overclocking problem will consequently be discussed.

Thai Laws relating to blocking website

The relevant laws can be classified in to period, i.e. prior to and after the revised version of the Computer related crime Act B.E. 2560.

1. The legal status of website blocking prior to the amendment of Computer related crime Act in B.E. 2560

There have been no laws authorizing website blocking until the computer related crime Act of B.E. 2550 came into force in B.E. 2550 with section 20 provides officials the power to ask Court order for blocking websites. However, the reasons for website blocking were restricted to websites relating to computer related crimes as stipulated in this Act, for example, blocking of websites containing “illegal content” according to section 14 which includes pornographic material, false or fake information, information affecting national security, terroristic content. Nevertheless, “online gambling” is not listed as a computer related crimes in this Act, though it is an offence of another law, i.e. The Gambling Act B.E. 2478. The Ministry of ICT asked the council of state for legal opinion of this issue in B.E. 2556. The council of state delivered an opinion that section 20 of the computer related crime Act provides

no legal basis for blocking websites relating to online gambling because there are no provisions in this Act that criminalizes gambling (Council of State, legal opinion no. 1024/2556). Although the operators and player of online gambling sites may be punished by the Gambling Act, this Act does not have rules on website blocking. In addition, computer related crime Act, the only law relating to website blocking, cannot be applied for gambling related content.

2. The legal status of website blocking after the amendment of Computer related crime Act in B.E. 2560

Recently, The Gambling Act B.E. 2478 has not been amended, providing no legal basis for website blocking. Although the amended Act does not established specific rules relating to online gambling, this paper found 3 areas of this law which can be applied to online gambling as follows;

Area 1: Criminalizes online gambling as illegal content

The content related offences of section 14 comprise subsection (1)–(4). Firstly, section 14 (1) main's element is "input the false, forged or distortive computer data into system with fraudulent intention or bad faith in a manner that could lead to the damage of people". Secondly, section 14 (2) and (3) cover the input of content affecting national security, terroristic content. Then, section 14 (4) punishes the input of pornographic material. Thus, the scope of "illegal content" as described in (1)-(4) does not cover "online gambling" even the case of online gambling which is contrary to the Gambling Act is not deemed to be illegal content according to section 14. However, certain situation of online gambling can be included in a scope of illegal content of this section, e.g. online website that deceives player or provides advertisement containing pornographic content.

Area 2: Notice and takedown mechanism

According to section 15 as amended by the Act version B.E. 2560, service provider could assumes liability if users input illegal content as described in section 14 to the system under the control of such provider. This section

then establishes exception of liability if service provider set up a "notice and takedown mechanism" by taking down illegal content after receiving complaint from user or other person. Nevertheless, the liability of service provider depends on the type of content which should be deemed illegal under section 14. Thus, this mechanism may not cover online gambling. However, this paper indicates that service provider may choose to include online gambling in the scope of their notice and takedown policy on voluntary basis due to the fact that the mechanism under section 15 is merely minimum requirement and does not prohibit service provider who choose to filter content in a broader scope.

Area 3: The blocking websites mechanism

The main rule on website blocking is established by section 20 which can be applied in case of online gambling in several possible ways as follows;

- The blocking order of section 20 (3) which includes illegal content according to other law relating to public order and moral that criminalizes such content. Consequently, online gambling that is a crime by the Gambling Act will fall into this scope leading to the issue of blocking order of websites providing access to such content. However, the Gambling Act does not provide general definition of gambling. This act criminalizes certain gambling types as stated in prohibited lists. Thus, gambling types not included in the list are not a crime resulting in the unapplicable of section 20 (3) to websites containing such gambling.

- The blocking order of section 20 paragraph 2 which includes content against public order and good moral despite the fact that such content is not a crime by any other laws. The scope of this type of bookable content is broad depending on a filtering committee established by this section who has authority to apply for blocking order from court.

Comparative analysis of website blocking law of Thai and the U.S.

In general, Gambling is legal under the federal law with certain restrictions of state laws which varies from state to state. However, federal law regulates

online gambling in certain aspects such as the Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) prohibits gambling businesses from knowingly accepting payments in connection with the participation of another person in a bet or wager that involves the use of the Internet and that is unlawful under any federal or state law (31 U.S.C. §§ 5361–5367). It provides certain exceptions such as legal intrastate gaming and does not cover state lotteries (Monkcom et al, 2017).

In a landmark case of enforcing UIGEA, the Department of Justice seized the domain name of three online gambling sites and the operator of those sites were prosecuted for violating UIGEA by engaging in financial transfer process to and from their customer (United States v. Scheinberg, 10 Cr. 336, 2011). due to the fact that financing illegal gambling is a federal crime (18 U.S.C. section 1955). Also, accepting credit, electronic fund transfers in connection with the unlawful internet gambling is also federal crime (31 U.S.C., section 5363, 5366). Thus, properties including domain names used in violation of 18 U.S.C. section 1955 or involved in money laundering transaction, are subject to forfeiture to the U.S. (18 U.S.C., section 981 & 1955 (d)).

Contrary to Computer crime Act of Thailand which has specific provision for website blocking, the UIGEA does not have provision and process enacted specifically for blocking online gambling sites. The main function of this law is to block financial transaction by prohibiting relevant businesses such as gambling provider from receiving money or financial institution from processing money transaction. As for the above mentioned case, it is a domain name seizure which is based on other law, not provision in UIGEA itself. Moreover, the practice of defendant involves the violation of money-laundering law which is another specific offence (Leslie, 2014). In addition, the relevant laws does not establish detailed process of website blocking. Thus, the paper will examine Singapore law which provides detailed rules on website blocking as part of gambling law.

Comparative analysis of website blocking law of Thai and Singapore

Remote Gambling Act 2014 (RGA) of Singapore provides specific rules relating to website blocking for illegal gambling which can be compared to section 20 of the Computer related crime Act of Thailand in following aspects;

- Basis of law for website blocking: Although Singapore enacts specific law of computer crime (Computer Misuse and Cybersecurity Act), this law does not establish website blocking mechanism. However, website blocking is included in Section 20 of Remote Gambling Act 2014. On the contrary, Gambling law of Thailand does not have rules on website blocking. The single law relating to this mechanism is section 20 of computer related crime Act.

Causes for website blocking order: Singapore law identifies specific causes for website blocking order by limiting the application of blocking order to the websites or services of ISP being used to access to an online location through which a remote gambling service is provided in contravention of the Act or online location containing an invitation to young persons to gamble, or containing material promoting remote gambling in violation of this law. Thus, the cause or the scope of blocking order is limited to illegal gambling related content. Unlike Singapore law, the scope of "illegal content" which can be blocked under section 20 of Thai law is broader including fake or false information, computer fraud, information affecting national security, content affecting "public order and good morals" (Section 14 and section 20).

Definition of Website blocking: Contrary to Singapore law which defines "access blocking order" as an order to disable access to an online location, section 20 of Thai law only states "order to suppress or erase computer data". However, ministerial regulation explains the suppression order is to disable access to online location such as IP address, URLs, domain name.

Regulating authority: Website blocking for online blocking in Singapore involves collaboration of several agencies, i.e. the Gambling Regulatory Unit (GRU) (under the Ministry of interior), The Info-communications Media

Development Authority or IMDA (under the Ministry of Communications and Information). Finally, IMDA has power to issue access blocking order. As for Thai laws, Ministry of Digital Economy and Society (MDES) and Technology crime suppression division of the Royal Thai Police are collaborating in the enforcement process but the final order from Court is needed.

Website blocking order: Contrary to Singapore where administrative authority (IMDA) has power to order, the final blocking order under Thai law is under the discretion of Court. Thus, administrative agency shall not have power to order website blocking. Both laws share certain similarities in that the request for the final order is initiated by authorized official after received of complaint or by their own initiative.

Person or Entity that executes blocking order: Contrary to blocking order of Singapore which obliges Internet Service Provider (ISP) to block websites, either service provider which includes "ISP" or officials could execute blocking order since section 20 authorizes official to decide whether to execute court order by himself or requests service provider to execute.

ISP obligation: Similar to Singapore law, Thai ISP has obligation to block websites in case the order is issued. However, the definition of ISP in Singapore law is more limited since it excludes person who provides Internet services to that person's own employees for use solely within that person's firm or corporation while the definition of ISP in Computer related crime Act does not have such limitation. In addition, obliged person under Thai law is broader because the definition of "service provider" includes not only ISP but other person or entity that collects and maintains computer data for user, e.g. social media provider.

Negative impact of Website blocking and the safeguard principles

This part will discuss the negative impact of website blocking law in two main aspects as follows;

Firstly, with regard to technical aspect, website blocking could threaten the fundamental principle of interconnectivity. Court-ordered removal

or replacement of entries from the series of interlocking databases that reside in domain name servers and domain name registries around the globe undermines the principle of domain name universality—the principle that all domain name servers, wherever they may be located across the network, will return the same answer when queried with respect to the Internet address of any specific domain name. In addition, mandated court-ordered DNS filtering will also have potentially catastrophic consequences for DNS stability and security (Lemley et al, 2011). Furthermore, website could affect the principle of network neutrality which require treatment of all data on the Internet the same, and not discriminate by user, content, website (Belli and Foditsch, 2016). Regarding the efficiency, this measure is easily bypassed by using VPN or Proxy (Caliskan, 2017).

Secondly, website blocking could have an impact on freedom of expression which is one of the important human rights (Human Rights Watch, 2005). This measure can be classified as internet censorship (Schell, 2014). In addition, due to the fact that illegal content can be located in association with other content in an online location, there is an opportunity for the "overblocking" which affects lawful content. For example, advertisement about illegal gambling is at one page of a webpage (online location if this particular content is described in URLs as "http://www.richrich.com/content/5894699", if the blocking order covers the broad location as a whole in URLs: http://www.richrich.com, this blocking order would affect other pages of this webpage.

Negative impact of Website blocking and the safeguard principles

Considering the negative impact discussed above, website blocking law should incorporate certain "safeguard rules" for balancing different interests. In this regards, Singapore law establishes certain conditions for officials prior to apply for blocking order as follows;

Comparing to the Singapore law, it establishes certain conditions for officials prior to apply for blocking order as follows;

- Condition I: The law states that before directing the IMDA to make an access blocking order the authorised officer must send a notice to the owners or operators of the online location informing them to stop doing activities relating to unlawful gambling. If they comply with this notice, the officer cannot proceed to apply for blocking order.

- Condition II: The law states that before directing the IMDA to make an access blocking order with respect to an online location, an authorised officer must have regard to, and give such weight all of the following matters, including whether the primary purpose of the online location is for use by others to commit an offence, whether the owner or operator of the online location demonstrates a disregard for the prohibitions and restrictions in this Act, volume of traffic at the online location by end users in Singapore, the burden that the making of the access blocking order will place on the Internet service provider, the technical feasibility of complying with the access blocking order.

The two conditions are considered as safeguard principles designed for balancing the conflicting rights and interests associated with website blocking such as burden of ISP. In addition, it could reduce the problems of overblocking by allowing only request of official with a solid cause of suspect and requiring official to take balancing factors into consideration which is consistent to principle of proportionality. However, there are no such conditions according to section 20 of Thai law.

Apart from not incorporating safeguard principle as Singapore law, this paper also argues that section 20 of Thai Act does not identify limitation or scope of blocking process. This can be analyzed by classifying the blocking process according to section 20 in 3 states as follows;

Stage 1: The submit of complaint to the court: Section 20 requires officer to "submit complaint with evidence" by not describing the details in complaint. In addition, the ministerial regulation relating only the stage after the court has ordered. Thus, it is no clear conditions which lead to two types of

practice. Firstly, officer submits complaint by identifying specific location, e.g. http://www.nofreespeech.com/content/188999. Secondly, offer submits broad location e.g. http://www.nofreespeech.com.

Stage 2: The consideration of court: Ministerial regulation merely states that "In case where court ordered to block website according to Related Online Location..." but not requiring order of Court to include specific details of location relating to illegal content. If officer's complaint submitted with a broad location, there is a potential that the court order would be broad.

Stage 3: The order of officer to service provider: After the court has ordered to block website, ministerial regulation states that officer shall make an order to identify which part of content to be blocked. Thus, the law does not explicitly require official to order particular piece of content.

In conclusion, this Act does not clearly stipulate that the entire process of website blocking should be limited to particular or specific data to be blocked leading to the possibility of over-blocking.

Conclusions

The Computer crime Act B.E. 2560 provides certain mechanisms that can be applied to block online gambling websites. This sanction has never been enforced since the original version of this law in B.E. 2550. Nevertheless, those measures of Thai law, by comparative analysis with foreign laws, is broader in scope without adequately providing safeguard principles for balancing the different interest such as freedom of speech. Consequently, the author suggests the amendment of this law by adding safeguard measures as modelled in Singapore law. In addition, the entire process of website blocking should be amended to prevent the overblocking.

References

Nikkinen, Janne. (2014). “The Global Regulation of Gambling : a General Overview”. **Working papers / Department of Sociology.**Vol. 2014.Issue 3.

Messerlian,Carmen et al., (2005). “Youth gambling problems: a public health perspective”. **Health Promotion International.** Vol. 20 : 69-79.

Monkcom Stephen, Gerald Gouriet QC, and Jeremy Phillips. (2017). **The Law of Gambling**. Bloomsbury Professional.

Leslie, Daniel A. (2014). **Legal Principles for Combatting Cyberlaundering**.Springer.

Lemley, Mark et al., (2011). “Don’t Break the Internet”. **Stanford Law Review Online**. Vol. 64 : 34.

Luca Belli and NathaliaFoditsch. (2016). “Network Neutrality : An Empirical Approach to legal interoperability”. in**Net Neutrality Compendium: Human Rights, Free Competition and the Future of the internet**. edited by Luca Belli and Primavera De Filippi. Springer.

Caliskan, Emin (2017). “Risk analysis of internet censorship circumvention : Case study of anonymizaiton tools and effects”. in**Strategic Cyber Defense: A Multidisciplinary Perspective**. edited by Unal Tatar, YasirGokce, and Adrian V. Gheorghe. IOS Press.

Human Rights Watch. (2005). **False Freedom: Online Censorship in the Middle East and North Africa**. Human Rights Watch.

Schell, Bernadette H.. (2014). **Internet Censorship: A Reference Handbook**. ABC-CLIO, LLC.