Development Trend of Information Communication Technology Related Laws

In light of the influence on social security of Internet-related crime, in 2007 Taiwan passed the amendment to the Communication Protection and Inspection Act (CPIA) to update the articles relating to the surveillance of Internet-related crimes. Moreover, the notification obligator clause was added to the Child and Adolescent Sex Trade Prevention ACT (CASTPA), and the penalty for copyright infringement over the Internet was prescribed in the Copyright Act in order to stop Internet-related crimes.

1. Amendment to the CPIA

On 15 June 2007, the legislature of Taiwan passed the amendment to the CPIA which was promulgated by the President of Republic of China on 11 July 2007. The amendment mainly concerns the update of the power of issuing surveillance warrants, the scope of emergency surveillance, the supervisory agencies of relevant surveillance activities, and the evidence power of illegal surveillance. The amendment will be brought into force in five months.

Currently, a surveillance warrant is issued (1) by the district prosecutor following an application made by the police or based on his authority for cases under investigation; and (2) by the judge based on his power for cases on trial. According to Article 5.2 of the amended CPIA, for cases under investigation, the district prosecutor should record the details of surveillance in writing following the applications made by the judiciary police or based on his authority and should state the reasons and submit relevant documents before applying to the jurisdiction court for the issue of the surveillance warrant. The district prosecutor should approve and reply to the applications made by the judiciary police within 2 hours. For cases of greater complexity, the approval and reply time may be extended for another 2 hours with the consent of the chief district prosecutor.

After receiving an application for a surveillance warrant from the district prosecutor, the jurisdiction court should approve and reply to the application within 24 hours. For cases on trial, a surveillance warrant should be issued by the judge based on his authority. Also, the judge may give appropriate instructions for the surveillance in the warrant. Moreover, if an application for a surveillance warrant is rejected by the court, the district prosecutor should make no objection in any form. In other words, the power of issuing a surveillance warrant for cases under investigation has been transferred from the district prosecutor to the judge.

Furthermore, the law-enforcement authorities are given the right to initiate an “emergency surveillance” before application during the investigation of serious criminal cases according to Article 6 of the CPIA. In an investigation of serious criminal cases involving obstruction of voting, kidnapping, offence of the President and Vice President Election and Recall Act, the judiciary police may request the district prosecutor to orally notify the implemental authorities of an emergency surveillance. However, the district prosecutor should report to the jurisdiction court to apply for a make-up issue of the surveillance warrant within 24 hours. The district prosecutor’s office should appoint a responsible district prosecutor or a head district prosecutor as the emergency contact for cases involving emergency surveillance. The court should also assign a special window to take charge of the applications for surveillance warrants made by the district prosecutor, and should issue a make-up surveillance warrant within 48 hours of the acceptance of the application. Should the make-up surveillance warrant not be issued within 48 hours, the emergency surveillance should be terminated immediately.

The district prosecutor, the court of law and agencies taking charge of the country’s intelligence work are responsible for the supervision of surveillance. According on Articles 12 and 16 of the amended CPIA, regulations governing the period and supervision of surveillance are summarized as follows:

(1) The period of surveillance should not exceed 30 days for serious and emergency cases involving endangering national security or social order and blackmailing as in Article 5 of the CPIA; or for cases involving obstruction of voting, kidnapping and offence of the President and Vice President Election and Recall Act as in Article 6 of the CPIA. The responsibility of supervision is the district prosecutor's office for cases under investigation and the court of law for cases on a trial.

(2) The period of surveillance should not exceed 1 year for collecting information of foreign powers or offshore opposing powers as in Article 7 of the CPIA. Intelligence authorities should send agents to supervise the electronic surveillance equipment or to the supplier of surveillance equipment to supervise the conditions of surveillance. Should continual surveillance be needed, the implemental agency should submit concrete reasons to make a second application for surveillance two days before the end of the first surveillance period. However, the surveillance should be terminated immediately when the chief of the intelligence agency believes that it is no need to continue the surveillance before the end of the surveillance period.

Lastly, the exclusivity of the evidence power of information collected from illegal surveillance is added to Articles 5, 6, 7 and 32 of the amended CPIA. According to Articles 5 and 6, should the surveillance involve severe offence of regulations, the information or evidence collected from the surveillance will not be accepted as evidence in a judiciary investigation, a trial or relevant procedure. Additionally, according to Articles 7 and 32, information or evidence collected from illegal surveillance will not be accepted as evidence in a judiciary investigation, a trial or relevant procedure. The severity of the offence should be determined by the judge based on individual cases.

2. Amendment to the CASTPA

Child pornography is easily distributed because of the advancement of Internet communication; and the prepubescent pornography market is expanding as a result. The legislature of Taiwan thus passed on 15 June 2007 the amendment to the CASTPA that was promulgated by the President of Republic of China on 4 July 2007. In the amendment, neighborhood heads, ISPs and telecommunication

system providers are the obligator of notification, and “possessors” of child pornography are to be penalized.
According to the explanatory statement of the act, child pornography is the permanent record of the abuse of the victims. This will inflict continual damage on the victims. Moreover, child pornography is considered a “serious child exploitation” all over the world. Therefore, there is an international understanding to penalize the possession of child pornography. Before the amendment, Article 28 of the statue simply penalizes people distributing and selling child pornography in the form of disc, videotape and printing. Those deliberately distributing, broadcasting and/or selling child pornography in the form of pictures, videotape, film, disc, electronic signal or other form will be penalized by imprisonment for a term of less than 2 years and with a fine of under NT$2 million. [In the amendment,] those deliberately distributing, broadcasting and/or selling child pornography are penalized and imprisonment for a term of less than 3 years and with a fine of under NT$5 million.
While child pornography inflicts continual damage on the victims, Article 28.3 has been added to statute. According to this new Article, those in possession without a proper reason of pictures, films, videotapes, discs, electromagnetic recordings and/or other articles containing sexual intercourses or acts of indecency by people under 18 are to be penalized. In this case, the “possession” of child pornography is penalized. The penalization falls into two stages: competent authorities of municipalities and local counties and cities may order the offender to receive guidance education for 2-10 hours if he/she is detected possessing child pornography without a proper reason for the first time; if offenders are detected for the second time or more, they will be fined NT$20000 to NT$200000. The amendment also refers to the legislation in Canada and the Netherland to reduce the scope of “proper reasons for possession” to scientific study, education and for medical treatment purposes in order to protect prepubescent children from sexual exploitation.
Moreover, the amendment has expanded the scope of the notification obligator by including ISPs and telecommunication system providers as the notification obligator. While the Internet and mobile phones are widely used by the public and prepubescent children often receive pornographic information via the chat rooms on the Internet and SMS, this will cause many side effects on prepubescent children in the absence of appropriate management and protection. According to the statistics provided by the Ministry of the Interior, about 300 prepubescent children are sexually assaulted every year from online dating. According to The Garden of Hope Foundation, 40% of sex trade with prepubescent girls found in Taipei County during 2003-5 was conducted over the Internet, and it was 100% for prepubescent boys. It is thus clear that the Internet has become a platform for distributing child pornography.
ISPs and telecommunication system providers are included as the notification obligator in Article 9 of the amended statute. Therefore, if they do not notify the authorities in the knowledge of child pornography, they will be fined NT$6000-NT$30000 according to Article 36 of the statue. Therefore, neighborhood heads, ISPs and telecommunication system providers must notify the local competent authorities or authorities specified in Article 6 of any prepubescent children who engage or probably engage in the sex trade in their knowledge. This is designed in order to strengthen the notification and prevention functions and to effectively stop those who deliberately use chat rooms on the Internet and SMS to engage in true sex trade in the disguise of online dating.
Though the scope of notification obligation has been expanded in the amendment to the CASTPA to strengthen the notification and prevention mechanisms of prepubescent children sex trade and to define the notification obligations of the supplier and provider of SMS, network chat rooms, BBS, blogs and e-news services, many problems arise as a result. First, when telecommunication system providers have the obligation of notification, they also need to submit relevant evidence. However, this may involve the infringement of privacy of communication. If telecommunication system providers must not commit illegal surveillance, they are unable to acknowledge the contents of communication of consumers. In this case, how can they notify any crime? On the other hand, though information over the Internet is open to the public, it is a tough question for law enforcement officers to provide solid evidence proving that the administrator of online chat rooms and blogs has failed to perform his obligation of notification.
3. Amendment to the Copyright Act
The online music downloading service debate has become a heated issue in recent years for the following reasons: “to select only the songs I like”, “comprehensive repertoires”, and “convenience”. According to the Online Music Downloading Survey by the Secure Online Shopping Association (SOSA), 85% consumers have tried the online music downloading service, thus giving rise to the comprehensive online music downloading software and services. However, to attract consumers with files containing unlicensed music, video or other files and charge users of such services, some ISPs provide computer programs or technologies, e.g. point-to-point (P2P), for users to exchange such outlawed materials and charge users for such services. Such acts of making profit from copyright infringement has inflicted disputes in copyright infringement.
For example, the IFPI’s accusation in 2003 of Kuro, a P2P platform provider, is the first convicted case of P2P music downloading service in Taiwan. Though the software supplied by Kuro is a neutral technology which is not illegal, Kuro recruited members and charged them membership fees for allowing them to illegally downloading, exchanging and reproducing a large amount of unlicensed copyrighted materials with such software and the platform services it supplies. Kuro also advertised that consumers can download tens of thousands of the latest popular songs with the Kuro software and even encouraged members to download them. Therefore, the court decided that Kuro and its members who have practically downloaded copyrighted music illegally are guilty of copyright infringement.
On the other hand, ezPeer, another P2P downloading platform provider, was not found guilty of copyright infringement because no law was practiced at that time to prohibit or restrict the use of P2P software. Also, as a transfer platform, ezPeer offers comprehensive functions and it is thus not a tool for committing crime. Even some users transfer or download unlicensed copyrighted materials with this tool, there is possibility for the non-liability reasonable use. Moreover, ISPs have no filtering obligations in the Copyright Act of the ROC. Therefore, even consumers may use the services for illegal activities, P2P service providers are not an accomplice.
Therefore, to define the liabilities of P2P platform providers, the legislature of Taiwan passed on 14 June 2007 the amendment to the Copyright Act to include P2P software providers in governance of the act. In the future, platform providers will be prohibited by the

Copyright Act from charging members for unlicensed activities. New objects of copyright infringement are added to the amendment, and the amendment includes the addition of Article 87.1.7, 87.1.2, and 97.1; and the revision of Article 93.4.

According to Article 87.1.7, attempt to allow the public to openly transfer or reproduce works of others without prior consent or licensing from the owner is copyright infringement, and supply of computer programs and/or technologies that can be used for public transfer and/or reproduction of such for the purpose of making profits is deemed as copyright infringement. As the supplier of computer programs and/or technologies is the focus of this article, behaviors categorized based on this article must also meet the following requirements: (1) attempt to allow the public to download and/or transfer over the Internet copyrighted materials without prior consent or licensing of the copyright owner; (2) the act of supply of computer programs and/or technologies; (3) and making profits from such behaviors. In other words, the focus of the amendment is to prohibit providers by written law from supplying computer programs and/or technologies for users to transfer and/or exchange unlicensed music, video and/or other copyrighted materials and from charging users or making profits from such services. However, the amendment has adopted the principle of technology neutrality and specifies that P2P software providers will only be penalized when they have the act of making profit and the intention of copyright infringement in order not to prevent technological development and to save ISPs from breaking the law all the time.

As the “intention” of copyright infringement is the criterion of judgment, Article 87.2 is added to the Copyright Act in the present amendment. According to this article, whether or not the doer instigates, guides or incites in advertisements or other active actions the public to use the computer programs and/or other technologies it supplies to commit copyright infringement is the criterion for determining the “intention” of copyright infringement. Also, the court will determine with severity whether or not the advertisements or other active actions are ready for instigating, guiding or inciting the public use the computer programs and/or other technologies the doer supplies to commit copyright infringement.

In general, when providers offer services, such as web photo albums, BBS, instant messengers, auctions, web disks and online discussions, it is not their initial intention to supply software and/or technologies for users to illegally download and/or transfer the copyrighted materials of others, nor do they encourage, instigate, guide, incite and/or convince users to commit copyright infringement. Even such software can be used for transferring and/or distributing unlicensed copyrighted materials, providers must not be restricted, and it should be the users who take the liability of copyright infringement.

After the enactment of the amendment, providers who make profit from supplying software for others to distribute unlicensed copyrighted materials and encourage users to exchange such materials with the software are to be penalized by imprisonment for a term of less than 2 years, community service, or fined, or penalty together with a find of under NT$500000 according to Article 93. Moreover, by adding Article 97.1, the competent authorities are entitled to order ISPs to shutdown or close the business when they are convicted for the abovementioned offences and refuse to stop such illegal acts after being determined for “severe copyright infringement” and “severely injury of the benefits of the copyright owner”.

After this amendment of the Copyright Act, service providers can no longer use the excuse “we simply provide a service platform and have no right to check the behavior of consumers” as an escape of their liabilities. In fact, P2P service providers who charge users monthly fees for the P2P software, such as Kuro and ezPeer, have already signed licensing agreements with music companies before the enactment of this amendment. Therefore, the music they provide for users to download is no more unlicensed copyrighted materials. Therefore, the amendment has certain effect on improving copyright protection.

Release : 2013/04

Tag

← Back

← Previous Next

You may be interested

The Coverage and Policies of Critical Infrastructure Protection in U.S.

Regarding the issue of critical infrastructure protection, the emphasis in the past was put on strategic facilities related to the national economy and social security merely based on the concept of national defense and security1. However, since 911 tragedy in New York, terrorist attacks in Madrid in 2004 and several other martial impacts in London in 2005, critical infrastructure protection has become an important issue in the security policy for every nation. With the broad definition, not only confined to national strategies against immediate dangers or to execution of criminal prevention procedure, th…

Norms of Critical Infrastructure Protection in Japan

The approaches to promote critical infrastructure protection in Japan The approaches to promote critical infrastructure protection in Japan are illustrated below: 1. Coverage of Critical Information Infrastructure In the "Action Plan on Information Security Measures for Critical Infrastructure" promulgated by the Information Security Policy Council (ISPC) in 2005, critical infrastructure is defined as: Critical infrastructure which offers the highly irreplaceable service in a commercial way is necessary for people's normal lives and economic activities, and if the service is discontinued or the supply is deficient …

Artificial Intelligence Governance - Taking Deep Fake as an Example

Artificial Intelligence Governance - Taking Deep Fake as an Example 1.Introduction With the increasing maturity of the use of neural networks, the application of artificial intelligence technologies is becoming more and more widely used. Among them, through the automated editor and convolutional neural network technology, the threshold of the technology of copying films is not very high. In November 2017, some films that superimpose the faces of social celebrities on pornographic film actors/actresses appeared in the American social networking platform, Reddit. These types of films analyze the…

Research on the Introduction of Privacy Protection Management Mechanisms and Data Value-Added Services into Communications Enterprises in 2020

Research on the Introduction of Privacy Protection Management Mechanisms and Data Value-Added Services into Communications Enterprises in 2020 2021/12/09 I. Introduction The global economy is shifting away from traditional economic models towards an emerging digital era as technology advancement and new applications are introduced. The rapidly changing digital age has led to a gradual transformation in the way digital technology is used in the industry, thereby driving the overall growth of the global digital economy. The digital economy is driven by "data," and how data is used, its…