Information Disclosure Mechanism for Technological Protection Measures in China

Lili Zhao†
Center for China Information Security Law, Xi’an Jiao tong University, Shaanxi Xi’an, P R China 710 049

Received 12 February 2012, revised 21 May 2012

With increasing cases of digital works being copied and pirated, technological protection measures have been greatly favoured by copyright owners for protecting the intellectual property in their digital works, while ensuring that these works can be used and disseminated. However, when any copyright owner or supplier fails to disclose the information of technological protection measures appropriately or effectively, damages such as privacy violations, security breaches and unfair competition may be caused to the public. Therefore, it is necessary to establish an information disclosure mechanism for technological protection measures, make the labeling obligation with regard to technological protection measures by copyright owners apparent and warning to security risks obligatory by legislation; effectively guarding against information security threats from the technological protection measures.

Keywords: Technological protection measures, TPM, information disclosure, label and warning

The advance of digital technologies make many things become possible, including the copy and dissemination of commercially valuable digital works through global digital network. Particularly, among the copyright owners of entertainment industry, technological protection measures (TPMs) have been regarded as a necessary creation to help digital works survive in global markets.

In 2005, it was found that the computers of about two million American users were unconsciously exposed to malicious hackers after installation of XCP (extended copy protection) of DRMs (digital rights measures) embedded with unknown software – ‘rootkit’, made users lose control over their computers. The installation of a ‘rootkit’ could hide any code to launch an attack on the user’s computer and network, and then damage their cyber information security. This case was considered as a typical case of the impact of TPMs on cyber information security. At the same time, the non-transparency of TPMs was also thought to be the principle factor to this accident.

As for the copyright owners and suppliers of the TPMs, they prefer not to inform their users the use of TPMs because they are not welcomed by users. Practices have shown that it is unrealistic to expect copyright owners to disclose the information of TPMs on their own, so in order to prevent potential risks of information security, it is necessary to integrate such acts in a standardized, normalized and legal manner. Therefore, to further prevent copyright owners from using insecure or untested software, protect information security and prohibit the abuse of TPMs; disclosure obligations should be established for the right holders of TPMs in the form of legislation. Thus, damage from TPMs to information security can be effectively prevented.

TPMs and Information Disclosure Mechanism

Definition of TPMs

TPMs of copyright refer to protection measures that are adopted by copyright owners to control the accessing, copying and transmitting of their works by effective technological methods. Therefore, as one kind of technological methods and means, TPMs of copyright must firstly meet the characteristics of technicality; secondly, TPMs of copyright should have close association with the object of copyright since it is created for protecting the transmission of works and realizing copyright and related rights; and thirdly, TPMs must have the desired effect of protecting copyright owners.

Legal Protection of WCT and WPPT

The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) afford legal protection to TPMs, and require Member States

†Email: lilihellozl@yahoo.com.cn
to provide technological adjuncts to the protection of copyright and related rights, when exploited on the Internet. According to the definition of Article 11 of WCT, ‘Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law’. Accordingly, effective technological measures for copyrights can be used by copyrights holders to prohibit infringement without the authorization of the holders and legislation.

Definition of Disclosure Mechanism for TPMS

Information disclosure mechanism of TPMs refers to the statement and explanation that the creator or operator of TPMs make with regard to the restriction in the running process of TPMs and the possible security accident and security risk that may cause damage to personal security, property security, public interest and national security. It is mainly composed of labels and warning: firstly, disclosure of the basic characteristics of TPMs as well as the restriction in the running process of TPMs to users before they install and run the software; secondly, disclosure warning users of the possible security risk and damage that may cause to their interests before installation; thirdly, disclosure of information relating to security risks to relevant safety supervision department, and cooperating with this department for further details under this circumstance, when any security threat that may endanger national security is found.

The Rationale behind Information Disclosure Mechanism for TPMS

Disclosure mechanism is one of the most effective ways to reconcile the conflicts between copyright protection and information security. Issues of Sony BMG’s TPMs on its CD products and Microsoft’s ‘Black Screen of Death’ indicate TPMs have posed a threat to information security. It has been acknowledged that users including individuals, governments, enterprises and other organizations may face information security threats, when TPMs are maliciously used by somebody to remotely control their system, track their usage information, and even break their system and steal their information. Article 51 of Constitutional Law of China stipulates that citizens in the exercise of freedom must respect and not harm others’ freedom and rights and also not harm national, social and collective interests. On this ground, the Civil Law of China categorically forbids the abuse of power by related subjects. Therefore, copyright holders or copyright-related subjects should bear corresponding obligations and responsibilities for adverse effects caused by improper use of their TPMs, when enjoying the freedom, rights and interests of using TPMs in their works. In this case, a systematic information disclosure mechanism is urgently needed to reconcile the conflicts between copyright protection and information security.

Information disclosure mechanism can improve the information equivalence between TPM owners and users. According to the Asymmetric Information Theory in economics, asymmetric information means that each subject participating in market activities is unique, in an asymmetric state and in an asymmetric status, which may result in adverse selection or moral hazard. Each subject in the market will bear different risks and benefits based on the volume of information in the digital space. In a market transaction, the more information a subject possesses, the stronger the position it will be in. When TPMs are inserted into digital products in the form of a series of code in order to protect copyright, the users will only have access to the code, without control or even fully understanding the risks involved in the use of digital products. Hence, in a transaction of digital products with TPMs, materials that can prove the damages caused by TPMs are not equally known to the creators or operators and users. Based on the fact that regulations for TPM labeling and warning obligations are absent in legislation, it is necessary to regulate disclosure obligations, so that users can make rational choices before buying and installing TPMs.

Obligation of Information Disclosure of TPMS: Global Perspective

The disclosure mechanism for TPMs was not specified in WCT or WPPT, but can be seen in some regulations in US, EU and France.

USA

To execute the obligations of WCT, the US Digital Millennium Copyright Act (DMCA) stipulates that protection measures should afford enough and effective provisions to prevent anyone from circumventing TPMs used by copyright owners,
namely anti-circumvention provision. According to the Act, this provision mainly includes the following three conditions: (1) access to protected works without permission is not allowed; (2) transacting on access and control of TPMs is forbidden; and (3) exercise of rights related to works protected by TPMs without permission is not allowed. Based on this provision of DMCA, an effective TPM means, measures that can protect the rights and interests of copyright owner and forbid or limit others from exercising rights and interests in copyright without permission. However, the DMCA mentions nothing about the disclosure of TPMs.

In the USA, it was Representative Rick Boucher’s bill in 2003 which first proposed that TPMs should be sufficiently disclosed to users; later such proposals were also presented in the bills of Wyden and Brownback. According to Wyden bill (Digital Consumer Right to Know Act), the TPMs ‘have the side effect of restricting consumers’ flexibility to use and manipulate such content for reasonable, personal, and noncommercial purposes’; and ‘could unfairly surprise consumers by frustrating their expectations concerning how they may use and manipulate digital content they have legally acquired’; and ‘could result in greater market power for the holders of exclusive rights and reduce competition, by limiting the ability of unaffiliated entities to engage in the lawful distribution channels, which was difficult to truly put into effect because of the disunity in the standard of TPMs. These proposals, however, made exceptions for the disclosure of the TPMs in the following two circumstances: (1) the disclosure aggravates consumers’ burden; and (2) the disclosure has no legal purpose. Such proposals undoubtedly have had a positive influence in preventing unjust and fraudulent practices in TPMs.

**European Union**

Provisions about TPM limitations can be found in many EU directives. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on privacy and electronic communications aimed at enabling each member provide equal protection for the basic rights and freedoms, especially for privacy rights in the personal data processing in electronic communication field, and ensuring that the regulations between these data and electronic communication equipments and services coordinate with each other well in this community. This directive was amended in 2009, which established the first compulsive security breach disclosure system. However, while this system created a restriction for the providers of public electronic communication service, there was only a basic framework for personal data owners.

In October 2011, in order to meet the changes in technology and the development of digital market, EU modified original consumer protection directives, and the Council passed the new ‘2011 EU Consumer Rights Directive’. The Article 6 of this Directive stipulates: ‘The seller should disclose the function of digital content and its appropriate protection measures including technologies of regional restriction, tracking and monitoring to the consumers in a way that is easy and clear to understand; the consumers have the right to demand full compatibility information between digital content and software/hardware’. This demand reflects the consumers’ desire for transparency and compatibility of digital products embedded with TPMs in network, and is helpful to realize the consumers’ right to know, maintain legal interests of consumers in the transmission of digital products, and reconcile issues between copyright protection and rights and interests of consumers.

**France**

It is required in the French laws that copyright owners should provide full disclosure of the restrictions relating to TPMs to their users. In order to translate the Directive on Copyright in the Information Society passed in EU in 2001, and guarantee copyright and copyright-related rights in the information society, the French Parliament passed Copyright and Related Rights in the Information Society (law n° 2006-961) for effective protection of copyright and copyright-related rights for digital content industry under network environment. This bill confirmed the legal status of TPMs. Meanwhile, in order to prevent improper TPMs endangering related groups’ interests, social public interests and national security, the Article 15 provided a new obligation, namely, information security compliance obligation, to related interest subjects of TPMs for the application of TPMs. The establishment of this compliance obligation by France through independent provision for the creators and operators of TPMs, not only
provided a new path for the resolution of conflicts between intellectual property and information security, but also presented a higher requirement for the providers and copyright owners of TPMs.

**Absence of Legal Disclosure Mechanism of TPMs in China**

The Paragraph 6 of Article 48 of the Copyright Law of the People’s Republic of China (Copyright Law), is considered as the principal provision of TPMs, and states ‘without the permission of the copyright owner or the owner of the copyright-related rights, intentionally circumventing or destroying the technological measures taken by a right holder for protecting the copyright or copyright-related rights in his work, sound recording or video recording shall bear the responsibility of infringement or shall be investigated for criminal liability if the case constitutes a crime unless other provisions are provided in law or in administrative regulations’. The regulation on Protection of the Right to Network Dissemination of Information promulgated in 2006 further endowed owners with the right to adopt TPMs to protect their copyright in the dissemination of information. Specific provisions are listed in Articles 18 and 26, where Article 26 defines TPMs as referring to the effective technologies, devices, or components used to prevent or limit others from browsing or enjoying works, performances, or audio-visual recordings without permission from the owner, or providing the works, performances, or audio-visual recordings to the public through the network without the owner’s permission; while Article 18 states that intentionally circumventing or destroying technological measures without permission from the owner constitutes an act of infringement.

To ensure the balance of interests in the copyright field, the Copyright Law limits the exercise of copyright through provisions of fair use in Article 22 and statutory permission in Article 23. The direct limitation to the use of TPMs is embodied under the four exceptional circumstances in Article 12 of the regulation on Protection of the Right to Network Dissemination of Information, where intentionally circumventing TPMs is exempted for classroom teaching or scientific research, non-profit service for blind, official duties and computer security testing.12

On 31 March 2012, the National Copyright Administration of China issued the Revised Draft of The Copyright Law of the People’s Republic of China. The Revised Draft includes provisions relating to the content of TPMs and power management information, such as the definition of TPMs, regulations of anti-circumvention, TPM exceptions and the legal liability for circumventing TPMs. Article 64 of this draft stipulates: ‘TPMs refer to the effective technology, device or components that copyright owners use to prevent or limit its works, performances, sound recordings or computer programs from being duplicated, browsed, run or transported through network’.13 All these TPM provisions are summarized in Table 1.

As a code, TPMs can be present in network system, physical system or control system. Because these systems are not running statically but dynamically, the TPMs are designed to control this dynamic running with effective mechanisms - information disclosure mechanisms. The above regulations, including those of Revised Draft in 2012, showed that the regulations on TPMs were mainly consistent with the international conventions on Internet, but did not

<table>
<thead>
<tr>
<th>Status of law</th>
<th>Name of law or regulation</th>
<th>Specific provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The revised Copyright Law (2001)</td>
<td>Article 47 (legal position of technological measures)</td>
<td></td>
</tr>
<tr>
<td>The revised Copyright Law (2010)</td>
<td>Article 48 (legal position of technological measures); Article 22 (fair use); Article 23 (statutory permission)</td>
<td></td>
</tr>
<tr>
<td>The Regulation on Protection of the Right to Network Dissemination of Information</td>
<td>Article 4 (confirmation of the rights of owners adopting TPMs); Article 26 (concept of technological measures); Article 12 (exceptional circumstances of anti-t circumvention); Article 18 (infringement)</td>
<td></td>
</tr>
<tr>
<td>Regulation for the Protection of Computer Software in 2001</td>
<td>Article 24 (prohibition of intentionally avoiding or destroying the software protected)</td>
<td></td>
</tr>
<tr>
<td>Draft</td>
<td>Copyright Law (Amendment draft) on 31 March 2012</td>
<td>Article 64 (definition); Article 65 (anti-circumvention); Article 67 (exceptional circumstances of anti-t circumvention); Article 74 (legal liability to anti-circumvention)</td>
</tr>
</tbody>
</table>
focus on disclosure of TPMs or the kind of criteria that the creator or operator of TPMs should meet. However, in order to control the security risks caused by TPMs, it is necessary to establish an information disclosure mechanism for TPMs in China.

**Conception of Framework for Information Disclosure Mechanism for TPMs for China**

The specific framework for an information disclosure mechanism for TPMs should involve the following aspects:

**Subjects of Information Disclosure Mechanism**

According to the provisions of Copyright law and The Regulation on Protection of the Right to Network Dissemination of Information, the owner of copyright or copyright-related rights could protect his work, performance, sound recording or video recording by the method of TPMs. This is the right that the owners of copyright or copyright-related rights should have. In practice, the owner of the copyright or copyright-related rights is not only the direct subject who operates technological measures, but also the subject who directly masters the information of technological measures. Therefore, when providing services to users, they have the obligation to specify the kind of technological measures or the characteristics of these technological measures which are used, especially the kind of restrictions they adopt. When TPMs are completely conceived and made by a third party, the third party also bears a corresponding obligation.

**Objects of Information Disclosure Mechanism**

Based on the legal relations involved in the application of TPMs, the objects of information disclosure for TPMs are included the following categories:

1. **Direct users under the protection of TPMs:**
   As both the beneficiary and victim of TPMs, according to Consumer Protection Law, Contract Law and other relevant laws, every user should be considered as the direct object of information disclosure mechanism because they have the right of knowledge regarding the products or services provided.

2. **Administrative organs of information network security:**
   Due to the complexity of information security under the network environment, threats to legal rights of citizens, legal persons and other organizations as well as threats to social interests, public security and national security may exist at the same time. The owner of copyright or copyright-related rights who has adopted TPMs should disclose them to related administrative organs while meeting security risks that may endanger national protective information security or intelligence. Specifically speaking, China chooses the ‘segregated operation, longitudinal supervision’ mode to supervise its network security. Administrative organs include Information Work Leading Group of the State Council and its office, Security Monitoring Bureau of Ministry of Public Security, Ministry of Information Industry, The Competent Information Industry Department of the State Council, The State Password Administration Institution, The State Council and other relevant departments that have corresponding duty on the supervision of network security in their respective fields. There are many complex and extensive issues in network security field, which may require each department to work with each other and not only work individually in their department. As a result, the Information Work Leading Group of the State Council and its office set up a specialized Network and Information Security Coordinating Group to coordinate the work of each department. However, as the administrative organ of copyright, when providing protection for the interests of the owner of copyright or copyright-related rights, the Press and Publication Bureau should audit the validity and rationality of TPMs adopted so as to further guarantee the security of their works.

**Cases for Information Disclosure Mechanism**

1. **Installation of TPMs and information disclosure of data collection:**
   Security breaches deployed in DRM of Sony BMG indicated that the TPMs could be covertly installed in users’ computers to monitor their activities, such as software download, data collection and data migration. The TPM can collect information of users’ listening habits (including IP address, and time, date and name of recordings installed in their computers) and pass them to the providers, mostly similar to spywares in many aspects. Therefore, the sufficient disclosure of TPM’s characteristics and a good description of data collection cases of TPMs are a must to respect the consumers’ right to know, and also help consumers make rational election before installation of technological measures.

2. **Information disclosure mechanism under the restriction of TPMs:**
   When referring to the range and restriction of TPMs, relevant subjects should make sufficient disclosure to
users regarding restriction of TPMs. This is consistent with requirement of Copyright Treaty of WIPO which suggests that Member States should adopt measures to prohibit circumvention of technological measures. Meanwhile, there are restrictions in this treaty, that is, one cannot violate the fair use provision in laws and public access to the works in public domain. This treaty demands that copyright owners who have adopted TPMs should make enough and effective disclosure, so as to ensure that the restriction of TPMs is consistent with the restriction to the rights of providers and copyright owners.\textsuperscript{14} Practice has shown that due to the failure of right holders of TPMs to provide sufficient or effective disclosure relating to the restriction of TPMs, users do have a good knowledge about the restriction scope and specific application of TPMs after they are installed on their computers.

(3) Warning of security risks of TPMs:
This subject is the core of information disclosure mechanism. It has been proved that risks are unavoidable, and therefore effective risk management measures are especially necessary. It is recognized that risk warning (informing) is the key under the risk control links, which plays an important role in reducing and diversifying risks.\textsuperscript{15} Due to the irreversibility and seriousness of damage caused by TPMs under a network environment, when acknowledging security risks of TPMs, copyright owners should be required to describe the accidents and damages to users’ information security to related supervision departments in a timely manner. Meanwhile, in order to prevent security risks and reduce the damages, copyright owners of technological measures should timely warn consumers of the existence of information security risks. When disclosing security risk information, necessary solutions should be with provided corresponding measures to enable users and related subjects to deal with network security risks and control the extent of damages.

The Requirement of Information Disclosure Mechanism

The disclosure of TPMs should be sufficient and effective. In other words, the sufficiency of disclosure should be reflected, and the sufficient and effective notification must enable general users to realize the reasonable requirements, compatibility and transparency of the application of TPMs. Firstly, before the digital works embedded with TPMs are installed in users’ computers, copyright owners should specifically explain the nature of the TPMs embedded in the digital works (for instance, usable scope of restricted digital content and its compatibility with other equipments, formats, platforms and applications), and carry out a forecast for possible risks, and then conduct the installation after users’ permission. Secondly, for the security issues caused by TPMs, the related subjects should make a statement regarding the incident within reasonable time and publish specific and operable solutions.

This requirement clearly indicates that the expression for specific information disclosure should be obvious and clear on the screen. According to judicial practice, if the disclosure cannot be read easily, it is generally regarded that the operators have not provided users the specific notification, and therefore, it is unenforceable.\textsuperscript{16} Often operators use unclear links, inconspicuous character style, and grey type in a grey background or link tags of fuzzy intents to inform users of the existence of disclosure. However, for the court, its standard of judgment is only whether the disclosure can be shown in an
obvious way, not the understanding of double traits to information disclosure content or the real understanding of users.

Exception to Information Disclosure

In practice, the confusion of copyright owners lies in their worry regarding possible panic among users, because prompt notification may not only endanger personal interests of copyright owners and the development of copyright industry, but also make the solution of security issues complex. In this case, to balance the interests between right holders and the users of TPMs, exception to information disclosure is required. For this purpose, the legislation of some states in the USA that contain provisions on report delay is worthy of noting. Thus, the requirements of announcement suspension should include—‘(1) based on the reasonable requests of law enforcement, when announcement may hinder the integrity of investigation and evidence collection or authorities; (2) necessary measures are required to determine the scope of security breaches and risks and recover the system into a reasonable and complete form for the case.’

This approach may provide the opportunity for copyright owners to take further measures, and may as well offer conditions for supervising authorities to make investigations and collect evidence.

Conclusion

In the digital environment, the positions of the owner of technology and the user are not duly balanced. As ordinary consumers are blocked from knowing the technological protection techniques, they are prevented from exercising their knowing and choosing right. Exposing or marking the technology protection techniques, especially the restriction techniques would, on one hand, offer suggestions to consumers for choosing the technological protection measures, avoiding risk causing by improper using, while respecting their knowing and choosing rights. One the other hand, sufficient exposure of information would also balance the information between owners and users, avoiding risks brought by unevenly distributed information. Therefore, creating a mechanism of exposure of the information is crucial for technology protection.

References

2 Samuelson Pamela, Schultz Jason, Should copyright owners have to give notice about their use of technical protection measures?, Journal on Telecommunication & High Technology Law, 6 (1) (2007) 42.