

Yimeei Guo *Editor*

---

# Research on Selected China's Legal Issues of E-Business

 Springer

# Research on Selected China's Legal Issues of E-Business

Yimeei Guo  
Editor

# Research on Selected China's Legal Issues of E-Business

 Springer

*Editor*  
Yimeei Guo  
School of Law  
Xiamen University  
Xiamen  
China

ISBN 978-3-662-44541-9      ISBN 978-3-662-44542-6 (eBook)  
DOI 10.1007/978-3-662-44542-6

Library of Congress Control Number: 2014947688

Springer Heidelberg New York Dordrecht London

© Springer-Verlag Berlin Heidelberg 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://www.springer.com))

# Contents

## Part I Anti-monopoly

- 1 **Baidu.Com’s Case Study—Pros and Cons of Web Site Ranking Service Under Chinese Anti-monopoly Mechanism.** . . . . . 3  
Yimeei Guo, Dongsheng Yan and Weiwan Zhang
- 2 **Anti-monopoly Analysis of Tencent QQ Versus 360 Dispute.** . . . . . 11  
Weiwei Hu and Yimeei Guo

## Part II Business Operation Dispute

- 3 **Legal Risks and Solutions to E-Marketers’ Data Mining** . . . . . 23  
Yimeei Guo and CunLu Zhang
- 4 **RFID V. Privacy Risks and Solutions** . . . . . 33  
Yimeei Guo and Ying Luo
- 5 **Tmall Incident—A Legal Problem or Business Operation Dispute** . . . . . 43  
Yimeei Guo and Weiwei Hu

## Part III E-Logistics

- 6 **An Overview of China’s Modern Logistics Development and Some Strategic Actions** . . . . . 55  
Yimeei Guo and Cunlu Zhang
- 7 **Barriers and Legal Solutions to e-Logistics in China** . . . . . 73  
Yimeei Guo and Jinquan Tang

## Part IV E-Privacy

- 8 E-privacy Protection—Centering on Global Main Legal Instruments and Prospects** . . . . . 91  
Yimeei Guo and Ying Luo
- 9 Monitoring Employee’s E-mail: An E-privacy Concern** . . . . . 107  
Yimeei Guo and Ying Luo
- 10 Privacy Concern in CRM Service** . . . . . 115  
Yimeei Guo and Haiyu Huang
- 11 Internet Industry’s Legal Risk and Solution to Personal Privacy Infringement** . . . . . 125  
Yimeei Guo, Weiwei Hu and Zhengzheng Fang

## Part V M-Commerce Security

- 12 Security Problem and Solutions to M-commerce** . . . . . 135  
Yimeei Guo and Ying Luo

## Part VI Online IPR Protection

- 13 IPR Management Strategies for Enterprises in the e-Commerce Era** . . . . . 145  
Yimeei Guo, Dongsheng Yan and Weiwan Zhang
- 14 How Would the Domain Name Dispute—Ikea “Cybersquatting” Case Be Decided Under American Law?** . . . . . 155  
Yimeei Guo
- 15 iPad Trademark Dispute: An IPR Management Lesson Not Just for Apple** . . . . . 165  
Weiwei Hu and Yimeei Guo
- 16 A Comment on Chinese Legal Environment of Online Copyright Protection** . . . . . 171  
Yimeei Guo
- 17 Copyright Disputes and Resolutions to P2P File-Swapping Application** . . . . . 183  
Yimeei Guo and Ying Luo

**18 Legal Risks and Solutions to Video-Sharing Web Sites—Focusing on Copyright Infringement** . . . . . 193  
 Yimeei Guo, Zhou Yu and Junjie Ji

**19 “Safe Harbor” Doctrine: A Panacea for Chinese Search Engine’s Copyright Infringement Liability or Not** . . . . . 203  
 Yimeei Guo, Zhengzheng Fang and Weiwan Zhang

**20 “Google Library”: Some Copyright Infringement Concerns in China** . . . . . 211  
 Yimeei Guo, Yixuan Liu and Zhou Yu

**21 Chinese Internet Industry’s IP Financing: Opportunity and Possibility** . . . . . 221  
 Yimeei Guo, Zhengzheng Fang and Xinfeng Zhang

**22 Combating Against Counterfeit: Third Party E-commerce Trade Platform’s Liability Analysis.** . . . . . 231  
 Weiwei Hu and Yimeei Guo

**23 Digital Music Copyright Protection Dilemma: A Discussion on Draft Amendments of China’s Copyright Law** . . . . . 239  
 Yimeei Guo and Weiwei Hu

**Part VII Third Party E-Payment**

**24 Legal Liability of Online Trade Platform Service Providers** . . . . . 249  
 Yimeei Guo, Zhengzheng Fang, Zhou Yu and Yixuan Liu

**Part I**  
**Anti-monopoly**



# Chapter 1

## Baidu.Com's Case Study—Pros and Cons of Web Site Ranking Service Under Chinese Anti-monopoly Mechanism

Yimeei Guo, Dongsheng Yan and Weiwan Zhang

**Abstract** Web site ranking service is a kind of pay-per-click (PPC) advertising offered by online search engine operators as Baidu.com, which is an efficient method for e-marketing in the network economy era. Besides, it also brings service providers much more profits. However, there are concerns that such Web site ranking service will create a space of commercial fraud and unfair competition, and more and more corporations will be kidnaped by this marketing mode because of the market dominant position of Baidu.com in the Chinese search engine service industry. Therefore, lack of legal risk management for the search engine companies in this field has made the Web site ranking service a significant source of disputes. By doing Baidu.com's case study, this article explores the legal problems arising from Web site ranking service and discusses Baidu.com as an Internet service provider (ISP)—its legal liability under Chinese newly enforced anti-monopoly law (AML) mainly. Then, this article tries to analyze other potential legal risks of Internet business under AML as an extensive thought from the discussion beforehand. Finally, this article puts forward some resolutions aiming at protecting the fair and efficient competition environment as well as the rights and interests of all parties. With the hope to achieve three wins, this article presents its conclusion with the suggestion of more clear legislation and other feasible administrative measures.

**Keywords** Web site ranking service · Anti-monopoly · Legal risks · Legal liability

### 1.1 Introduction

Web site ranking service, known as a kind of pay-per-click (PPC) advertising via online search engine, is an efficient method for e-marketing in the network economy era. Companies which pay for this service from search engine can directly

---

Y. Guo (✉) · D. Yan · W. Zhang

Center for Economic Law, Law Department, Xiamen University, Xiamen 361005, China  
e-mail: yimei\_guo@necmail.xmu.edu.cn

get a front position in some keyword search results. Natural ranking results can easily be changed by money; this is a convenient way for some enterprises to do Web sites promotion. Therefore, the service is more attractive and efficient than traditional search engine optimization (SEO) service which is based on the pure network technology method.

Current Web site ranking service seems to be a double-win business mode. By using this kind of service, companies can obtain the goal as “Let Clients Ask for You” to seize more opportunities to do business with their potential customers. According to the online survey, the top 10 Web sites appear on the search engine account for 72 % of all clicks (Yongjun and Xiaoming 2008). Meanwhile, with the increasing uses of search engine in China, plenty of small- and medium-sized (hereinafter SMS) enterprises are investing much more than ever in search engine advertising. As a result, it brings search engine companies quite a huge profit. According to the 2008 financial annual report of Baidu.com, the revenue brought from online marketing services (mainly the Web site ranking service) accounts for 99.8 % of total revenue, which makes a great contribution for surpassing the revenue of 2007 with a big rate as 83.5 % (Baidu, Inc. 2009).

However, lack of efficient legal regulation and risk management in Web site ranking service field also brings commercial fraud and unfair competition to cyberspace. For instance, Google’s Adwords and Baidu.com’s Web site ranking service has been sued for joint torts in trademark infringement cases. Furthermore, the absolutely dominant position in Chinese search engine market now has made Baidu.com in anti-monopoly disputes. Baidu has been increasingly criticized by the captioned market about its inappropriate choice between commercial interests and ethics.

By conducting Baidu.com’s case study, this article explores the legal problems arising from Web site ranking service and discusses Baidu.com as an Internet service provider (hereinafter ISP)—its legal liability under Chinese newly enforced anti-monopoly law (hereinafter AML) mainly. Then, this article tries to analyze other potential legal risks of Internet business under AML as an extensive thought from the discussion beforehand. Finally, this article puts forward some resolutions aiming at protecting the fair and efficient competition environment as well as the rights and interests of all parties. With the hope to achieve three wins, this article presents its conclusion with the suggestion of more clear legislation and other feasible administrative measures.

## **1.2 Baidu.Com’s Case Study**

### ***1.2.1 Case Overview***

The first case against Internet monopoly under Chinese anti-monopoly mechanism has recently been exposed. Qmyy.com, China’s first online information platform linking medicine manufacturers with distributors and users, sued the biggest Chinese language search engine Baidu.com on December 25, 2008, for

its monopolistic conduct Hao (2009). Qmyy.com required Baidu stop blocking its Web pages from appearing on its search results and pay ¥ 1.106 million yuan (US\$161,460 dollar) for the losses that such conducts have incurred. Beijing First Intermediate People's Court accepted the case on December 26. Besides, the company has requested the State Administration of Industry and Commerce (SAIC) to investigate into Baidu's abuse of its monopoly position in the market.

In this case, the plaintiff argues that if Web sites bought Web site ranking service before and now refuse to continue, it will probably be screened by Baidu.com. Although these Web sites can be found at the top place in searching results of other search engines, at the same time, they will disappear from sight in Baidu.com's search results. Aiming at this problem, as early as in 2005, some Web sites even built a "Anti-Baidu Union" and get the number for record (Yu ICP R 05009507) in Ministry of Information Industry of the PRC (Present Ministry of Industry and Information Technology of the PRC) (Legal Daily 2008). On March 30, 2009, in order to change the negative images of Web site ranking service, Baidu.com even change the name of this service to "Search Marketing Service" as a core part of Baidu.com's new online marketing services plan.

## ***1.2.2 Legal Status of Baidu.Com Under Chinese AML Mechanism***

### **1.2.2.1 Dominant Position—How to Judge Online Market Share**

In order to find a fair and reasonable solution in this case, Baidu.com's legal status should be taken cognizance of. Particularly in an anti-monopoly case, market position of the enterprise as well as its behavior is the key points. According to Article 19 of China's *AML*, we can clearly see that: "undertakings that have any of the following situations can be assumed to be have a dominant market position: (1) the relevant market share of one undertaking accounts for 1/2 or above." However, how to judge online relevant market share is more difficult than in traditional market. For this, Article 12 of China's *AML* prescribes that: "a 'relevant market' in this law refers to the territorial area within which the undertakings compete against each other during a time period for relevant products."

Obviously, as a domestic case, the relevant market should be defined as Chinese search engine service market. Furthermore, as an ISP, user's click and loyalty should be mainly taken account of. According to a research report of China Internet Network Information Center (CNNIC), Chinese Internet search provider Baidu.com continued its leading role on domestic searching market in 2008 with 76.9 % of users choosing Baidu.com as their priority. The loyalty of first priority for Baidu.com has hit 96 %, and other search engines have suffered decline of loyalty, in comparison with that in 2007 (CNNIC 2009). Although Google is the king in international search engine market, but the relevant market is Chinese search engine market—based on Chinese language.

Another report made by iResearch Consulting Corporation also shows that: the Matthew Effect exist and development in Chinese search engine market, the market share of Baidu.com is 73.2 % based on Web sites searching requests, while the No.2 Google.cn's market share is just 20.7 % (iResearch 2009). Therefore, boycotts and public criticism have not had strong enough impacts to challenge Baidu.com's leading positions in the market. Still, Baidu.com has an unparalleled position in China's search engine market. "Baidu" almost is used as a verb when people want to search something online.

### **1.2.2.2 Abuse of Dominant—What Should Enterprises Be Care Of**

Enterprise which gains the dominant position in a market from competition is to give no cause for much criticism; public choices impel this monopoly (Zhaofeng 2008), but if it abuses, this dominant position can become a strong power to imperil the market competition. Baidu.com's dominant position in Chinese search engine market is mainly based on its excellent management and advanced technology, and its diversified services have won the good graces of netizen. Therefore, due to Baidu's wide market coverage, its Web site ranking service has become an important type of online marketing for many domestic companies. They have to join the game to keep the click rate of their Web sites; if not, they will probably fall behind on the search results. There are concerns that more and more SMS enterprises will be kidnaped by this marketing mode without other choice because of the market dominant position of Baidu.com in the Chinese search engine service industry.

In the case above, for most of small- and medium-sized Web sites, Baidu.com is their entrance to customer visits. Most of netizen can just remember the name of Web sites or companies; they have to use the search engine to find the Web sites. Therefore, these companies' Web sites once be screened on the search results, and it can be a great loss to them in the market. Also, consumers will be confused by the misleading search results. Baidu.com's behavior is damage for fair competition, and it should be judged as abuse of dominant position. However, because of the characteristic of Internet, there is no clear definition that whether behaviors like Baidu.com's should be abuse of dominant position in China's AML, but it does not mean that Baidu can easily circumvent the legal regulation. According to Article 17, "... (7) other conducts identified as abuse of a dominant position by anti-monopoly execution authorities." Thus, anti-monopoly execution authorities have the right to define and decide new kinds of abusing behaviors.

## **1.2.3 Legal Liability**

### **1.2.3.1 Analysis Based on Current Legislation**

Since Baidu.com bears the risk to be punished under Chinese anti-monopoly mechanism, its legal liability should be taken into consideration. In accordance

with Article 47 of China's *AML*, "In case there exists an act abusing dominant market position by the undertakings in violation of this law, the anti-monopoly execution authorities shall order the undertakings to cease such act, the illegal gains shall be confiscated, and a fine between 1 and 10 % of the turnover in the preceding year shall be imposed." However, Baidu has not fulfilled the legal obligations, and it has decided everything about this service even including the bidding methods and the down payments without public notification and other proceedings. Once disputes arise, Baidu uses its technologies to screen those users on the Internet, causing additional costs for users. Therefore, Baidu.com's behaviors should be punished under Article 47 of China's *AML*, and it also should pay those users for their loss arising from its infringement.

But actually, the current laws and regulations are not clear in this field, which brings about many troubles. The Internet industry is different from traditional industries in terms of the standards for judging whether an anti-monopoly case can be established. Some online behaviors have not been defined. The newly born *AML* has yet to include the terms on Internet malpractices. This can be bad for enterprises and ISPs because their activities' consequence under relevant law cannot be predicted by themselves. Therefore, clearer judicial interpretation of *AML* should be made as soon as possible.

### 1.2.3.2 Analysis Based on Economics

Abuse of dominant position is not only a legal problem but also an economic issue. Baidu.com's case reflects an economic phenomenon called "Path Dependence." "Path Dependence" theory was originally developed by economists to explain technology adoption processes and industry evolution (Wikipedia 2009). There may not have been any particular reason to prefer one place to another before the industry developed, but as it has become concentrated in one place, any new entrants elsewhere are at a disadvantage and will tend to move into the hub if possible, further increasing its relative efficiency. The system which causes this is a network effect, related to the statistical concept of a power law (D'Souza et al. 2007). As for Baidu.com, its rapid development in the past years was partly because it was the first popular search engine in China which occupied the market. Therefore, someone argues that this dominance will cause market's dependence on Baidu.com which may lead to low efficiency to technology progress. But this article insists that the dominance "per se" is not guilty, while abuse of it is guilty. Baidu has developed its technology and service to maintain its dominance, and this is good for market maximization.

Nevertheless, in this case, Baidu's behavior is doubtlessly harmful to SMS enterprises. Besides, based on cost-benefit analysis, its Web site ranking service also mixes the information with plenty of advertising and raises the search cost of consumers. Many SME enterprises are kidnaped and pay for this service. This is bad for the market and only beneficial to Baidu.com itself. Not only Baidu.com but also the lack of legal regulation is liable for such infringing conduct, and more effective regulation is necessary.

### **1.3 Other Legal Risks of Internet Business with Anti-monopoly Concerns**

Under China's AML, the following behaviors are under fire: monopoly agreement, abuse of a dominant market position, concentration of undertakings, and abuse of administrative power to eliminate or restrict competition. Network companies also have to pay enough attention to these legal provisions. Here, this article will analyze two risks which are unclear under current AML regulation, in order to remind Chinese ISPs especially Baidu.com for sure not to do some activities which can probably be deemed as illegal.

#### ***1.3.1 Information Screen***

Sanlu, the Hebei-based dairy company that was accused of making toxic baby milk powder, reportedly asked Baidu.com to screen reports about the scandal on its Web site (China Daily 2008). That is why Baidu.com has been increasingly criticized by the public. Although Baidu.com has tried to clarify this event, its commercial image has already been tarnished. Therefore, as an Internet service provider, behaviors such as information screen will confront big risk. Particularly, Baidu.com is a dominant search engine company, and if a third party can pay for a service of screen information at will, Baidu can be found as abuse of dominant market position to assist a third party to do illegal actions. Abuse of dominant market position also can be determined whether a search engine assists a third party to decline its competitors' Web sites, and this third party's action is without doubt an unfair competition behavior.

#### ***1.3.2 Illegal Advertising***

Recently, there are repeated press reports of fraudulent online marketing. For instance, CCTV reports that it now has evidence that Baidu.com is engaged in dubious activities. Some Web sites which run illegal medicine business and doing cheating advertising on the top of search results by Baidu.com's service. This behavior can make Baidu.com as a contributor of infringement to consumers. If this illegal medicine business and cheating advertising are natural ranking on the search results, relevant law permits Baidu.com to delete this message after noticed by others without legal liability, Baidu.com is not network police. However, all these illegal behaviors are based on Web site ranking service provided by the dominant search engine. It is serious that Baidu.com placed such a cheating Web site at the top position of its search engine ranking; it will get involved in many disputes and lawsuits.

China has already regulated ISPs by imposing on them obligations to monitor and control the content that passes through their systems. The model used is a mixture of positive law and self-regulation (Reed 2004). Baidu as an advertising operator undertakes a legal obligation to content review in advance. Otherwise, it can be a misleading and cheating behavior to consumers who trust such dominant ISP. Baidu has legal risks under both Advertising Law and AML. Public opinion argues that Baidu.com should pay damage to the consumers regardless of the service quality the Web site provided to the netizens.

## 1.4 Conclusion and Suggestions

Till now, the disputes of pros and cons of Web site ranking service are continuing. But the most important point of view is that the three-win (i.e., the wins of consumers, ISPs, and presiding agency) results are based on every party's efforts. After an analysis of Baidu.com's case as well as other risks under Chinese anti-monopoly mechanism, this article has made the following conclusion and suggestions:

- Web site ranking service via online search engine is an efficient method for e-marketing in the network economy era. It brings much more profits while cause some disputes under the newly born Chinese AML. Enterprises' interests are hurt, and consumers are misled. Besides, ISPs which ignore legal risk management are under legal punishment for their abuse dominant market position. Therefore, changes are needed to protect the interest of each party.
- As for legal agencies, clearer regulation should be established. Particularly, the Supreme People's Court has to make some judicial interpretations to clarify the detail of AML. These interpretations should take specific conditions of Internet into account. Another key point is how to set up an effective mechanism to assure anti-monopoly enforcement agencies to have the enough capability to decide whether a behavior is beneficial to economy and society or not. Besides, a sound e-business legal system is necessary for China to regulate the Internet business.
- For search engines as Baidu.com, more overall legal risk management is needed. First, Baidu had better to separate Web sites which enjoy Web site ranking service from natural search results by different ground color. Removing the advertising Web sites to the right of searching page is another good choice. The form of Web site ranking service should be improved. Second, ISPs should proclaim the standard of information management, and screen and deletion cannot be used at will. Third, if an ISP wants to do something which may have influence on others (such as screen an illegal Web site), evidence reservation is vital.
- In order to protect themselves, enterprises and netizens should not do anything illegal online. Once their interests are hurt by ISPs or a third party, notifying them to stop infringement at first, consultation, and legal weapon is effective choice afterward. Do not forget to reserve evidence and fulfill the notice obligation.

Finally, this article suggests that more research is needed in this field. The first ever litigation against Internet monopoly shows that the awareness of protecting users' rights is on the rise. E-business are challenged under China's new anti-monopoly mechanism, and China has to apply legal methods and other feasible administrative measures to improve the development of e-business and give SMS enterprises more space to live and grow. This article insists that although there is a long way to go, we cannot give up creating a fair and equitable Internet environment.

## References

- Baidu, Inc. (NASDAQ: BIDU). 2009. Baidu announces fourth quarter and fiscal year 2008 results. [http://media.corporate-ir.net/media\\_files/irol/18/188488/reports/Q408PressRelease.pdf](http://media.corporate-ir.net/media_files/irol/18/188488/reports/Q408PressRelease.pdf).
- China Daily. 2008. Guard against net monopoly. [http://www.chinadaily.com.cn/opinion/2008-11/13/content\\_7200397.htm](http://www.chinadaily.com.cn/opinion/2008-11/13/content_7200397.htm).
- Chris Reed. 2004. Internet law, 2nd edn. Cambridge: Cambridge University Press, 95 (Published by "Proceedings of IEEE international conference on e-business engineering. 1 Oct 2009 <EI indexed>).
- CNNIC. 2009. 2008 China search engine users behavior research report. <http://www.cnnic.net.cn/html/Dir/2009/03/05/5483.htm> (in Chinese).
- D'Souza, Raissa M., Christian Borgs, Jennifer T. Chayes, Noam Berger, and Robert D. Kleinberg. 2007. Emergence of tempered preferential attachment from optimization. *Proceedings of the National Academy of Sciences* 104(15): 6112–6117.
- iResearch. 2009. 2008–2009 China search engine research report. <http://www.caijing.com.cn/2009-03-10/110117165.html> (in Chinese).
- Legal Daily. 2008. Baidu encounter the first case under Chinese AML. [http://news.xinhuanet.com/legal/2008-11/09/content\\_10329579.htm](http://news.xinhuanet.com/legal/2008-11/09/content_10329579.htm) (in Chinese).
- Tong Hao. 2009. Baidu sued for alleged monopoly. [http://www.chinadaily.com.cn/bizchina/2009-01/07/content\\_7375269.htm](http://www.chinadaily.com.cn/bizchina/2009-01/07/content_7375269.htm).
- Wikipedia. 2009. Path dependence (economics). [http://en.wikipedia.org/wiki/Path\\_dependence](http://en.wikipedia.org/wiki/Path_dependence).
- Yongjun, Chen, and Meng Xiaoming. 2008. *E-business and E-marketing*, 53. Beijing: Publish House of Electronic Industry. (in Chinese).
- Zhaofeng, Xue. 2008. *Commerce without frontiers: The economics revolution in antitrust*, 22–23. Beijing: Law Press. (in Chinese).



# Chapter 2

## Anti-monopoly Analysis of Tencent QQ Versus 360 Dispute

Weiwei Hu and Yimeei Guo

**Abstract** Anti-monopoly concerns are becoming more and more frequent for Internet industries competing all over the world. This paper makes a case analysis of Tencent QQ versus 360 dispute, then has some further thought from such dispute. Finally, it is hoped by this paper that China's anti-monopoly law (AML) be healthily and perfectly enforced in the future.

**Keywords** Anti-monopoly · Internet industries · Case analysis

### 2.1 Introduction

Anti-monopoly concerns are becoming more and more frequent for Internet industries competing all over the world. For example, in February 2011, Apple launched a new service that allows for magazine and newspaper subscriptions for its popular devices, might draw claim from publishers that Apple dominates the market for consumer tablet computers and that it has allegedly used that commanding position to restrict competition (Koppel 2011). Also in February 2011, Hudong.com, an online encyclopedia, is alleging that Baidu unfairly blocks its

---

(Published by Proceedings of 2011 International Symposium on Advances in Applied Economics, Business and Development (ISAEBD 2011), Part II, Aug 2011 pp.133–141<EI indexed>).

---

W. Hu (✉) · Y. Guo  
Law Department, Xiamen University, Xiamen 361005, China  
e-mail: helusi420hw@163.com

Y. Guo  
e-mail: yimei\_guo@necmail.xmu.edu.cn

Web pages from search results in favor of its own encyclopedia service, Baidu Baike (Wang 2011). On April 1, 2011, Microsoft plans to file a complaint with the European Commission demanding action against competitor Google on competition law grounds. Microsoft claims that Google stops other companies from accessing the information needed to run effective search operations (Microsoft files EU 2011).

Notably, in 2010 in China which has more than 400 million netizens (2011), a “war” called “Tencent QQ versus 360 battle” happened in front of the desktop of tremendous Internet users and was well known both inside and outside the industry. The number 360, which relies on its 360 free anti-virus software become world renowned, is a top company of security software services company chiefs, and Tencent QQ, which is an “overlord” of instant messaging supported by 600 million users, these two desktop client software giants revealed a typical case of Chinese Internet industry’s competition. Undoubtedly, this case is regarded as an anti-monopoly law (AML) issue; however, compared to the traditional anti-monopoly cases, it has its own feature, i.e., it took place in Internet area.

Under the frame of analysis on AML to prohibit abusing the market dominance position, first of all, we must identify whether or not Tencent owns the dominant market position, and secondly to identify whether or not it carries on the action of abusing the dominant market position. But to identify the dominant market position, we have to begin from defining the relevant market (including commodity market and geography market).

In ordinary market, the definition of relevant market is a complex question, involving substitutable demand and supply analysis of alternatives, sometimes even having the hypothetical monopolist test. And in Internet market, it is even more complex. It is temporal and spatial boundary is difficult to determine. Internet market is in dynamic development because of the rapid technology innovation and Internet industry’s vivid characteristic of network externality. Thus, the traditional definition method for relevant market is limited in its application.

Moreover, a dominant market position in Internet market is more complex to determine either the market share or market entry barriers; all of this exhibited some characteristics different from the ordinary market. For example, Internet market entry barriers are mainly expressed as the network effects and intellectual property (IP), technical standards or other non-price factors.

For this reason, although the public tend to make sure that Tencent QQ has a conduct of violating the AML, but it is difficult to convict legally that Tencent QQ violates AML, this article thinks that this issue is very complicated and has a long way to go; it still wants to provide an analysis on the captioned Tencent QQ versus 360 case according to China’s Anti-Unfair Competition Law (AUCL) and the AML and brings forward some further thought and suggestion.

## 2.2 Anti-monopoly Analysis of Tencent QQ Versus 360 Dispute

### 2.2.1 *Fact Summary*

Tencent Technology (Shenzhen) Limited is an Internet service provider (ISP)—its most well-known product, however, is an instant messaging system known as “QQ” (Tencent QQ).

Beijing Qihoo Technology Limited supplies security software—its most well-known line of products, are its “360” line of security software (including software, which protects user’s privacy on the Internet and anti-virus software) (Qihoo 360).

In September 2010, Qihoo 360 launched the software called “360 Privacy Protector.” This product is used to keep tabs on other software on a user’s computer and is able to detect a number of things, for instance, the type of data that software extracts from a user’s computer. The objective of this product is to shield a user from software that illegally extracts or retains a user’s personal data—in other words, to protect a user’s privacy.

On September 26, 2010, Qihoo 360 published an article on their Web site entitled “360 Privacy Protector 1.1 Beta—new function—privacy clean up function.” In this article, Qihoo 360 alleged that its 360 Privacy Protector software had recently detected that “a certain instant messaging software” was found to be “peeping” at the private files and data of users, without first obtaining the approval of those users. The article itself did not name which instant messaging software Qihoo 360 was referring to. However, a screenshot in the article bore the logo of the Tencent QQ instant messaging software.

On October 14, 2010, Tencent Technology (Shenzhen) Limited and Shenzhen Tencent Computer System Limited (hereinafter Tencent QQ) filed an application with the Beijing Chaoyang District People’s Court, alleging that:

Beijing Qihoo Technology Limited (manufacturer and copyright holder of 360 Privacy Protector; and owner of [www.360.cn](http://www.360.cn)); Qizhi Software (Beijing) Limited (company which supplies 360 Privacy Protector software); and Beijing San Ji Wu Xian Internet Technology Limited (operator of [www.360.cn](http://www.360.cn)) (hereinafter Qihoo 360) have fabricated or spread false facts about Tencent QQ’s instant messaging software resulting in the Tencent QQ’s business reputation or “commodity fame” being damaged. This conduct was allegedly in breach of Article 14 of the AUCL.

Further in Tencent QQ’s court application, they claimed that they could properly be construed as a competitor to Qihoo 360 as the latter also manufactures and supplies their own anti-virus or security software (i.e., called “QQ Computer Housekeeper”). In its complaint, Tencent QQ requested that the court prohibit Qihoo 360 from fabricating or spreading false facts about Tencent QQ’s instant messaging software; that Qihoo 360 apologize to Tencent QQ for the conduct described above; and that Qihoo 360 pay damages of RMB 4 million.

On November 3, 2010, the court accepted this case (the AUCL allegation).

On the same day, Tencent QQ issued a newsletter to all its users entitled “A letter to all users of QQ.” Through this newsletter, Tencent QQ informed all users that they have made the “difficult” decision of making the use of QQ instant messaging service incompatible with the use of 360 privacy or anti-virus software. In other words, QQ users who choose to use 360 privacy or anti-virus software will no longer be able to use QQ instant messaging in the same instance. Tencent QQ explained that this was mainly because they were not confident that they could continue to protect their user’s privacy (including data such as chats and passwords), if they continued to use the 360 line of security software. In its newsletter, Tencent QQ also requested that users use its “QQ Computer Housekeeper” or other anti-virus or security software in place of the 360 line of security software.

Notably, from November 3, 2010, users of QQ reported that they were not able to use the 360 line of security software and QQ at the same time. However, a few days later, reports suggest that government agencies intervened and users reported that their QQ and 360 softwares were able to be used concurrently.

On November 4, 2010, Li Changqing (a Beijing-based lawyer) filed a complaint with the State Administration of Industry and Commerce (SAIC) requesting that the SAIC should commence an anti-monopoly investigation against Tencent QQ. In his application, Li alleged that Tencent QQ had abused its dominance by restricting QQ users or “forcing” QQ users to uninstall 360 software, without a valid reason (in breach of Article 17(4) of the AML). Li also submitted a study report issued by iResearch Consulting Group—this report showed that Tencent’s market share in the instant messaging software market was approximately 76.2 %. Li requested that the SAIC impose an appropriate penalty on Tencent QQ for its alleged breach of Article 17(4) of the AML (the AML allegation) (Ning et al. 2010).

This paper then discusses and analyses the AUCL allegation and the AML allegation outlined above in some detail as follows.

### ***2.2.2 The Anti-unfair Competition Law (AUCL) Allegation***

As mentioned above, Tencent QQ’s allegation is that Qihoo 360 is in breach of Article 14 of the AUCL. Article 14 of the AUCL prohibits entities from fabricating or spreading false facts to damage the business reputation or commodity fame of a competing entity.

In order to prove that a breach of Article 14 has occurred, Tencent QQ would need to prove the following elements:

- that Tencent QQ and Qihoo 360 are “competing” entities (first element);
- that Qihoo 360 has undertaken conduct amounting to “fabricating or spreading false facts” about Tencent QQ (second element); and
- that the business reputation or “commodity fame” of Tencent QQ has been damaged (third element).

In respect of the first element, we note that a lot would depend on what the court would construe as the “relevant market”. If the court construes the relevant market to be a broad “market for Internet services,” for instance, then it is likely that Tencent QQ and Qihoo 360 could be construed as “competitors.” However, if the relevant market is more narrowly drawn, it might be more challenging for Tencent QQ to prove that they should rightly be considered “competitors” to Qihoo 360.

As mentioned above, Tencent QQ’s primary business is in providing QQ instant messaging software to users; whereas Qihoo 360’s primary business is in providing the 360 line of anti-virus or security software to users. In Tencent QQ’s court application, they have argued that they are competitors to Qihoo 360’s line of anti-virus or security software, because Tencent QQ also provides similar software in the form of “QQ Computer Housekeeper.”

The second and the third elements would depend on whether the court is satisfied that Tencent QQ has provided sufficient evidence to prove that Qihoo 360 has “fabricated false facts” and that this has resulted in “damage” to the former’s business reputation.

### ***2.2.3 The Anti-monopoly Law (AML) Allegation***

As mentioned above, Li’s allegation is that Tencent QQ breached Article 17 of the AML.

Article 17 of the AML prohibits entities, which hold a dominant position to abuse their dominance by engaging in several specified acts, including by restricting other entities to transact only with the original entity or only with specified entities, without a valid reason (Article 17(4), AML).

In order to prove that a breach of Article 17 has occurred, Li would need to prove or the SAIC would need to be satisfied that the following elements have been fulfilled: that Tencent QQ is “dominant” in the relevant market (the first element); that Tencent QQ has abused its dominance in the relevant market by restricting other entities to transact only with Tencent QQ or only with specified entities (thereby excluding others), without a valid reason (the second element).

With regard to the first element, Article 19 of the AML is instructive. Article 19 of the AML outlines three scenarios in which an entity would be considered a dominant entity, most relevant of which is an entity would be deemed dominant where the entity holds half of the market share (i.e., more than 50 %) in the relevant market. However, this is a rebuttable presumption—in other words, an entity which has been “deemed” as dominant may provide evidence that it is not dominant in the relevant market.

As mentioned above, Li submitted a study report, which alleged that Tencent QQ is dominant in the instant messaging software market (with a market share of 76.2 %). It remains to be seen if a court or the SAIC would be of the view that the report provides sufficient evidence that Tencent QQ is dominant in the instant messaging software market.

Another issue is, that, if indeed the allegation is that Tencent QQ is dominant in the instant messaging software market but that the alleged “abuse” has resulted in effects in the security or anti-virus software market; would a court or authority still consider this to be an abuse of dominance? In other words, if an entity is dominant in Market A but the alleged abuse has taken place in Market B—would such conduct still be construed as an abuse of dominance? If so, what are the factors that a court or authority would consider as relevant in proving such a case?

The allegation appears to be that Tencent QQ has somehow “made use” of or “leveraged” its dominance in the instant messaging market to influence another “market,” arguably the “anti-virus” or “security” software market. Whether an entity has “leveraged,” its dominance in Market A to influence conduct or outcomes in Market B is a complex issue—in overseas jurisprudence (such as the EU), there is conflicting jurisprudence on whether Market A and Market B have to be “related” markets, for an abuse of dominance breach to be made out.

In addition, even if a court or authority was willing to accept that an “abuse” may occur in a separate market, then the next step would be to prove the second element or nature of the abuse. In this case, it appears that the allegation is that Tencent QQ has restricted users from transacting or using the 360 line of anti-virus software, without a valid reason—in breach of Article 17(4) of the AML (Ning et al. 2010).

### ***2.2.4 Brief Comment***

Nevertheless, having a dominant market position itself is not illegal. Only the abuse of such a status falls under the jurisdiction of AMLs. Although in the above analysis, Tencent was suspicious of abusing dominant market position, but the concrete determination requires adequate reasons and evidence. In fact, the foregoing China’s AML, Article 17 (4), provides the condition that corresponding actions constitute an abuse of dominant market position is “not justified,” so obviously, there is need for an application of rule of reason, whether the relevant conduct of Tencent QQ is justified, it is not only a fact-finding problems, but a standard for judgment.

From the Tencent QQ versus 360 dispute, the relevant facts here cannot be fully established; now the parties just act on their own; thus, it requires the fact to be identified by presiding agencies. There are different opinions about the nature of relevant conduct acted by Tencent QQ, whether or not it is a legitimate defensive conduct or an abuse of dominant market position also need further judgment after relevant facts are clear. If it can support that Tencent is “justified” to act this conduct in relevant fact finding, then the behavior does not constitute abuse of dominant market position.

Obviously, even though all the captioned analysis supports that Tencent QQ constitutes the act of abusing dominant market position, going through the whole investigation and analysis must be a very complicated procedure and long process.

Furthermore, in fact, Tencent QQ stopped such suspicious conduct immediately under the strong public opinion pressure and after presiding agency's intervention. Therefore, the problem of prohibiting such suspicious conduct to continue does not exist any more. Certainly, it does not influence the attribution and enforcement of penalty, etc., punishment against such happened conduct, only the level of punishment will be different.

## **2.3 Further Thought Arising from Tencent QQ Versus 360 Dispute**

### ***2.3.1 Need We Different Anti-monopoly Law in Internet Area***

Despite the anti-monopoly issue in Internet area has its own characteristic; this paper thinks that it does not mean the application of law must be totally different.

The above analysis shows that, related to anti-monopoly in traditional markets, the anti-monopoly enforcement of Internet area is much more complex and difficult. Comparing with the traditional economy, the Internet economy has the characteristics on faster innovation, easier market entry, market share instability, as well as first-mover advantage, network effects, two-sided markets, and so on.

On the one hand, technical renovation brings impact on the maintenance of the dominant market position and can reduce the demand of rapid anti-monopoly action, but on the other hand, network effects, especially combined with IP, allows the enterprises to rely on its customers, who have already been locked in the use of many existing products and services, to prevent new competitors and high-tech challenges.

Therefore, we must think over these characteristics when enforcing AML in Internet area and developing the analytical methods of AML enforcement, but not completely confined to the traditional AML. For example, such as "price discrimination," "tying," "predatory pricing," and other conducts, which is concerned by the anti-monopoly policy, it is a strategy for the companies that have considerable market power in the traditional economy; however, in the Internet economy, it becomes just one way to survive for the enterprises and it is a necessary way to keep the most of them survived, so the rationality of "tying" conduct problems requires further research combining with the characteristics of the industry. But these characteristics of the Internet economy has not shaken the basic principles and institutional mechanism of AML, it just needs to consider its distinctive feature when making a concrete analysis.

In this respect, there can be specific guides or regulations aiming at the AML enforcement in Internet area, which come into being based on fundamental principle and system by State Council Anti-Monopoly Committee or relevant legal authority of anti-monopoly enforcement.

### ***2.3.2 Accurate Understanding on Anti-monopoly Law in China Is Required***

Undoubtedly, the public pay close attention to the Tencent QQ versus 360 dispute is in favor of popularizing and propagating the AML in China, but it requires an accurate understanding on this law.

The Tencent QQ versus 360 dispute caused universal public concern and widely reported by the media had a strong influence on the society. For the feverish comments and discussions, in addition to refer to concern for right and wrong and resentment between the two companies in China's Internet industry, it also involves a large number of monopoly and anti-monopoly issues. This makes China's AML, which has implemented more than 2 years, become the focus of public attention again. Whether or not they look forward to the AML enforcement agencies' intervening in the dispute effectively and dissatisfied with reality, or the discussion of applicable law and the assumption of improving law concerning the specific conduct, all of these have played a very important role in publicizing the knowledge of AML, but there are some conditions that are seemingly right but actually wrong even misread the law in the feverish comments and discussions here.

For example, several reports mentioned that the supervision agency considers to split the Tencent Company; this is an unfounded claim. As a private enterprise and listed company, Tencent does not have a responsible supervision agency like state-owned enterprises. Although administration regulator can supervise the conduct of their operations, yet it is without foundation to split. Even the anti-monopoly enforcement agencies of a few countries like the USA can apply to the court to split companies, which made monopolistic conduct, but the AML enforcement agencies in China have no power in this regard.

Except the operators who conduct illegal concentration, the State Council Anti-Monopoly Law Enforcement Agency can order to stop conducting concentration, disposing stocks or assets for duty by the prescribed time and taking other necessary measures to restore the status before the concentration. Except which belong to structural relief measure, for relief measures of the other monopolistic conduct (including abuse of dominant position) are behavioral, that is to say, the Anti-Monopoly Enforcement Agency can order to stop illegal conducts, confiscating illegal gains, and fining more than 1 %, fewer than 10 % sales last year.

Therefore, even if Tencent is convicted of having the monopolistic conduct to abuse dominant market position, according to the laws of China, although they have to receive the appropriate punishment, but the situation to be split is impossible. In a word, intertype competition is a good thing, it is terrible without it; but, we need to regulate competition in order to ensure it is free and fair.

Both 360 and Tencent are all Internet industries, although their main business scopes are different, but there are many intersected areas, and they both take the business model of free services like advertising or add-service, to attract users and to dominate the market quickly, then to be profitable, so there is an obvious competition between them. Under the condition of market economy, an intertype competition in the market is a normal thing, which is the market mechanism to play



a role in the fundamental mode. Technological progress, economic development, as well as the rational allocation of resources, all of which can only be achieved in this competition. If there is no competition between the parties (for example, according to plan instruction to manufacture to produce under the planned economy), and even restrict competition artificially (for example, in a case of one party has a monopoly or the both parties conspire to make a plan for monopolize), that have problems and are more terrible.

Therefore, it is a normal phenomenon that fierce competition between the operators in order to survive and develop themselves under the condition of market economy, from another standpoint; this is a proof of China's market economy status. Of course, the market competition has a difference both in intensity and even in means. Even though competition is a good thing, it has advantages and disadvantages of the means and results. Not all of people like competition in any conditions; on the contrary, the tendency to distort and limit competition is always existent.

For this reason, despite the competition of spontaneous market can't guarantee its fairness or even freedom, it becomes necessary to ensure free and fair competition in modern society by enacting and enforcing of competition laws and regulations Anti-Monopoly Law (2010).

## 2.4 Conclusion

As we know, the promulgation in August 2007 and implementation in August 2008 of the AML is a milestone in the history of China's legislation. However, the implementation of AML has been accompanied by endless controversies in every country just as several cases we mentioned in the beginning in this article. Anti-monopoly is an exotic area in China's legal system, so it lacks sound local resources for self-growth and independent improvement. China's legislative, law enforcement, and judicial sectors are all quite unfamiliar with AML and have virtually no independent experience. They mainly depend on foreign experiences and theoretical research at the literary level. Anti-monopoly is a complex issue involved with legal, policy, economic, and social factors and should be considered thoroughly from various perspectives (You 2010). Nevertheless, it is hoped by this paper that China's AML be healthily and perfectly enforced in the future.

## References

- According to "the 27th statistical report on internet development in China" released by CNNIC on January 19, 2011, up to the end of December 2011, the number of netizens in China has reached 457 million. Such Report (in Chinese) is available at <http://www.cnnic.net.cn/dtygg/dtgg/201101/P020110119328960192287.pdf>.
- Anti-monopoly law needs to be correctly understood: the plausibility of tencent monopoly case (in Chinese). [http://www.legaldaily.com.cn/economical/content/2010-12/31/content\\_2424660.htm?node=21506](http://www.legaldaily.com.cn/economical/content/2010-12/31/content_2424660.htm?node=21506).

- Microsoft files EU competition complaint against Google. 2011. <http://www.out-law.com/page-11844>. 31 Mar 2011.
- Nathan Koppel. 2011. *Apple's subscription rules raise possible antitrust issues*. <http://online.wsj.com/article/SB10001424052748704409004576146613997208194.html>. 16 Feb 2011.
- Susan Ning, Ding Liang, and Angie Ng. 2010. *The QQ / 360 disputes—who, what, where, when and preliminary anti-monopoly analysis*. <http://www.chinalawinsight.com/2010/11/articles/corporate/antitrust-competition/the-qq-360-disputes-who-what-where-when-and-preliminary-antitrust-analysis/>. 12 Nov 2010.
- Wang Xing. 2011. *Baidu accused of abusing dominant position*. [http://www.chinadaily.com.cn/bizchina/2011-02/23/content\\_12063335.htm](http://www.chinadaily.com.cn/bizchina/2011-02/23/content_12063335.htm). 23 Feb 2011.
- You Minjian. 2010. *To understand abuse of market dominance in anti-monopoly law*, *Chinaipmagazine*, 36. 5 June 2010. Available at. <http://www.chinaipmagazine.com/en/journal-show.asp?id=593>.

**Part II**  
**Business Operation Dispute**

# Chapter 3

## Legal Risks and Solutions to E-Marketers' Data Mining

Yimeei Guo and CunLu Zhang

**Abstract** Nowadays, data mining is popular in the science and mathematical fields but also is utilized increasingly by marketers trying to distill useful consumer data from Web sites. Data mining is a powerful new technology with great potential to help companies focus on the most important information in the data they have collected about the behavior of their customers and potential customers. In addition to e-privacy concern of data mining, other disputes are also becoming more popular for e-marketers. Therefore, this article discusses some legal risks of e-marketers' data mining imposed by the captioned issues on the net and presents some solutions that enable data mining projects to proceed without violating these constraints.

**Keywords** Data mining · e-Privacy · Copyright infringement · Trespass · Legal solutions

### 3.1 Introduction

As we enter the twenty-first century, every opinion, interest, and lifestyle known to man seem to have found a home somewhere on the Internet. The new technology and the new form of commerce it has generated have opened up much debate about how to deal with traditional business issues, namely privacy, security, and intellectual property protection right (IPR).

---

(Published by "2005 Int'l Conference on Services Systems and Services Management-Proceedings of ICSSSM'05" of IEEE, Inc., June 2005, pp. 1085–1089<EI,ISTP indexed>)

---

Y. Guo (✉) · C. Zhang  
Management Science Department, Xiamen University, Xiamen 361005, China  
e-mail: yimei\_guo@necmail.xmu.edu.cn

C. Zhang  
e-mail: zclu@sina.com

According to Thearling (1995), a senior director of Wheelhouse Corporation, “data mining” is a set of automated techniques used to extract or previously unknown pieces of information from large databases. He points out that data mining is not a business solution but simply the underlying technology. In technical terms, data mining is described as the application of artificial intelligence (AI) and other intelligent techniques such as neural networks, fuzzy logic, genetic algorithms, decision trees, nearest neighbor method, rule induction, and data visualization, to large quantities of data to discover hidden trends, patterns, and relationships.

Whereas Cavoukian (1998), the Information and Privacy Commissioner of Ontario, says that successful data mining makes it possible to reveal patterns and relationships and then uses this “new” information to make proactive knowledge-driven business decisions.

Nowadays, data mining is popular in the science and mathematical fields but also is utilized increasingly by marketers trying to distill useful consumer data from Web sites. Data mining is a powerful new technology with a great potential to help companies focus on the most important information in the data they have collected about the behavior of their customers and potential customers.

For the hundreds of companies that develop and market such online tracking and data mining capabilities, the development of these technologies and their adoption by millions of Web sites represent vital entrepreneurial opportunities. Clearly, these online data tracking and analysis products are much in demand. For all types of companies that do business on the Web, learning as much as possible about visitors is a precondition for offering customized services and may be the key to growth and expanded revenues.

With data mining tools running on massively parallel-processing computers, someone may have access to all kinds of data about anyone in a database. All these data do not have to reside in one physical location; as the Web grows, information of this type becomes more available to more people.

For example, [www.Amazon.com](http://www.Amazon.com) started featuring thousands of individual best-seller lists calculated by zip codes, workplace, and colleges. DoubleClick, the Internet’s largest advertising company, faithfully captures each Web browser’s mouse click and uses the information to direct consumer advertising. MessageMedia Inc. (a Softbank Holdings Inc.) company even links traditional direct marketing databases to cyberspace pitches. Other companies such as Microsoft, Netscape, and FireFly Networks also track individual interests in everything from music to Web pages.<sup>1</sup>

All these practices could raise serious privacy concerns. Among them, under pressure from privacy advocates, DoubleClick announced in March 2000 that it

---

<sup>1</sup> Mun (2000).

would postpone its profiling scheme until the federal government and the e-commerce industry agree on privacy standards.<sup>2</sup>

In addition to e-privacy concern of data mining, other disputes are also becoming more popular for e-marketers. For instance, data mining involves copying data from one site and reproducing it on the other. Queries can be set out to extract information from another site and report it on your site. A number of sites that contain large amounts of data are very concerned about this. In 2000, Australia Web site Telstra was in dispute with Desktop Marketing over the ownership of its white pages entries and whether or not copyright exists.

Earlier in 2003, American Airlines (AA) sued Farechase, Inc. in Federal District Court in Texas, claiming that Farechase's screen-scraping of AA's flight information from [www.AA.com](http://www.AA.com) was illegal and won a temporary injunction against Farechase, Inc., prohibiting it from the sale or distribution of its Web automation software. [www.Register.com](http://www.Register.com) also won a preliminary injunction in 2004 enjoining Verio, Inc., from either utilizing a search robot to obtain information from [www.Register.com](http://www.Register.com)'s Whois database or utilizing information derived from that database for mass unsolicited advertising by telephone, direct mail, or electronic mail.

Therefore, this article plans to discuss some legal risks of e-marketers' data mining imposed by the captioned issues on the net and presents some solutions that enable data mining projects to proceed without violating these constraints.

## 3.2 e-Privacy Concern on Data Mining

As Mary J. Cronin, professor of management at Boston College, pointed out: If companies on the Internet continue to soak up information as fast as customers can click through a Web site, then privacy will be hostage to technology.

A May 1999 survey on privacy in *The Economist* notes that "the trade in consumer information has hugely expanded in the past 10 years. One single company, Axicom<sup>3</sup> Corporation in Conway, Arkansas, has a database combining public and consumer information that covers 95 % of American households." In fact, Axicom has databases profiling most households in the USA. The company sells its information to both the public sector, including law enforcement, and the private sector, including such industry giants as Walmart and Citicorp.

A *Forbes*' cover story in November 1999, "I Know What You Did Last Night," further highlights the way different slices of consumer data can now be pulled together to create a composite picture of any individual's life. "Computers now hold half a billion bank accounts, half a billion credit card accounts, hundreds of millions of mortgages and retirement funds and medical claims and more. The web

---

<sup>2</sup> Jeffrey Rosen, "The Eroded Self," *New York Times Magazine*, April 30, 2000.

<sup>3</sup> Axicom is the largest data mining company in the USA. It has 5,600 employees, and its sales exceed \$1 billion annually, cited from Seung-Hwan Mun, *supra* note 1.

seamlessly links it all together. As e-commerce grows, marketers and busybodies will crack open a cache of new consumer data more revealing than ever before.”<sup>4</sup>

In an effort to survive the dot-com bust, many online retailers have become even more dependent on online profiling. Many marketing companies argue that they do not use individual personal information, but rather they use trends to target their marketing activities. But there is still the concern that these companies, should they wish, may access personal information of Internet users.<sup>5</sup> The fact is that there is virtually no regulation of Internet marketers or data mining companies. Internet consumers are forced to place concern for confidentiality in a company’s goodwill and internal privacy policies.

However, any discussion of e-privacy also requires consideration of international aspects. The Internet does not stop at any countries’ borders, nor does the transfer of personal information. In Europe, privacy of personal information is considered a basic human right. The European Union Data Directive<sup>6</sup> requires the protection of personal information of European Union citizens. This EU law requires that no information be shared with companies in other countries who do not agree to protect said personal information.

The directive adopts a broad definition of the term “personal data,” so as to include any information relating to an identified or identifiable person. For instance, in AIMedia,<sup>7</sup> personal data consist of collected data (the user has answered questionnaires) and extracted data (the AIMedia deduces user characteristics based on purchase history and statistical comparisons). These data form a user profile, which is directly related to the customer’s identity. Thus, all user-related data in the AIMedia user profile are considered “personal data.”

In July 2000, the EU and the US Department of Commerce worked out a “Safe Harbor” agreement to protect the privacy of European Union citizens. The “Safe Harbor” agreement became effective on November 1, 2000. Under this agreement, US companies that establish privacy polices will be protected from prosecution by EU nations.<sup>8</sup>

Notably, Canada has pursued legislation similarly based on the EU philosophy that privacy of personal information is a human right. The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) came into full effect on January 1, 2004, which would apply to all businesses in Canada that use

---

<sup>4</sup> Mary J. Cronin, “Privacy and Electronic Commerce”, adapted from *Imparato (2000)*.

<sup>5</sup> See Business Week/Harris poll, March, 2001, finding that 35 % were “not at all comfortable” and 28 % were “not very comfortable” with anonymous profiling.

<sup>6</sup> Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ No L 281, 23.11.1995, p. 31. The Directive should be transposed into the legislation of the Member States by October 24, 1998, and has now become a legally binding instrument.

<sup>7</sup> AIMedia is a European e-commerce Web site which develops a commercial integrated intelligent and secure framework for highly targeted advertising.

<sup>8</sup> “Safe Harbor Workbook”, Department of Commerce, [http://www.export.gov/safeharbor/sh\\_workbook.html](http://www.export.gov/safeharbor/sh_workbook.html).

direct marketing and/or data mining that collect, store, and communicate personal information respecting employees and/or customers and businesses with partners and business allies, or outsource company functions of this nature. The Act specifically requires that businesses disclose the purposes for the collection of personal information and that they obtain consent for such use. The Act also contains restrictions against repurposing or publishing/sharing that information.<sup>9</sup>

The new Canadian privacy legislation will force US companies that exchange personal information with their Canadian subsidiaries or with Canadian firms to implement policies and procedures to protect that information, in accordance with the 10 principles set out in the law. US companies should note that the law does not contain a grandfather clause, which means that as soon as the law comes into effect, consent to use all personal information that has been collected in the course of business in Canada must be in place.<sup>10</sup>

In China, legislation related to personal information can only be found in Article 101 of the General Principles of Civil Law, which stipulates that citizens and legal persons shall enjoy the right of reputation and privacy, and these rights shall be protected by law. That is to say, protection of reputation includes protection of privacy. According to the law, violators of reputation rights only assume civil responsibility and this usually only happens after they are sued in court.

The draft of the Law for Personal Information Protection of the People's Republic of China, completed in January 2005, after 2 years' deliberation, has been submitted to the Information Office of the State Council for processing. With a definition of personal information that is broader than just including privacy, the drafted law places a wide range of information under protection, including cell phone numbers, family addresses, medical records, and occupation. Once the law is proclaimed, violators of personal information will be charged with administrative, civil, and even criminal responsibility.<sup>11</sup>

That may be great news for Chinese citizens. As to the e-marketers or data mining companies, continuing to focus their efforts on security, staying one step ahead of those who would invade Internet user's privacy is much better than just guessing or worrying about what possible liability they will assume in the future.

### **3.3 Other Legal Concerns on Data Mining—Selected Foreign Cases Study**

#### ***3.3.1 Copyright Infringement***

As mentioned afore, in 2000, Australia Web site Telstra was in dispute with Desktop Marketing over the ownership of its white pages entries and whether or

---

<sup>9</sup> Krause (2001).

<sup>10</sup> "New Canadian Personal Information Protection Legislation", STAT-USA, [http://www.ad-mkt-review.com/public\\_html/docs/imi001.html](http://www.ad-mkt-review.com/public_html/docs/imi001.html).

<sup>11</sup> "Do We Need Legislation to Protect Personal Information?", Beijing Review, March 24, 2005, Vol. 48, No. 12, at Column 44.



not copyright exists. But in earlier 2003, Desktop Marketing was unsuccessful in seeking a grant of special leave to appeal the Full Court of the Federal Court's decision in favor of Telstra, which found in particular, that

- Copyright subsisted in Telstra's white pages and yellow pages directories;
- Telstra owned such copyright;
- Desktop infringed the copyright by its production of a CD-ROM form of directory, which utilized the entries in the white pages.

The Full Court found that copyright could subsist in a compilation as an original work, in circumstances where such work was created through the industrious collection of information.<sup>12</sup>

In Australia, there is no specific law protecting data or databases in their own right. Instead, databases may be protected under general copyright law.<sup>13</sup> A database may receive copyright protection as a "literary work" in two separate ways:

- (a) if the content of the database is original, in the sense that it has originated from the author and has not been collected from other sources, or
- (b) sufficient skill and labor have gone into the selection, presentation, and arrangement of the data so as to make the "compilation" the original work of the author.<sup>14</sup>

### 3.3.2 *The CFAA Violation*

A US Federal Court has ruled that using data mining tools to search Internet sites for competitive information may be a crime under certain circumstances in *EF Cultural Travel BV versus Zefer Corp.*,<sup>15</sup> (*EF II*). [The court's earlier treatment of the subject appears in the related case, *EF Cultural Travel BV versus Explorica, Inc.*,<sup>16</sup> (*EF I*).]

The facts underlying both *EF* cases involve a dispute between EF Cultural Travel (EF) and defendant Explorica, Inc., competitors in the student travel industry. Importantly, Explorica was founded by several of EF's former employees. Explorica contracted with Zefer Corporation to design and code a software program that would scrape EF's pricing information from the EF Web site and download it into an automated spreadsheet.

Based on this information, Explorica set off to compete with EF by setting its own prices, on average, 5 % lower. Altogether, Zefer ran the scraper twice (comprising more than 30,000 interrogations of the EF Web site), to collect 2000 and 2001 tour prices, collecting approximately 60,000 lines of data.

---

<sup>12</sup> Desktop Marketing Systems Pty Ltd v *Telstra* Corporation Ltd (Hayne and Callinan JJ, 20 June 2003).

<sup>13</sup> Copyright Act 1968 (Cth).

<sup>14</sup> Section 10(1), *id.* See also *Ladbroke (Football) Ltd v William Hill (Football) Ltd* [1964] 1 WLR 273.

<sup>15</sup> 318 F. 3d 58 (1st Cir. Jan. 28, 2003).

<sup>16</sup> 274 F. 3d 577 (1st Cir. Dec. 17, 2001).

EF sued Zefer and Explorica in Federal Court, seeking a preliminary injunction on the grounds of copyright infringement and under the Computer Fraud and Abuse Act (CFAA). The district court refused to grant summary judgment on the copyright claim, but issued a preliminary injunction on the basis of the CFAA, because the scraper software exceeded the “reasonable expectations” of authorized access of ordinary users of the EF Web site.

The court ruled that Explorica was in probable violation of CFAA (18 U.S.C. §1030) and that a preliminary injunction to halt Explorica from similar conduct in the future was justified. The court held that although the defendants did not physically damage the plaintiff’s system or data, the plaintiff suffered business loss, goodwill, and the cost of diagnosing and shoring up its computer system.

The appeals court in *EF I* concluded that EF would likely succeed on the merits on its CFAA claim and upheld the district court’s injunction. The court did not, however, address related arguments concerning whether mere use of scraper software constituted unauthorized access under the statute.

Upon lifting of the automatic stay resulting from its bankruptcy proceedings, Zefer appealed the validity of the injunction as applied to it. The 1st Circuit, after reviewing the findings of its earlier decision, noted that the evidence before it concerning Zefer’s knowledge of the confidential nature of the information provided by Explorica was inconclusive and that, in any event, the same information could have been obtained by Zefer through a manual examination of the EF Web site. The court focused once more on whether the use of the scraper software had exceeded authorized access under the CFAA.

However, the court rejected the district court’s “reasonable expectations” standard for determining what conduct constituted “unauthorized access” under the CFAA where no express limits on access exist. Instead, the court observed, “..... we think that the public website provider can easily spell out explicitly what is forbidden and, consonantly, that nothing justifies putting users at the mercy of a highly imprecise, litigation-spawning standard like ‘reasonable expectations’. If EF wants to ban scrapers, let it say so...”

Finally, the court concluded with some cogent advice for Web site operators: “[W]ith rare exceptions, public website providers ought to say just what non-password protected access they purport to forbid.” The opinion strongly suggests, although it does not hold, that a clear statement by a Web site provider that scraping is unauthorized will give rise to a cause of action under the CFAA.<sup>17</sup>

### 3.3.3 Trespass

In *AA, Inc. versus Farechase, Inc.*,<sup>18</sup> the district court issued a temporary injunction against Farechase, Inc., prohibiting it from the sale or distribution of its Web automation software. The software, also a type of screen scraper, was designed to

<sup>17</sup> Kenneth (2003).

<sup>18</sup> No. 167-194022-02 (67th District Court, Texas March 8, 2003).

access AA's Web site and automatically seek out and aggregate AA's flight, seat availability, and pricing information, including fares available only through [www.AA.com](http://www.AA.com) and not generally available for commercial purposes. Farechase had marketed the software to commercial users, travel distribution centers, and travel agents.

AA repeatedly notified Farechase to cease and desist from scraping [www.AA.com](http://www.AA.com) and distributing software designed to access and scrape data from [www.AA.com](http://www.AA.com). In response, rather than ceasing its scraping activities, Farechase revised its software to include a "masking" feature that permitted the software to disguise itself to prevent detection by AA.

AA argued that Farechase violated [www.AA.com](http://www.AA.com)'s terms of services by accessing the fare and flight information for commercial purposes, thus, as the court noted, "frustrating American's objectives and efforts in developing and maintaining [www.AA.com](http://www.AA.com)." The court classified Farechase's actions as "intentional," "without authorization," and interfering with AA's possessory interest in its computer system.

The court concluded, "Farechase's conduct intermeddles with and interferes with American's personal property. Such conduct constitutes a trespass" that substantially interfered with the airline's "efforts to reduce the cost of distribution of its airline tickets." Interestingly, the court also found that the unauthorized access "may be a violation" of § 33.02 of the Texas Penal Code (criminalizing a breach of computer security).<sup>19</sup>

### 3.3.4 *The CFAA and Lanham Act Violations and Trespass*

Also, in [www.Register.com](http://www.Register.com), *Inc. versus Verio, Inc.*,<sup>20</sup> the court issues a preliminary injunction enjoining Verio Inc. from either utilizing a search robot to obtain information from [www.Register.com](http://www.Register.com)'s Whois database or utilizing information derived from that database for mass unsolicited advertising by telephone, direct mail, or electronic mail. The court holds that Verio's actions will likely constitute a breach of plaintiff's Terms of Use, as well as a violation of both the CFAA and the Lanham Act<sup>21</sup> and a trespass to chattels.

In reaching this conclusion, the court holds that [www.Register.com](http://www.Register.com)'s "Terms of Use" is likely to create a contract between [www.Register.com](http://www.Register.com) and the users of its Whois database, notwithstanding the fact that these users are not required to click an "I Agree" button, indicating their agreement to be so bound.

Verio Inc. is a company that provides a variety of Internet services, including Web site hosting and development. To assist it in developing its business, Verio

---

<sup>19</sup> See supra note 17.

<sup>20</sup> 126 F. Supp. 2d 238 (S.D.N.Y., December 12, 2000) aff'd. 356 F.3d 393 (2d Cir. 2004).

<sup>21</sup> The Lanham Act allows lawsuits for false representation of competitors' services or products.

decided to market its services to individuals who recently registered domain names. Verio obtained information concerning the identity and whereabouts of these individuals, in part, by using a search robot to search [www.Register.com](http://www.Register.com)'s Whois database. Verio then utilized this information to solicit business from these individuals via telemarketing and e-mail.

It is worthy to note that the Court found that Verio's marketing activities would likely violate the Lanham Act. Many individuals, shortly after they register a domain name with [www.Register.com](http://www.Register.com), received a solicitation which indicated the caller was calling from Verio "regarding a recently registered domain name" or "regarding the registration of your domain name." This second solicitation further asked the registrant to "Please contact me at your earliest convenience ... If I don't hear from you in a couple of days I will call back."

The Court was of the opinion that such solicitations, even though they did not use the [www.Register.com](http://www.Register.com) mark or name, would likely create confusion as to their source. This conclusion was supported by evidence of actual registrant confusion submitted by [www.Register.com](http://www.Register.com). The Court accordingly held that such conduct was likely to constitute unfair competition and false designation of origin in violation of §43(a) of the Lanham Act and accordingly enjoined it.<sup>22</sup>

### 3.4 Conclusion and Suggestions

Undoubtedly, technology and the Internet have provided the marketing industry a new gold mine of information to target online consumers. If used responsibly, data mining can benefit both e-marketer sector and Internet users. However, it will only work if there is an acceptable level of security, privacy, and IPR protection on the Internet.

According to the abovementioned discussion, unless there is some external pressure to place limits on how much customer information is collected, or how it is used, it seems likely that online data mining practices will be fine-tuned and expanded as quickly as the technology that supports them.

While e-privacy concern in data mining becomes very important, it is suggested by this article that customers should be told how the data collected about them would be used and whether or not it will be disclosed to third parties. In other words, e-marketers had better give their customers three levels of "opt-out" choices for any data that have been collected:

1. Do not allow any data mining of customer's data
2. Allow data mining only for internal use
3. Allow data mining for both internal and external uses

Besides, e-marketers contemplating using Internet data mining tools such as scraping programs to access a public Web site should consider whether such action is

---

<sup>22</sup> For detail discussion on Verio's case, visit [http://www.phillipsnizer.com/library/cases/lib\\_case23.cfm](http://www.phillipsnizer.com/library/cases/lib_case23.cfm).

authorized by reviewing the terms of use and other terms or notices posted on or made available through the site. Owners of Web sites should consider adding or revising appropriate terms of use to their sites while clearly specifying how their Web site content can be displayed, accessed, and used by site visitors, as well as any prohibitions on such access and use.

## References

- Arnesen, David, W. 2002. On-line privacy-is more protection necessary? Presented at the Pacific Southwest academy of legal studies in business annual conference. 22 Feb 2002.
- Cavoukian, Ann. 1998. Data mining: Staking a claim on your privacy. Information and privacy, Commissioner Ontario. [http://www.ipc.on.ca/english/pubpres/sum\\_pap/papers/datamine.htm](http://www.ipc.on.ca/english/pubpres/sum_pap/papers/datamine.htm).
- Conan, V., M. Foss, P. Lenda, S. Louveaux, and A. Salaün. 2000. *Legal issues for personalized advertising on internet: The AlMedia case study*. <http://www.iiia.csic.es/AMEC/paper2.doc>.
- Imparato, Nicholas (ed.). 2000. *Public policy and the internet: Privacy, taxes, and contract*. Stanford: The Hoover Press.
- Kenneth, A., Adler. 2003. Controversy surrounds 'screen scrapers'. *New York Law Journal*. 24 July 2003.
- Krause, Brent. 2001. An overview of the Canadian personal information protection and electronic documents act. <http://www.gigalaw.com/articles/2001-all/krause-2001-02-all.html>.
- Mun, Seung-Hwan. 2000. Can data mining and data privacy coexist? Policy making between data privacy and data mining, Seminar paper for ADV 391K, Fall 2000.
- Thearling, Kurt. 1995. From data mining to database marketing. <http://www3.shore.net/~kht/text/wp9502/wp9502.htm>.

# Chapter 4

## RFID V. Privacy Risks and Solutions

Yimeei Guo and Ying Luo

**Abstract** Radio frequency identification (RFID) is a generic term for technologies that use radio waves to automatically identify objects. An RFID chip comprises a microchip and a tiny antenna that transmits data from the chip to a reader. The reader is activated whenever the antenna comes into range, and the data can be used to trigger an event—such as raising an alarm or signaling that a pallet of goods has arrived in a warehouse. Usually, the range is no more than a few feet. But there are concerns that such applications will breach the privacy rights of individuals and threaten the security of both organizations and individuals. There are also a range of technical, business, and political barriers to RFID’s development. To avoid being off the pages limit, this paper wants to focus on the critical privacy risks to individuals by RFID. Then, it discusses feasible legal and technical solutions to RFID with some emphasis on the former, i.e., selective current legislative developments in different jurisdictions, to provide companies with insight on what compliance with legislations may entail and to assist companies in possible self-regulation to address these concerns as well. Finally, this article presents its conclusion and suggestion aiming at a healthy and sound atmosphere to RFID’s development.

**Keywords** RFID · Privacy risks · Solutions · Self-regulation

---

Published by “Proceedings of the 4th Int’l Conference on Innovation & Management” Vol. II, 2007.12.5-6, pp.1849-1853<ISTP indexed>

---

Y. Guo (✉) · Y. Luo  
Management Science Department, Xiamen University, Xiamen 361005,  
People’s Republic of China  
e-mail: yimei\_guo@necmail.xmu.edu.cn

Y. Luo  
e-mail: yuhe\_ly@sina.com

## 4.1 Introduction

Radio frequency identification (RFID) is a generic term for technologies that use radio waves to automatically identify objects. An RFID chip comprises a microchip and a tiny antenna that transmits data from the chip to a reader. The reader is activated whenever the antenna comes into range, and the data can be used to trigger an event—such as raising an alarm or signaling that a pallet of goods has arrived in a warehouse. Usually, the range is no more than a few feet.

The chips can be incorporated into a range of products and have an advantage over barcodes in not requiring a line of sight between the chip and the reader. They offer a means of navigating complex global supply chains, allowing companies to track their products from factory to distribution centre, from warehouse to sales floor.

The decision taken by leading global retailers to mandate use of RFID by their suppliers, aided by the emergence of global technical standards, has eliminated any doubt that the technology will be used on a broad scale, says a report by the economist intelligence unit (EIU) released in early 2006. Pilot programmers in retail, consumer goods, logistics, life sciences, automotive, and government are under way and are already producing tangible benefits such as reduced costs, better inventory control, and improved responsiveness to consumer demand.

The supply chain is becoming smarter as a result of the technology, with companies such as Wal-Mart, Tesco, and Gillette using it to track inventory and improve stock replenishment. But to fulfill its potential, the technology needs to be integrated into operational management tools such as enterprise resource planning (ERP) software. It highlights RFID's role as a catalyst for much greater collaboration between companies along the supply chain.

For example, it says a retailer referring to a specific product with one numbering system and a department store that refers to that same product—but with a different numbering system—has no idea that each is selling the same item. By utilizing RFID technology, the two companies could change that situation by sharing consistent data that would allow collaboration through purchasing, development, and promotion of the product.

Outside of the supply chain, a range of other applications are emerging, especially in applications that enhance customer convenience, such as “contactless payment” systems. Another growth area will be in identifying and authenticating people or items for safety or security purposes, such as within passports or to verify a patient's identity at the operating table.

But there are concerns that such applications will breach the privacy rights of individuals and threaten the security of both organizations and individuals. There are also a range of technical, business, and political barriers to RFID's development.

To avoid being off the pages limit, this article wants to focus on the critical privacy risks to individuals by RFID. Then, it discusses feasible legal and technical solutions to RFID with some emphasis on the former, i.e., selective current legislative developments in different jurisdictions, to provide companies with insight on

what compliance with legislations may entail and to assist companies in possible self-regulation to address these concerns as well. Finally, this article presents its conclusion and suggestion aiming at a healthy and sound atmosphere to RFID's development.

## 4.2 Privacy Concerns to RFID

While RFID technology has the potential to provide numerous benefits and opportunities for businesses, it also raises concerns for consumers regarding the privacy of their personal information. Although privacy concerns may be premature given current RFID technology and limited adoption of this technology, there has already been considerable debate regarding privacy and security of personal information and the measures necessary to safeguard personal information.

For instance, Paula Bruening, Staff Counsel at advocacy group the Center for Democracy and Technology, warned at a U.S. Department of Commerce workshop on RFID on April 6, 2005, that RFID is one example of a growing trend toward businesses collecting and using their customers' personal data.

Bruening also pointed out: while most current forms of RFID are not capable of compromising privacy by doing things such as tracking customers' movements, the technology is rapidly moving forward and may soon catch up to consumer and privacy advocates' fears.

In essence, privacy advocates have said that RFID uses small processors and antennas that are integrated into a paper or plastic label. Those chips can then be read by an electronic scanner, and unlike barcodes, RFID chips withstand dirt and scratches. As the range of RFID scanning grows beyond the current 25 ft (7.6 m), RFID could allow corporations and governments to track people's movements and purchases.

But representatives of RFID technology vendors including Texas Instruments and Microsoft, along with users PepsiCo and General Motors, talked of the potential for RFID to revolutionize the way companies manage their inventories, fight counterfeiters, and stop shoplifters.

Generally, privacy concerns regarding adoption of RFID technology include (among others) the following:

- The unauthorized reading of RFID tags.
- The security of personal information contained on RFID tags to prevent the unauthorized use or dissemination of such information.
- The ability of third parties to profile individuals by their possessions containing RFID tags.
- The use of RFID technology to provide covert tracking or surveillance of individuals.

It is possible that many of the public's privacy concerns could be addressed through industry self-regulation, which would require adherence to privacy



policies encompassing fair information practices and possible implementation of privacy-enhancing technologies. Given the increasing rate of adoption of RFID, public perception of a privacy threat to personal information, and lack of current standard industry practices to address these concerns, there is mounting support for the need for legislation to address these privacy risks.

## **4.3 Solutions to RFID Privacy Risks**

### ***4.3.1 Legal Solutions***

#### **4.3.1.1 The European Union**

The European Union (EU) is exploring ways to protect citizens' privacy with regard to personal data gathered using RFID technology. The union created a working group that in mid-January 2005 published its first assessment—"Working document on data protection issues related to RFID technology" (also Known as "Working Document 105"). The group is asking individuals to e-mail comments on its findings by March 31, 2005, to [markt-privacy-consultations@cec.eu.int](mailto:markt-privacy-consultations@cec.eu.int).

The document outlines RFID's potential in a variety of business sectors, including health care, retail, pharmaceutical, and logistics, and calls attention to the need for companies to comply with principals in EU privacy directives whenever personal data are collected using RFID technology. The document also guides makers of RFID tags, readers, and applications, as well as standards bodies, on their responsibility to develop privacy-compliant technology.

Europe already has sweeping privacy laws in place to protect consumers across the continent. For example, retail stores must disclose the presence of RFID tags on products and the presence of readers, how the retailer intends to gather and control the information, the purposes for which the information will be used, who will control the data, how to discard the tag from the product, how to exercise the right to access the information on the tag, and more.

The new working group says it has found other issues with regard to RFID that need to be addressed. RFID technology increases the potential for direct marketing with item-level tagging, since shoppers could be recognized and their movements tracked while in stores, according to the group.

Another concern for the EU working group is the use of applications that link an RFID-enabled plastic card with a consumer's bank account number to enable payment processing, similar to a credit card, without having to swipe the magnetic strip.

Manufacturers of RFID equipment and applications should be held equally responsible for building tags, readers, and printers that protect consumers' right to privacy, the document states. The group stresses there is continuing need for further research and development on issues related to encryption that protect personal information on the tags. It wants to make sure the RFID tag does not divulge

information that would link the consumer with the product which the consumer is buying. If the tag is permanently affixed to the garment, for example, the working group says there should be a way the consumer can delete the information written on the RFID tag or cut it out once the garment is paid for.

For passports and other government-issued identification that must not be altered, the working group suggests using standard authentication protocols from the International Standards Organization (ISO) to encrypt the data and make it unavailable to those without authorization.

In short, according to the European Commission (EC) which has announced the beginning of a public inquiry to identify citizens' concerns about the technology as above mentioned, new legislation may be required to regulate the widespread use of RFID tags.

#### **4.3.1.2 The United States**

On a national level, there is little law currently directed at RFID privacy issues. Of some significance, however, is a not-for-profit lobbyist named consumers against supermarket privacy invasion and numbering (CASPIAN), which has been dedicated to protecting consumer privacy in the marketplace. This organization drafted the "RFID Right to Know Act of 2003," which seeks amendments to the "Fair Packaging and Labeling Program," the "Federal Food, Drug, and Cosmetic Act Relating to Misbranding," and the "Federal Alcohol Administration Act" (Title 15, Chaps. 36 and 94).

Though no legislation has been enacted based on CASPIAN proposed Act, it does address privacy concerns with a set of primary requirements:

- "Notice": Labels that are conspicuous in size, location, and contrasting print are required on products containing RFID tags with a warning that the tag can transmit unique identification information to a reader both before and after purchase.
- "Limitation of Use": Businesses are prohibited from: (1) combining or linking an individual's non-public personal information with RFID tag identification information beyond what is required to manage inventory; (2) disclosing such information to a non-affiliated third party; or (3) using RFID tag identification information to identify an individual.
- "Education": Requiring the Federal Trade Commission (FTC) to establish appropriate standards for businesses to follow to protect an individual's personal information and publish documents to educate the public about RFID technology.

In other national RFID privacy dialogue, U.S. Senator Leahy of Vermont presented a speech entitled "The Dawn of Micro Monitoring: Its Promise, and Its Challenges to Privacy and Security" in March, 2004. Leahy encouraged public discussion of the issues and spoke of the possibility of congressional hearings on RFID technology.

While RFID legislation on the federal level is still taking shape, at least 12 states introduced legislation to address privacy concerns raised by the implementation of RFID technology (including CA, MD, MA, MO, NV, NH, NM, RI, SD, TN, TX, and UT) in 2005. The proposed measures in these bills vary significantly, from simply calling for the establishment of a task force to address the implications of the proliferation of RFID technology, to requiring RFID “kill” technology to deactivate RFID tags upon completion of sale, to seeking to establish criminal liability for misuse of personal information obtained through RFID. However, many of the proposed bills have common minimum requirements. Often among the requirements are including conspicuous notice requirements similar to those in the CASPIAN proposed Act.

#### **4.3.1.3 China, the Hong Kong SAR, and Taiwan**

With Integration of the world’s culture, economy, and infrastructure driven by the lowering of political barriers to transnational trade and investment and by the rapid proliferation of communication and information technologies, developing countries are fast learning both best practices and mistakes of retailing giants in developed countries. For countries such as India, Brazil and China, usage of RFID in retail stores is minimal; nonetheless, these countries are gearing up to meet Wal-Mart and other retailer’s mandates.

Here, we would like to examine current laws and regulations related to privacy in China, the Hong Kong SAR, and Taiwan (if any) as follows:

- China

The Chinese Constitution—like that of the former USSR—provides limited rights to privacy, notably the declaration that “the freedom of the person of citizens of the People’s Republic of China is inviolable” (Article 37) and that “Freedom and privacy of correspondence of citizens of the People’s Republic of China are protected by law.” (Article 40)

China has decided to introduce legislation to tackle the misuse of personal data in daily life. The Institute of Law of the Chinese Academy of Social Sciences has drafted the “Personal Data Protection Act of the People’s Republic of China” and submitted the draft act to the Information Office of the State Council in January 2005.

The bill aims to balance the free movement of information, which is recognized as important in modern society, with protection of basic human rights. The scope of the protection will extend to personal mobile phone numbers, family addresses, medical history, and career status. The Bill also regulates some “hot topics.” For example, it will provide rules for installation and use of cameras in public areas, as well as photography and video recording without consent.

Once enacted, violation of the Bill will trigger not only civil liability but also administrative and criminal liability.

Nevertheless, compared with the US legislation procedure to RFID having started already, it seems that China still has a long way to go.

- The Hong Kong SAR

Hong Kong was the first part of the region to enact legislation based on the EU Directive, with a Personal Data (Privacy) Ordinance covering the public and public sectors and a Code on Access to Information. The statutory Privacy Commissioner (PCO) is currently engaged in work of particular importance regarding privacy aspects of identity cards and health databases.

Notably, the Hong Kong International Airport has announced that it has adopted RFID technology in its baggage handling and cargo services in August 2005. It is believed to be one of the first such projects to go live worldwide in the industry.

If the tags were to contain information personal to the traveler (such as the name, flight number, address, or even passport number) that a signal reader could detect, the set of data stored on the tag would constitute “personal data,” and the Personal Data (Privacy) Ordinance would come into play.

Under Data Protection Principle 4, the airport authorities and airlines would be required to take “all practicable steps” to protect such data against unauthorized access. This would certainly entail consideration of encrypting the data so as to make it unusable by third parties.

- Taiwan

Across the straits, the 1994 Taiwanese Constitution articulates a restricted right of privacy, i.e., that “The people shall have freedom of privacy of correspondence.” That has been extended through legislation such as the 1995 “Computer-Processed Personal Data Protection Law” (*CPPDPL*) concerning the collection and use by government agencies and some private sector bodies of personally identifiable information.

The 1995 law requires that “collection or utilization of personal data shall respect the rights and interests of the principal and such personal data shall be handled in accordance with the principles of honesty and credibility so as not to exceed the scope of the specific purpose,” with a principle right of data access, correction, and deletion. Data flows to countries without privacy legislation can be prohibited.

As to the content recording and the data collecting by RFID tag, it is argued by some expert from Technology Law Center, Information Industry Institute (III) in Taiwan that they both should be limited by CPPDPL.

### ***4.3.2 Technical Solutions***

Opponents of RFID tags have proposed measures to sidestep the chips’ relentless information gathering, ranging from disabling the tags by crushing or puncturing them to simply boycotting the products of companies which use or plan to implement RFID technology. One way to destroy the tags is to microwave them for several seconds.

Another method is to obstruct the information gathered by RFID readers using blocker tags. When carried by a consumer, blocker tags impair readers by simulating many ordinary RFID tags simultaneously. Blocker tags can also block selectively by simulating only designated ID codes, such as those issued by a particular manufacturer.

As claimed by some experts, blocker tags may be available from many sources, merchants may include them for free with purchased goods, or consumers may be able to buy them at the checkout counter. Consumer rights organizations may supply them for nominal cost. As noted earlier, there is no reason why blocker tags should not be cheaply and widely available.

#### **4.4 Conclusion and Suggestion**

There is certainly a great deal of public debate regarding RFID and privacy concerns. While industry self-regulation may be able to address many of these concerns, legislation will continue to be proposed as the appropriate solution until standard privacy procedures and technologies are adopted.

While this article provides an overview of RFID legislation in the EU, USA, China, the Hong Kong SAR, and Taiwan, there are other international implications, including momentum for legislation in other geographic regions.

When formulating privacy policies and procedures relating to RFID implementation, companies should be aware of the current issues being discussed by regulatory bodies and the proposed legislations relating to RFID. Companies could then better assess what measures should be adopted to address compliance with possible RFID-related laws.

Although RFID technology has many current and future benefits, yet policymakers need to be aware of potential privacy and security problems of the rapidly evolving technology. RFID has the potential to expand what people around you know about you, and its uses are worth a policy debate.

Nevertheless, policymakers should not focus new rules on all uses of RFID when many existing uses cause no privacy or security problems. Just as James Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies, a Washington think tank, puts it: "If you're putting a chip in the ear of a cow, is there really a privacy concern?" "A one-size approach won't work." And although rules on the proper use of RFID are needed, they could be industry rules instead of ones set by the government.

Finally, this article suggests that standard bodies and academic institutions need to harmonize hardware and software standards globally, while companies should lay out a framework that helps them understand and address the process changes required to get value from the technology.

## References

- Ari Juels, Ronald L. Rivest, and Michael Szydlo. 2007. *The blocker tag: Selective blocking of RFID tags for consumer privacy*. [http://66.102.7.104/search?q=cache:7prnEPBIP0EJ:theory.lcs.mit.edu/~rivest/JuelsRivestSzydlo-TheBlockerTag.pdf+RFID&hl=zh-CN%20target=\\_blank](http://66.102.7.104/search?q=cache:7prnEPBIP0EJ:theory.lcs.mit.edu/~rivest/JuelsRivestSzydlo-TheBlockerTag.pdf+RFID&hl=zh-CN%20target=_blank).
- Growth of RFID must respect privacy, says EIU*, OUT-LAW News. 9 Mar 2006. <http://www.out-law.com/page-6715>.
- Grant Gross. 2005. *RFID policy panel raises privacy concerns*. 6 Apr 2005. [http://www.infoworld.com/article/05/04/06/HNrfidprivacy\\_1.html](http://www.infoworld.com/article/05/04/06/HNrfidprivacy_1.html).
- Kenneth A. Adler, Esq. 2005. *RFID and privacy issues: A snapshot of proposed laws*. <http://www.rfidproductnews.com/issues/2005.09/feature/08.php>.
- Laurie Sullivan. *The European Union works out RFID privacy legislation*. <http://informationweek.com/story/showArticle.jhtml?articleID=59301363>.
- Peter Sayer. 2006. *EC to investigate RFID privacy concerns*. 9 Mar 2006. <http://www.techworld.com/applications/news/index.cfm?NewsID=5536>.
- Shaping ubiquity for the developing world*. Paper presentation and panel discussion at International Telecommunications Union (ITU) Workshop on Ubiquitous Network Societies, 6–8 Apr 2005. [http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Paper\\_Ubiquity\\_and\\_developing\\_world.pdf](http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Paper_Ubiquity_and_developing_world.pdf).
- Vanessa Huang. 2005. *China contemplates privacy legislation*. 7 Mar 2005. [http://www.twobirds.com/English/publications/articles/China\\_contemplates\\_privacy\\_legislation.cfm](http://www.twobirds.com/English/publications/articles/China_contemplates_privacy_legislation.cfm).
- Zhenhao Gu. 2006. *The potential legal problems of RFID*. *TEEM monthly*. <http://www.teema.org.tw/publish/moreinfo.asp?autono=2845>.

# Chapter 5

## Tmall Incident—A Legal Problem or Business Operation Dispute

Yimeei Guo and Weiwei Hu

**Abstract** Tmall incident invokes legal concerns in certain aspects and is a business operation dispute by nature. This article brings forward the suggestion to make a balance between both parties and hopes a good and healthy development of China's e-commerce.

**Keywords** Tmall incident · Legal concerns · Business operation dispute · E-Commerce

### 5.1 Introduction

In early November 2011, Taobao Mall (hereinafter Tmall), part of the e-commerce operations of Alibaba Group and considered as China's biggest business-to-consumer (B2C) retail platform, suffered from a stormy protest from small vendors against its new rule.

This article provides an overview of the whole incident, analyzes legal concerns related to Tmall incident from certain aspects, e.g., violation of the principle of honesty and credibility, abuse of market power and violation of consumers benefits and rights, and examines whether on earth it is a legal problem or just a business operation dispute as well. Finally, this article brings forward the suggestion to make a balance between both parties and hopes a good and healthy development of China's e-commerce.

---

(Published by "Proceedings of 2012–2013 Advanced Manufacturing Technology, Vols. 472–475, Part 4" (ICMSE 2012. <EI indexed>).

---

Y. Guo (✉) · W. Hu  
School of Law, University of Xiamen, Xiamen 361005, China  
e-mail: ymguo@xmu.edu.cn

W. Hu  
e-mail: helusi420hw@163.com

## 5.2 An Overview of Tmall Incident

Launched in April 2008, Tmall ([www.tmall.com](http://www.tmall.com)) is an online B2C retail platform wholly owned by Alibaba Group.<sup>1</sup>

In June 2011, it was separated from Alibaba Group's online customer-to-customer (C2C) platform—Taobao Marketplace ([www.taobao.com](http://www.taobao.com)) and became an independent business. According to information on Alibaba Group's Web site, Tmall contributes to 48.5 % of China's B2C online retail market as of 2011 Q2 and is also the most visited B2C online retail Web site in China (<http://news.alibaba.com/specials/aboutalibaba/aligroup/index.html>). Tmall currently features more than 70,000 major multinational and Chinese brands from more than 50,000 merchants.

On October 10, 2011, Tmall announced its new merchant rule which, among other things, is set to charge significantly higher annual technical support fee and security deposit to vendors on Tmall. Under the new Tmall rule, the annual technical support fee of 2012 would hike fivefold to tenfold, from RMB 6,000 yuan in 2011 to RMB 30,000 yuan to RMB 60,000 yuan (varied by the size of the B2C stores) in 2012; the security deposit of 2012 would hike fivefold to 15-fold from RMB 10,000 yuan of 2011 to RMB 50,000 yuan to RMB 150,000 yuan (also varied by the size of the B2C stores) in 2012. Both fees are fully or partially refundable depending on a store's sales.

The new rule also includes terms on a 7-day return period for all purchases, stricter rules on shipping time upon order confirmation, and stricter policies against selling of fake products. According to Tmall, the new rule is purely for motivating vendors on Tmall to provide quality goods and better services to customers. The new rule immediately angered small vendors, which would be under huge cash flow pressure and might find it hard to survive.

At the night of October 11, 2011, several big vendors on Tmall were attacked by some 4,000 well-organized attackers, most of which are small vendors on Tmall. These small vendors placed massive orders with the big vendors and then immediately returned the products demanding refunds, while giving the big vendors poor ratings simultaneously. The online protest escalated later with more big vendors affected and the number of attackers growing to over 40,000. The online attacks were said to bring losses of up to RMB 10 million yuan to some of the big Tmall vendors.

On October 15, the Department of Electronic Commerce and Information of the Ministry of Commerce (MOFCOM) started to intervene and ordered mediation. Tmall then changed its uncompromising attitude and started to open online discussions with the attackers, who immediately suspended online attacks. On

---

<sup>1</sup> Alibaba Group is a China-based company group running Internet-based businesses, including online retail, wholesale and payment platforms, a shopping search engine, and data-centric cloud computing services. [Alibaba.com](http://Alibaba.com) is said to be the world's largest online business-to-business trading platform for small businesses.



October 17, Tmall announced that it would delay implementation of the new rates and commit to invest RMB1.8 billion yuan to help small Tmall vendors. The Tmall incident appeared to have temporarily settled (Susan et al. 2011).

## 5.3 Legal Concerns Analysis

### 5.3.1 *Whether Small Vendors' Activities Are Violation of Law or Not*

There are certain differential opinions toward small vendors' conduct in the legal field. Is such conducting a serious illegal one or just a self protection by utilizing the rule of game?

Some legal personnel point out that small vendors are clever enough to fully use the rule of game during the process of game. If we look superficially, that small vendors buy goods, give poor comments and return goods complying with the rule because most of the people are vendors and buyers of other goods at the same time. Therefore, small vendors' conduct is exactly reasonable just like to set a person's own spear against his own shield.

But most legal personnel think on the contrary. First, according to Article 4 of China's *Contract Law* which provides that: "The parties shall have the rights to be voluntary to enter into a contract in accordance with the law. No unit or individual may illegally interfere." After the contract reaches the deadline, both Tmall and its merchants have the right to choose whether or not to renew the contract and how to renew the contract. Tmall is a privately owned e-commerce platform. Its operator has the right to develop its own operation strategy and independently decide the price for the product and service provided by it. Speaking from this meaning, Tmall's new merchant rule is the display for the right to operate independently, while the small vendors' collective attacking activity against the big merchants belongs to serious violation.

Second, Article 4 of China's *General Principles of the Civil Law (GPCL)* provides that: "In civil activities, the principles of voluntariness, fairness, making compensation for equal value, honesty and credibility shall be observed." The principle of honesty and credibility is the reflection of market ethics and standard of civil law, i.e., when civil subject has civil activities, it should have honest intention, good faith, enforce the right without infringing other, and the society's interest, abide by basic trading morality, perform the duty, keep the promise, and comply with the laws and regulations, and finally achieve the goal that all the obtaining civil benefit activities not only make the balance among the parties, but also among the parties and the society. Thus, the "Anti-Tmall Alliance" is utilizing the loopholes of Tmall's rule to engage in malicious attack and violates the principle of honesty and credibility.

Recently, as the extension of the principle of honesty and credibility, there is the principle of prohibition of abusing right commonly recognized by the civil law

of various countries and regions. Such principle indicates that when civil subject is doing civil activities, it should correctly exercise the right and cannot exceed the due limit, or else it constitutes abuse of right. As to how to judge the right abuse, according to *GPCL* and related civil laws and regulations, civil activities should be at first in accordance with the law, if there is no regulation, it should be complied with the national policy and customs. Civil subject exercises the right should respect society's public morality, may not impair the same protected other's interest and society's public interest, and may not disrupt society's economic order.

Besides, following the development of society, the application aspect of the principle of honesty and credibility in *Contract Law* is more and more wide. In addition to complying with the principle of honesty and credibility, when fulfilling the contract, such principle also applies at the stage of concluding contract, i.e., precontract stage and in certain conditions after terminating contract, i.e., post-contract stage.

Article 42 of *Contract Law* provides that: "The party shall be liable for damages if it is under one of the following circumstances in concluding a contract and thus causing losses to the other party:

- (1) Disguising and pretending to conclude a contract, and negotiating in bad faith;
- (2) Concealing deliberately the important facts relating to the conclusion of the contract or providing deliberately false information;
- (3) Performing other acts which violate the principle of good faith."

Inter alia, the so-called disguising and pretending means the party without any purpose to sign contract with the other party, to negotiate with the other party as an excuse, and the purpose is to damage the other party or the third party's interest. The so called negotiating in bad faith in general indicates that one party begins or continues to proceed negotiation under the circumstance of no intention to reach agreement with the other party. According to the principle of voluntariness, the parties may freely decide whether or not to sign the contract, with whom to sign the contract and to sign what kind of the contract. One party who proceeds negotiation with the other party for concluding contract, once the negotiation fails, normally does not assume liability. But the parties proceeding negotiation should abide by the principle of honesty and credibility. If one party violates such principle to proceed a malicious negotiation or stop negotiation in bad faith and cause damage to the other party, it shall assume contracting fault liability.

Para.1 of Article 2 of China's *Anti Unfair Competition Law* provides that: "Managers shall abide by the principle of voluntariness, equality, impartiality, honesty and good faith, and also adhere to public commercial morality in their business transactions." Under "Tmall's October Fortress Besieged incident", small vendors' attacks concentrated on big vendors, pretended to buy goods, refused the delivery after placing the order or gave malicious poor comment. All these conducts not only made big vendors become innocent victims but also disrupted Tmall's trading order, injured innocent third party's, especially, consumer's interest, and let Tmall's goodwill be reduced simultaneously. Speaking from jurisprudence, those attacks' performers violate the principle of honesty and credibility in market trading. They not only have to assume contracting fault liability under *Contract Law* but also suspiciously constitute the act of unfair competition

(i.e., premeditated commercial fraud). As the provider of credit investigation, Tmall should recover the original credit. Tmall's vendors have the right to claim infringement against organizers and asked compensation within the range of losses.

### ***5.3.2 Whether Tmall Abuses Its Market Power or Not***

#### **5.3.2.1 Does Tmall Have a Dominant Market Position?**

For all abuse of dominance cases, the threshold issue would be to define a relevant market and then to explore whether the business operator at issue has a dominant position in the relevant market or not.

There is no easy answer here as to whether or not the relevant market shall be defined as the B2C market, B2C and C2C markets as a whole, or even all retail channels including both online platforms and brick-and-mortar stores.

Even if the relevant market is defined as the relatively narrow B2C market, the above-mentioned market share data (48.5 %) is not able to support a presumption of dominance under Article 19 of the *Anti-monopoly Law (AML)*. Under Article 19, only if a single company holds more than 50 % share of a relevant market could a (rebuttable) presumption of dominance be established.

#### **5.3.2.2 Does Tmall's Conduct Constitute an Abusive Act?**

Each of the abusive conducts listed under Article 17 of the *AML* requires a "reasonableness" test. In other words, a conduct will become abusive only if it is implemented by a dominant company without a valid reason. Since the charged fees are refundable, it will be reasonable for Tmall to argue that the new rules are designed for valid reasons, namely, to improve the overall quality of Tmall vendors and to combat selling of fake goods on Tmall for the ultimate benefits of consumers (Susan et al. 2011).

### ***5.3.3 Whether the Consumers Benefits and Rights are Impaired or Not***

Article 9 of the *Law on Protection of Consumer Rights and Interests* provides that: "Consumers shall enjoy the right of free choice of commodities or services. Consumers shall have the right to make a free choice of business operators for supply of commodities or services, select freely among varieties of articles or forms of services and decide independently to buy or not to buy any kind of commodities, or to accept or not to accept any item of services. Consumers shall have the right to make comparisons, differentiations and selections when they make a free choice of commodities or services."

In this “network riot” with small vendors attacking big vendors, consumer’s right to choose big vendors to consume was impaired to certain degree, because small vendors adopted extreme measures such as launched attacks against Tmall’s big vendors by crazily auctioning goods, submitting poor comments, and returning goods without reason. Via small vendors’ crazy participation in attacking and collectively purchasing from named merchants, if the merchant vendors do not deliver the goods within 72 h, then such small vendors may apply for compensation from Tmall, and the merchants’ points will be deducted at the same time. If the merchant vendors deliver the goods within 72 h, then such small vendors may apply for refund after receiving the goods according to 7 days guarantee of refund or exchange, and uniformly gave out the score of 0 or 1 as evaluation. Many merchants including Hstyle, Osa, etc., were affected by the captioned incident. To encounter the attacks from small vendors against merchants with brand names, part of them have temporarily closed the function of pay on delivery (P.O.D.). Some of them even closed the shops temporarily. Therefore, consumer’s right to choose such vendors to engage in transaction was damaged.

As to Taobao’s excluding small vendors by using the method of raising capital threshold, it is must for transformation and upgrade for Taobao. The major direction of Tmall is not wrong. B2C is the main stream of e-commerce market. There is a mingling of good and evil in C2C which cannot become the main force of Tmall’s profit contribution. Thus, only to strengthen the genuine goods guarantee and service level of Taobao’s B2C Mall, can it maintain the leading status in its industry. The main purpose of Tmall’s this time “price increase” is to enhance the threshold to provide more resources for big vendors with scale advantage. In the long run, focusing the resources on big vendors will raise income. After all, under the same traffic and input of promoting resources, the output level of big vendors apparently are higher than that of small ones. Of course, such measures of Taobao do not definitely mean that consumers are forced to bear higher price and lower quality of service finally because Taobao may refuse bad-quality small vendors’ permission to enter the Mall and build much better ecological environment. Besides, after big vendors have formed scale advantage, it may reduce the cost, provide much better quality, service, and shopping experience, but the premise is that it can not go to monopoly.

Although currently Tmall occupies the governorship in B2C market, yet it confronts two insidious threats: First, “fake” and irregular operation is the most inveterate disease. In 2010, Taobao had dealt 1,400 pieces of goods infringing intellectual property (IP). The existence of large volume fake goods and parallel imports harms consumer’s right and benefit in one side, and injures Taobao’s goodwill in another side. Second, the competition in online retail market is very keen. Taobao meets impacts from competitors everywhere. For example, the genuine goods service image and strong logistics support established by Jingdong Mall within 5 years is deeply rooted in people’s heart gradually. Jingdong Mall’s annual sales amount topped RMB10 billion yuan in 2010. In addition to Tmall’s market shrinkage, the market share of its competitors such as [dangdang.com](http://dangdang.com), [yihaodian.com](http://yihaodian.com), Jingdong Mall, and VANCL grows several hundred percentages

simultaneously. Compared with C2C, B2C owns stable annual fee and the income of transaction commission. In the USA, the income of B2C mode Amazon is much higher than C2C mode Ebay. This is the main reason that Tmall can be independent. But in recent years, the B2C Web sites represented by VANCL and dangdang.com build warehouse, express mail and can make quick delivery pour. Compared with Taobao and Tmall, those B2C Web sites may guarantee delivery speed, after sales service and genuine goods, and are favored by online purchasers, e.g., suning.com combining purchase, capital, and logistics advantages together harvested No. 4 status in this industry.

People in the circle think that e-commerce industry in the future will transmit from the original competition stage of low price promotion plus Ads bombing to the overall competition upgrade stage of supporting by technology and innovation and considering customer's experience. Setting up technical barrier and contesting for key point talents will be the decisive factor of competition in the future. It also means that compared with C2C market, B2C market will be the main battlefield for online retail competition.

To face the development trend of online retail market, Jack Ma, founder and CEO of Alibaba Group said: *If Tmall doesn't make a change, it will die after 3 years.* Therefore, Taobao Alibaba's online retail unit split into three sections in June 2011. It made a separation between B2C mode Tmall and C2C mode Taobao, and its development core would be slanted to Tmall. Thereafter, it announced the new fees collection rule. According to Taobao's statement, the newly announced rule was to promote its merchants more aggressively and seriously conducting their operation behavior in Tmall and optimize the purchasing environment of Tmall.

## 5.4 Tmall Incident—A Legal Problem or Business Operation Dispute

It should be spoken that Tmall as a privately owned e-commerce platform, its operator has the right to develop itself operation strategy and independently decide the price for the product and service provided by it. Thus, Tmall's new fee collection rule is the enterprise's adopted measure to adjust the change from market development and promote itself competition and is the display for the right to operate independently without doubt. Besides, as mentioned above, according to Article 4 of China's *Contract Law*, after the contract reaches the deadline, both Tmall and its merchants have the right to choose whether or not to renew the contract and how to renew the contract. If the merchants think Tmall's charge is unreasonable, then they can completely refuse to renew the contract after it expires. Therefore, the small vendors' "network riot" is untenable in the legal aspect.

What "Tmall incident" reflects indeed is the process between Tmall and small vendors to mutually play game for contract conclusion. By the way of raising

the threshold to optimize the Mall's shopping environment so as to strengthen Tmall's competitive power is the display for the right to operate independently. According to Para. 2, Article 5 of China's *Company Law* which provides that: "The company's lawful rights and interests are protected by law and shall not be infringed upon." Besides, *Contract Law* enacts clear regulations for contract's conclusion, performance, and liability for breach of contract, etc. Both parties can completely apply *Contract Law* to resolve the disputes in contract. As to the certain loss of interest suffered by the small vendors, this is the outcome of industry marketization and the government should not intervene too much. As to whether or not it is necessary for the government to enact legislation toward "Tmall incident," the existing law can completely solve this problem. Also, it is not realistic to enact legislation toward individual incident, since law emphasizes stability and prevalence.

## 5.5 Conclusion

Generally speaking, it is completely in line with market logic for Tmall to elevate the access threshold in order to dismiss substandard shops and raise its brand value and services. Because Tmall has long been faced with a flood of fake goods and endless complaints, elevating the access threshold will greatly benefit Tmall and consumers. The move will also help small and medium (S&M) shops to enhance product quality and marketing levels and create an honest and sound commercial environment in the long run.

The contradictions in the appeals of both sides appear to be "terrible pain" amid the development of China's e-commerce sector. Jack Ma has insisted that they have *acted as it should*. Although many people regard Tmall's new rule as the "direction of e-commerce," many people have still blamed Tmall for its "immoral practices." How to get rid of the objective contradictions between the needs of enterprises to expand and the protection of numerous small and vulnerable vendors? The "pain of transition" needs a rational solution.

As to Tmall, as mentioned above, what kind of business model and operation strategy to choose is the display for the right to operate independently and is protected by law. But law after all is the lowest conduct standard. As to a years long lasting business model which adopts a domineering and no scope for consulting attitude or more conciliatory method while changed, it is not only the legitimate or illegitimate problem but also a display for operation strategy and morality in the business circle. In other words, raising the entry requirements would be beneficial for Tmall in terms of improving its services. But Tmall was too quick to announce the new management rules before giving an adjustment time to retailers, which is very important for small businesses (Zhu 2011).

Nevertheless, with regard to small vendors, to use which method to maintain right is also a problem related to commercial civilization and culture. It will be much better to establish an S&M merchants association or the similar organization

to initiate negotiation with Tmall than to appeal to the brutal method such as “network riot.” After all, to combat brute hood by brute hood only can be both failed situation. Certainly, Tmall finally made compromise as mentioned above but only temporarily left aside this problem. Viewing on this incident, S&M merchants should respect market principle in one side and should maintain right reasonably in another side.

Besides, this incident, together with the previous “3Q dispute,” is certainly a warning to the presiding agencies. Since the e-commerce is soaring, they had better accelerate their steps to establish a proper legal environment based on the interests of the platform enterprises, sellers, and consumers for the development of the e-commerce, and they also had better strengthen the market supervision of the e-commerce under the network background, safeguard the order of the e-commerce and build up an outstanding environment for the development of the e-commerce.

For whether the e-commerce or the economy of China, China should not only encourage more enterprises to grow bigger and stronger but also protect the subsistence and development rights of the great number of S&M enterprises operating legally. That is the right road of China’s development (Pang 2011).

## References

- Pang, Zili. 2011. Taobao Mall suffers from growing pains. <http://english.peopledaily.com.cn/90780/7620212.html>, 18 Oct 2011.
- Susan, Ning, Liu, Jia, Sun Yi, Ming, and Yin, Ranran. 2011. Tmall incident—another chinese internet giant accused of abusing dominance. <http://www.chinalawinsight.com/2011/10/articles/corporate/antitrust-competition/tmall-incident-another-chinese-internet-giant-accused-of-abusing-dominance>, 27 Oct 2011.
- Zhu, Shanshan. 2011. Attacks on Taobao end as authorities intervene. <http://www.globaltimes.cn/NEWS/tabid/99/ID/679496/Attacks-on-Taobao-end-as-authorities-intervene.aspx>, 17 Oct 2011.

**Part III**  
**E-Logistics**



# Chapter 6

## An Overview of China's Modern Logistics Development and Some Strategic Actions

Yimeei Guo and Cunlu Zhang

**Abstract** As part of the terms of its World Trade Organization (WTO) entry, China agreed to open market sectors and services that, in the past, were protected from global competition. The opening of the distribution and logistics sector is expected to spur the modernization of the sector over the next 3–5 years starting from 2001. This article plans to discuss the overall situation of China's distribution and logistics development especially focus on China's WTO entry's commitment; and point out the business risks for foreign companies. Finally, this article wants to suggest some strategic actions which foreign companies can adopt as the conclusion. Hopefully, this article may help foreign companies enter China's logistics market and do business smoothly.

**Keywords** China's distribution and logistics development · China's WTO entry's commitment · Strategic actions · E-Logistics

### 6.1 Introduction

China, the world's largest foreign direct investment (FDI) recipient, has maintained its attractiveness to foreign capital in 2004, despite the country's macroeconomic control policies. The country's FDI inflows hit US\$62 billion in 2004,

---

(Published by "Proceedings of 4th Academic Research Conference on Cross-Straits Industry Development and Operation Management", May 2, 2005, pp. B3-1–B3-9).

---

Y. Guo (✉)

Department of Management Science, Tulane University, New Orleans, USA  
e-mail: yime\_i\_guo@necmail.xmu.edu.cn

Y. Guo · C. Zhang

School of Management, Xiamen University, Jiageng Building 1, P.O. Box 953,  
Xiamen 361005, China

C. Zhang

Department of Management Science, Shanghai Jiao Tong University, Shanghai, China

compared with US\$53.5 billion in 2003, according to the World Investment Report (2004), released by the United Nations Conference on Trade and Development (UNCTAD) on January 12, 2005.<sup>1</sup>

Today, China is greatly concerned with and enthusiastic about the logistics industry. It could be said that logistics has become a new industry of great vitality and has caused high attention from various aspects of society including government institutes, manufacturers, wholesalers, logistics service providers, educational organizations, and research institutes.

As part of the terms of its World Trade Organization (WTO) entry, China agreed to open market sectors and services that, in the past, were protected from global competition. The opening of the distribution and logistics sector is expected to spur the modernization of the sector over the next 3–5 years upon accession, i.e., starting from 2001.

Nevertheless, the distribution and logistics sector remains highly fragmented, with strongly protected local interests. Although foreign companies often possess better management systems and technologies, knowledge of the local operating environment, culture, and customer needs helps local firms create and maintain competitive advantages.

This article plans to discuss the overall situation of China's distribution and logistics development especially focus on China's WTO entry's commitment; and point out the business risks for foreign companies. Finally, this article wants to suggest some strategic actions which foreign companies can adopt as the conclusion. Hopefully, this article may help foreign companies to enter China's logistics market and do business smoothly.

## 6.2 Review of the Literature—Trends in China's Distribution and Logistics

Distribution and logistics sector presents a significant challenge for companies doing business in China. Morgan Stanley (2001) estimates that China annually spends 20 % of its nominal gross domestic product (GDP), or US\$215 billion on logistics. This compares unfavorably with total logistics costs in the US market, which, at the end of 2000, were 10.1 % of nominal GDP, or US\$1,006 billions.<sup>2</sup> Morgan Stanley also predicts that the logistics sector in China will continue to grow at 20 % annum during the next 10 years.<sup>3</sup> According to an Economist Intelligence Unit report (December 2001), on average, 90 % of Chinese manufacturer's time is spent on logistics and 10 % is spent on manufacturing.<sup>4</sup>

---

<sup>1</sup> "China's FDI hit US\$62 billion in 2004, ranked No.2 and was only less than the United States", *Oriental Morning Post*, <http://gb.chinabroadcast.cn/7212/2005/01/13/1166@421174.htm>.

<sup>2</sup> Ho and Lim (2001).

<sup>3</sup> Australia the Pulse of Chinese Logistics (2002).

<sup>4</sup> Bolton and Wei (2003) at p.9.

Today, selling costs in China are significantly higher than those in the West. Annual working capital turnover (a measurement that compares the depletion of working capital [current assets minus current liabilities to the production of sales] over a specific time) in China is, on average, 1.2 times for manufacturing state-owned enterprises (SOEs) and 2.3 times for commercial SOEs. These figures compare with averages of 15–20 times in the USA. For many commodities, logistics costs are proportionally 40–50 % higher than they would be in the USA. Accounts receivable—a key measure of inefficient logistics practices—often exceed 90 days.<sup>5</sup>

Despite these weaknesses, China's distribution and logistics sector is growing rapidly. In fact, the logistics industry has reported annual revenue growth rates of 31 % for 1999, 35 % for 2000, and 55 % for 2001 and is forecasted to grow 50 % annually for the next 3 years.<sup>6</sup>

For example, as of 2003, China's logistics market has been as large as RMB ¥ 240 billion (\$29 billion), after just 2 years of expansion.<sup>7</sup> Also, the total value of China's domestic logistics in the first quarter of 2004 arrived at RMB ¥ 8.21 trillion (US\$993 billion), 31.7 % higher than the corresponding period in 2003, according to statistics from the National Logistics Information Center in 2004.<sup>8</sup> The sector has changed significantly as a result of overall market growth, evolving customer requirements, liberalization of government policies, and China's WTO entry.

### 6.3 Impact of WTO on Distribution and Logistics in China

The goal of the rules under the WTO is to help producers of goods and services, exporters, and importers conduct their business, while allowing governments to meet social and environmental objectives. The overriding purpose of the system is to encourage trade flow as freely as possible, so long as there are no undesirable side effects. In part, this means removing obstacles or barriers. It also means ensuring that individuals, companies, and governments know what the trade rules are around the world and giving them the confidence that there will be no sudden changes in policy. In other words, the rules have to be transparent and predictable.<sup>9</sup>

As a member of the WTO, China is to issue rules and regulations that fully comply with the above approach of the WTO, i.e., rules and regulations, including those in distribution and logistics that are transparent and predictable.

---

<sup>5</sup> Ibid.

<sup>6</sup> Bolton and Wei (2003) at p. 9.

<sup>7</sup> Wei (2004).

<sup>8</sup> "China's 1st-quarter logistics value totals US\$993b", Xinhua, May 12, 2004, [http://www.chinadaily.com.cn/english/doc/2004-05/12/content\\_330078.htm](http://www.chinadaily.com.cn/english/doc/2004-05/12/content_330078.htm).

<sup>9</sup> World Trade Organization (2001).

## 6.4 China's Market Access Commitments on Logistics and Distribution

### 1. *Transport*

- **Road transport**  
Foreign investors may establish joint ventures (hereinafter JVs) to handle freight transport by road upon accession. Majority-owned JVs and wholly owned subsidiaries will be allowed in the following year and **3** years, respectively.
- **Rail transport**  
Foreign investors may establish JVs to handle freight transport by rail upon accession. Majority-owned JVs and wholly owned subsidiaries will be allowed in **3** and **6** years, respectively.
- **Sea transport**  
Foreign investors may operate international sea freight and passenger service. Minority-owned JVs may register for operation under Chinese flag. Foreign investors may also set up JVs to operate auxiliary services such as cargo handling, container yard, and shipping agency.

### 2. *Freight Forwarding*

Foreign freight forwarders with at least **3** years of experience may establish freight-forwarding JVs upon accession. Majority-owned JVs and wholly owned subsidiaries will be allowed in **1** and **4** years, respectively. JVs which have been in operation for **1** year or more may open branches. At present, a foreign freight forwarder with a JV in China for **5** years may set up a second JV. This requirement will be relaxed from **5** to **2** years.

### 3. *Storage and Warehousing*

Foreign firms may establish warehousing JVs in China upon accession. Majority-owned JVs and wholly owned subsidiaries will be allowed **1** and **4** years after accession, respectively.

### 4. *Courier Service*

Foreign firms may hold minority shares in forming JVs upon accession. Majority-owned JVs and wholly owned subsidiaries will be allowed in **1** and **4** years, respectively. JVs may provide postal services using one or more transport modes, except those services monopolized by the Chinese postal authorities.

### 5. *Road and Water Transport Infrastructure*

Foreign firms may set up majority-owned JVs upon accession. Wholly foreign-owned enterprises will be allowed 3 years after accession, but certain limitations on the scope of contracts will remain.

### 6. *Port Facilities*

Foreign firms may form JV shipping companies to provide international passenger and cargo services, with foreign equity capped at 49 %. Foreign investors may also

set up JVs to offer shipping agency, cargo handling, and container yard services. Foreign vessels may have access to port facilities in China. Wholly foreign-owned vessel inspection service will be allowed 4 years after accession.

In the meantime, wholly foreign-owned enterprises can undertake infrastructure projects related to water transport on a conditional basis. According to the latest "Catalogue for the Guidance of Foreign Investment Industries" which took effect on April 1, 2002, Chinese majority shareholding is no longer required for the operation of public wharves.

In keeping with China's WTO commitments, the majority of projects relating to logistics development are classified as encouraged. Only a small number of them are listed under the restricted and prohibited categories:

7. Encouraged

Construction and operation of rail trunk lines (Chinese majority shareholding required); railway branch lines, local railways and connecting bridges, tunnels and ferry service (restricted to JVs only); roads, bridges, and tunnels; public wharf facilities; civilian airports (Chinese majority shareholding); warehousing facilities related to transport service. Freight service by road and air (Chinese majority shareholding); general aviation service for agricultural, forestry and fishery sectors (restricted to JVs only); scheduled and non-scheduled international sea transport service; and international, inter-modal container freight service. Multimedia is popular.

8. Restricted

Cross-border trucking, water transport, rail freight, and agency business (shipping, freight service, cargo handling on board foreign vessels, and advertising, etc.).



Fig. 6.1 Logistics services subsectors. Source Loo (2002)

**Figure II: China's liberalization measures**

Pre-WTO Accession Barriers and Rules	Terms of WTO Agreement
<p style="text-align: center;"><b>Freight Forwarding</b></p> <p>Foreign freight forwarders can have no more than a 50% share in JVs and require an investment of no less than US\$1 million. Foreign partners have to be in business for a minimum of three years to qualify for a first JV.</p> <p>Required to observe a five-year waiting period for forming a second JV, and a one-year waiting period for establishing branches. An additional investment of US\$120,000 is required for each additional branch.</p> <p>The business of JVs is limited to certain geographical areas.</p> <p>Very few JVs are allowed to handle domestic freight forwarding.</p>	<p>Majority ownership in JVs allowed <b>1</b> year after accession.</p> <p>Wholly owned subsidiaries allowed <b>4</b> years after accession.</p> <p>JVs are not limited to conduct international freight forwarding business only.</p>
<p style="text-align: center;"><b>Storage &amp; Warehousing</b></p> <p>Foreign firms are permitted to own warehouses only in foreign trade zones (FTZs), provided that such warehouses are used to store materials necessary to their own production and service activities in China.</p> <p>Outside the FTZs, foreign firms are not permitted to own or manage warehouses.</p>	<p>Foreign service suppliers are permitted to establish as minority-owned JV upon accession and hold a majority equity share within <b>1</b> year.</p> <p>Restrictions to be phased out within <b>3</b> years.</p>
<p style="text-align: center;"><b>Express Operator</b></p> <p>Prohibited from taking a majority share in a JV, and required to invest no less than US\$1 million in an entity whose term may not exceed 20 years.</p> <p>A waiting period of one year for establishing branches and five years for forming a second JV.</p>	<p>Commitments cover land-based international courier services and all services related to an international shipment handled by an express carrier.</p> <p>Majority ownership in JVs allowed within one year. Wholly-owned subsidiary allowed <b>4</b> years after accession.</p>
<p style="text-align: center;"><b>Transportation (ground)</b></p> <p>Only Chinese nationals and Chinese-owned companies are permitted to conduct surface transportation.</p> <p>Foreign participation for cross-boundary operations with Hong Kong requires JV partnership.</p>	<p>For road transport, foreign service supplier will be able to establish as JV upon accession, hold a majority equity share within <b>1</b> year, and be free of restrictions within three years.</p> <p>For rail transport, foreign service suppliers will be able to establish as JV upon accession, hold a majority equity share within two years, and be free of all restrictions within <b>6</b> years.</p>

**Fig. 6.2** China's liberalization measures. *Source* Loo, *ibid*

### 9. *Prohibited*

Although postal service is classified as prohibited, foreign investors may still invest in market segments that are not reserved for the Chinese postal authorities. For instance, courier service is open for foreign participation. In fact, DHL, UPS, and FedEx are already operating in the China market. Further, a series of new measures adopted in recent years on foreign investment in water transport, rail cargo transport, and freight forwarding marked the gradual relaxation of certain activities under the restricted category (Figs. 6.1 and 6.2).<sup>10</sup>

## 6.5 China's Market Access Commitment with Regard to Distribution

In the USA–China bilateral WTO agreement, China's commitment with regard to distribution is comprehensive, covering commission agents' services, wholesaling, retailing, and franchising. In each of these sectors, commitments on market access, national treatment, and other areas have been made under which there are four forms of supplying services, including cross-border delivery, offshore consumption, commercial presence, and movement of natural persons.

Market access is the most crucial of all issues. China agrees to gradually liberalize the wholesaling and retailing of all but a few commodities within 5 years of accession. Quantitative, geographical, equity, and incorporation restrictions on the establishment of JVs by foreign companies will also be phased out. This is bound to have a considerable impact on China's distribution enterprises, but will also bring them a host of business opportunities.<sup>11</sup>

In line with its commitments to the WTO, China will further reinforce its opening up of the retailing sector. After December 11, 2004, restrictions on geographical location, equity participation, and the number of foreign-invested retail enterprises were removed.

By now, most of the multinational retail giants have entered China. In 2003, the annual revenue of Carrefour reached RMB 13.4 billion (USD 1.62 billion), an increase of 25.7 % over the previous year. Walmart has opened 33 branch stores in China, and its annual sales reached RMB 5.85 billion (USD 708 million) in 2003.

Experts indicated that foreign investment in the retailing sector is still very low in China. Foreign-invested retailing is mostly concentrated in the eastern part of China and is mostly in the form of hyper-markets.

As the opening up gradually takes place, there will be more types of retailing and more companies in the central and western part of China, whereas the Deputy Minister of Commerce, Mr. Zhang Zhigang, pointed out that currently, the

<sup>10</sup> WTO Entry Unleashes Greater Opportunity and Competition in Logistics Sector (2002).

<sup>11</sup> China to Fully Liberalize Its Distribution System (2000).

logistics industry in China is still relatively weak. The opening up of the retail industry will impact the logistics industry and bring new opportunities to it.<sup>12</sup>

## 6.6 China's Logistics Barriers Is Scheduled to Be Knocked Down in 2005

The year 2005 should prove to be an extraordinary year for the logistics industry. According to its WTO agreements, China will completely open its logistics market. In 2005, China will grant international companies equal footing in its domestic logistics market. China is also a signatory to "Closer Economic Partnership Arrangement (CEPA)," along with Hong Kong and Macao, and has opened the services market to the two regions.

The Ministry of Commerce officially issued "Provisions on the Establishment of Investment Companies by Foreign Investors" on June 27, 2004. According to the provisions, as a prelude to the complete opening of the logistics industry in 2005, foreign investors will be able to establish investment companies and invest in outsourcing of services, purchasing, and logistics in China. Meanwhile, the provisions also say that these investment companies can hold non-tradable corporate shares of domestic enterprises.<sup>13</sup>

## 6.7 Foreign Players Jostling for Position

Many of the world's leading logistics giants have been in business in China for many years. These foreign firms have been operating in the mainland in the following three areas:

### 1. *Third-party logistics (3PL)*<sup>14</sup>

Many foreign firms team up with Chinese partners in offering 3PL services. For instance, Mitsui OKK Lines (MOL) of Japan and Fuji jointly operate a logistics and warehousing company in Suzhou to take care of all the logistics involved in making the Fuji film available across the China market. UPS's JV logistics

---

<sup>12</sup> "Complete opening-up of retail industry to foreign investors" *Xinwen Morning Post*, March 17, 2004, edited by CS Shanghai, cited from China Commercial Brief—March 19, 2004, Vol. 2 No. 154, issued by the U.S. Commercial Service—American Embassy, Beijing. <http://www.mac.doc.gov/china/CommBriefArchive.html>.

<sup>13</sup> See *supra* note 7.

<sup>14</sup> Third-party logistics (3PL or TPL) refers to logistics provided by a third party other than the service provider and end user. 3PL enterprises mainly provide clients with sea and air freight rail and road transport services.



company plans to open 19 offices in China. DHL and Sinotrans have extended their JV agreement by 50 years.

Other foreign companies such as Exel Logistics, TNT, and Nippon Express are setting up offices or negotiating JV deals in Shenzhen and Guangzhou. The US\$30 million logistics JV between TNT and Shanghai Automotive Industry Corp (Group) is the first of its kind in China specializing in the automobile sector. APL Logistics has formed JVs with two local transport giants in Shanghai and Shenyang to develop the mainland logistics market. APL Logistics currently has branch companies in 7 cities along the southeastern coast, with plans to expand to 12 cities over the next 2 years.

While many foreign companies team up with local partners, some prefer to go it alone. Typically, these companies provide 3PL service to foreign and domestic companies. The Maersk Group, since receiving the green light to enter the China market in 2001, has set up 11 branches across the country. It has also opened its first distribution center in Shanghai, with plans to set up 10 more. Meanwhile, Nippon Express has formed logistics companies in Dalian, Shenzhen, and Shanghai to facilitate business expansion in China. NYK Lines (China) has also established a branch in Shanghai and is now moving to set up logistics companies in Tianjin, Qingdao, Fuzhou, Xiamen, Guangzhou, and Dalian. OOCL has located its China headquarters in Shanghai with 21 offices all over the country.<sup>15</sup>

Foreign companies with strong international networks and better management are gaining market share, while many domestic companies rely on underdeveloped domestic operations. And local and regional distribution systems are replacing state-owned and centrally managed trading and distribution systems.

According to a report, jointly published by the China Federation of Logistics and Purchasing and Mercer Management Consulting (2002), the outsourcing of logistics and transportation will continue to expand by roughly 25 % annually through 2005 because of stronger global interest and demand for third-party services. Multinational companies (MNCs) relying on China as a global sourcing base are inclined to use—and are experienced in using—third-party services, especially those of third-party providers. More than 90 % of MNCs in China currently contract at least a portion of their logistics business to third parties.

Though the concept of outsourcing, these basic logistics functions are still relatively new to most Chinese companies, many leading foreign firms in China—such as McDonald's Corp. and Dell Computer Corp—have demonstrated great success by using third-party service providers' expertise, capabilities, and assets to offer nationwide distribution and logistics service. These foreign companies have shown Chinese companies that they do not need to own all of the assets involved in service provision to gain the capability and expertise to offer a full line of services.<sup>16</sup>

---

<sup>15</sup> See *supra* note 8.

<sup>16</sup> Bolton (2004).

## 2. *Own logistics system*

German retail group Metro has 15 distribution centers in China with 3 more on the drawing board. Mitsubishi is constructing an all-in-one distribution center in Guangdong. Siemens has set up a specialized logistics company in Beijing. Also in Beijing, retail giants such as McDonald's, KFC, and Ito Yokado have their own distribution centers.

## 3. *Fourth-party logistics (4PL)*<sup>17</sup>

Exel, the world's second largest logistics group, has teamed up with Tengfei Co to provide 4PL services to business operators in Nokia's Xing Wang Industrial Park.

# 6.8 Domestic Players Meeting WTO Challenge

Facing the WTO challenge and growing competition from foreign logistics companies, China is making great efforts to improve its market environment, strengthen infrastructure construction, expedite the consolidation and retooling of traditional logistics resources, and promote the development of 3PL companies and distribution centers through corporate restructuring and stock market listing.

## 1. *Building mega logistics parks*

Shanghai is understood to be giving priority to the development of three large-scale logistics parks, namely Waigaoqiao, Pudong Konggang, and Xibei, during its tenth five-year plan period. Among these, Xibei is the logistics hub through which goods from Shanghai are distributed by land to the Yangtze River delta region and inland provinces. At present, 936 logistics enterprises are operating in the Xibei park with a total warehousing area of 600,000 sqm. Tenants of the park include such large logistics enterprises as APW of the USA, Schneider of France, Marubeni of Japan, T. Join of Taiwan, Dazhong Transportation, Hualian Distribution Centre, and PG Logistics. The other two logistics parks have also attracted renowned international players such as APL, Maersk, Marubeni, UPS, FedEx, TNT, and DHL.

Beijing plans to form a highly effective logistics platform by 2010 serving not only the whole city but also the adjacent Bohai rim. The platform will initially

---

<sup>17</sup> Fourth-party logistics (4PL or FPL) provider acts as an integrator of functions not covered by 3PL. Due to the growing popularity of global supply chain management, the services provided by 3PL alone may not be comprehensive enough. In order to offer speedy and effective services, 3PL providers must collaborate with others, namely 4PL, in order to boost their own capabilities. 4PL has the following characteristics: 1. As an integrator, it controls the point-to-point supply chain operations with client companies through subcontractors. 2. It provides integrated solutions for the supply chain. 3. It organizes the integration and implementation of the supply chain solutions. 4. As a supply chain integrator, it exercises central management of its own resources, capabilities, and technologies and those of complementary service providers.

consist of 3 logistics bases, 4 logistics distribution areas, and 13 specialized distribution centers. At present, three facilities—Jingtai logistics port, Tongzhou Logistics Park, and Xinan logistics base—are being planned and constructed.

In fact, logistics parks are on the drawing boards of a number of large cities including Guangzhou, Shenzhen, Tianjin, Wuhan, Chongqing, Dalian, Fuzhou, and Xiamen. All these cities are striving to turn logistics into a pillar of the local economy.

### *2. Turning traditional enterprises into specialized logistics operations through resource redeployment and transformation*

Since Zhonghai Group founded Zhonghai Logistics in 2000, it has established another company in Shanghai and eight regional operations across the mainland. Through resource redeployment, the company has shifted its focus from internal trade services to foreign trade-related logistics services and from traditional freight forwarding to 3PL.

In January 2002, China Overseas Shipping Company (COSCO) formed COSCO Logistics. More recently, it teamed up with Kelon and Little Swan in a tripartite logistics JV. COSCO is also understood to have plans for a 3PL JV with Haier. Meanwhile, Guangdong Post has set up Guangdong Post Logistics Co, the first of its kind to be formed by a postal authority in China. Other enterprises are also making great efforts to transform from traditional to modern, integrated logistics service providers.

### *3. Forming JVs with foreign players to tap both domestic and world markets through introduction of foreign capital, advanced technology, and management know-how*

In April 2002, Chang'an Automobile Group of Chongqing, Minsheng Industrial Group, and APL Logistics formed a JV, Chongqing Chang'an Minsheng Logistics Co. The JV aims to capitalize on logistics opportunities in China's southwestern region arising from the "Go West" initiative. Meanwhile, China Railway International Freight Forwarding, Lanzhou Railway Bureau Container Transport Co, and three of the bureau's container subsidiaries have concluded a JV agreement with Canadian Pacific Railway to form a logistics company.

Rilu Wailianfa Logistics (Shanghai), a JV between Chinese and Japanese parties, is the first dangerous goods logistics enterprise in China. Tsingtao Beer and China Merchants Logistics of Hong Kong established a JV in early 2002. COSCO and Japan Post have agreed to cooperate on developing logistics services in their respective markets and world markets, personnel training, and other business areas.

### *4. Developing modern logistics through assets optimization on the financial market*

At present, about 40 listed companies in China are involved in logistics. Some of these companies have already entered the 3PL market by drawing on their own strengths in terms of capital, management know-how, and technology. In early

2002, Shenzhen Energy Group announced that its 40 %-owned Shenzhen Energy Logistics will be making a foray into the 3PL market. Meanwhile, chinese.com has also undergone a series of share transfers to optimize its assets. The company plans to offer integrated logistics service to clients based on e-commerce applications. Enterprises in other sectors are also mooting similar moves, including retail groups, such as Hualian Supermarket and Chengda of Liaoning, and manufacturing giants such as Tsingtao Beer, Haier of Qingdao, and Yanjing Beer.<sup>18</sup>

## 6.9 Foreign Business Risks in China

### 1. *Potential Delays in WTO Rule Implementation*

More than 80 % of Fortune 500 companies have already invested in China. However, small- and medium-sized foreign companies are just now entering the country. But regardless of the depth of their experience in China, all companies face ongoing risks in the regulatory, political, and market arenas. One such risk involves WTO commitment delays. China may delay WTO implementation and regulate competition to help local companies compete in the market.

As other WTO members have done, China also may work around WTO rules to maintain barriers against imports, for example, by erecting WTO-compatible non-tariff barriers, such as licensing, health, technical, and packaging standards. In 2003, China released a draft regulation that would require “one license, one product” dealership licenses in the auto sector. These would prevent newcomers from using existing distribution channels and give local manufacturers more time to prepare for direct competition.<sup>19</sup>

### 2. *Regulatory Fragmentation*

Another important risk is regulatory fragmentation. China’s distribution and logistics industry has been micro-regulated for years, with different logistics service components governed as distinct subsectors by various government departments. For example, the Ministry of Communications governs land and waterway transportation; the Ministry of Commerce administers trading rights and international freight-forwarding licenses; and the General Administration of Customs of the People’s Republic of China (PRC) controls brokerage services.

Despite central government efforts to promote coordination, this shared jurisdiction system is unlikely to disappear quickly, so companies still must acquire separate licenses through various governing bodies to undertake different activities. Look at the Table 6.1.

---

<sup>18</sup> See supra note 16.

<sup>19</sup> See supra note 4 at p.13.

**Table 6.1** Regulatory framework for foreign participation in subsectors

Subsector	Foreign participation encouraged/regulated	Related authority for license approval
International freight forwarder	Regulated	MOFCOM
Air freight forwarder	Regulated	CAAC, MOFCOM
Logistics center	Encouraged	MOC, MOFCOM
Domestic trucking	Regulated	MOC, MOFCOM
Consolidation	Regulated	MOC, MOFCOM
Warehousing	Encouraged (sole-owned enterprise possible)	MOC, MOFCOM
Customs brokerages	Heavily regulated	CGA, MOFCOM
Shipping line	Regulated	MOC, MOFCOM
Airline	Heavily regulated	CAAC, MOFCOM

*Abbreviations* MOFCOM—Ministry of Commerce, CAAC—Civil Aviation Administration of China, MoC—Ministry of Communications, CGA—Customs General Administration  
*Source* Loo, *ibid* and some modifications by Guo, Yimeei

### 3. Lack of Enforcement Capability and Local Protectionism

Lack of enforcement capability and local protectionism also can cause problems. China's governing structure encompasses multiple layers of central and local governments. Despite central government efforts to liberalize the market, local-level interpretation and enforcement of laws and regulations can often be arbitrary and inequitably disposed toward local interests.

### 4. Large Fluctuations in Capacity and Demand

Business risks associated with fluctuating capacity and demand are yet another concern. China has one of the most dynamic markets in the world, making errors in market demand forecasts more frequent and severe than those in other areas. In addition, almost all major cities and regions in China have invested in some form of distribution or warehousing center or logistics park. But, according to research conducted by the China Storage Association in 2002, 60 % of the country's logistics centers are empty. Lastly, social and political risks must be considered.<sup>20</sup>

### 5. Not Quite Ready for the Revolution in e-Logistics

Rosen (1999) suggested that a closer electronic linkage to global supply chain might foster export growth.<sup>21</sup> While the Internet, and the need to regulate e-commerce via the Internet, has made the process of drawing up new law more

<sup>20</sup> See *supra* note 4 at p.13.

<sup>21</sup> Rosen (1999).

complex,<sup>22</sup> it is also the case that the uneven use of the Internet in China may itself prove to be a barrier to the country-wide management of logistics.<sup>23</sup>

A survey by the China Internet Network Information Center (CNNIC) showed that the number of WWW Web sites Establishes in different provinces and municipalities as on January 19, 2005, varied greatly. Beijing, the capital, had the highest number of Web sites in China at 125,297, i.e., 18.7 % of all Web sites in the country. This figure was 270.6 times that of Qinghai. The top ten places including Guangdong, Zhejiang, Jiangsu, Shanghai, and Fujian comprised 82.4 % of the total number of Web sites in China.<sup>24</sup>

## 6.10 Conclusions and Recommendations

Generally speaking, China has seen spectacular growth over the last few years as a result of ongoing liberalization of the market and acceptance into the global economy. The logistics industry has been one of the main beneficiaries of this phenomenon, with forwarders, 3PL providers, airlines, and shipping lines struggling to meet demand. However, despite the hype surrounding exponential growth rates, there are still huge challenges in doing business in China.

To take advantage of China's soaring economy, global transport and logistics companies are investing billions in infrastructure, acquisitions, and operations. However, as well as offering huge opportunities, the market is one of the most difficult into which to break. Regulations, culture, weak infrastructure, and an undeveloped industry are just some of the problems being faced by companies. Without a basic understanding of the country, its markets, its logistics sectors, and potential partners, doing business in China is impossible.

In detail, foreign companies planning to enter China through a partnership or joint venture must be extremely careful about their potential partners' visible and invisible liabilities. For example, protecting local employment is a high priority for PRC governments, so appropriate benefits for excess workers can be a huge issue in contract negotiations. Deft handling of corruption (particularly common at local levels) also is essential.

As some successful companies are proving, effectiveness in distribution and logistics helps to achieve market share and profitability growth in China. However, to realize the true potential of the burgeoning China market, a great deal of homework and due diligence is still essential.

---

<sup>22</sup> For a thorough discussion on this part, see, e.g., Chan (2002) at pp. 64, 65, Jimmy (2004) at p. 14.

<sup>23</sup> Jimmy Ng, *supra* note 21 at p. 12.

<sup>24</sup> "CNNIC 15th Report: WWW Web Sites Number", Jan 19, 2005, <http://it.people.com.cn/GB/8219/43564/43565/3131007.html>.

### 1. *Seeking Deep Knowledge of the Market*

First and foremost, companies must work to understand this radically different market. Contrary to what some experts think, cost and time concerns will limit the swiftness with which shippers develop their own sales and distribution approaches once China fulfills its WTO commitments in distribution services. Instead, smart players will work to enhance the capabilities of the PRC distributors with which they already have relationships.

They also will pay attention to regional and local particulars and acknowledge the intense emphasis that Chinese companies place on relationships. Every city or investment zone has different policies designed to attract certain types of foreign investment. Some zones provide local tax incentives, land leasing, and lower utility fees. For example, Xiamen Xiangyu Bonded Zone has already applied to establish the nation's second zone-port interaction area to follow Shanghai, which was selected as a pilot in 2003.<sup>25</sup> Therefore, a well-connected and trustworthy local partner also is important.

### 2. *Focusing on Value*

The need to focus on value is a second key strategy. Companies should bypass inefficient parties and middlemen—thereby removing unnecessary layers of bureaucracy and streamlining distribution chains. This is already happening in many industries, such as personal computers and consumer electronics. Nokia and Dell, for example, have sidestepped the widely used industry distribution model that follows a “manufacturer, general agent, regional distributor, second tier distributor, retailer, consumer” pattern. Instead, it supplies large regional distributors and retail outlets directly, thus cutting distribution costs and raising market responsiveness.

### 3. *Streamlining Distribution and Logistics*

Companies and their distributors must integrate, centralize, and streamline distribution and logistics functions, assets, infrastructure, staff, and operations. The long-term goal is for the supply chain to become a separate—yet shared—organization across different business units. Few companies can build or provide a full range of distribution services alone, which is why it is vital to build partnerships and alliances with local distribution service providers.

---

<sup>25</sup> A zone-port interaction area is a combination between bonded land and a nearby international port. A bonded logistics zone will usually be set up in a port area. The combination will benefit enterprises in the former bonded zone by offering better logistics services, helping solve the bottleneck affecting China's bonded zones. But what seems most attractive to firms should be an updated tax rebate mechanism. Rebates will be granted upon the entry of domestic goods into zone-port areas, rather than the current practice of providing refunds after those goods leave China. See Zhang Jin “Xiamen bonded zone targets free trade area”, China Daily, August 6, 2004, [http://www.chinadaily.com.cn/english/doc/2004-08/06/content\\_363197.htm](http://www.chinadaily.com.cn/english/doc/2004-08/06/content_363197.htm).

#### 4. *Avoiding Duplicating Services*

By focusing on improving flows, companies' distribution and logistics functions in China can be based more on the transmission of reliable and timely information and less on direct control of the physical movement of consignments. To help make this happen, they also must emphasize the creative use of technology.

#### 5. *Using Technology as a Key Differentiator*

The distribution and logistics sector in China is typically slow to adopt new technologies, partly because of the complexity and cost of setting up an integrated information technology (IT) platform. For instance, the lack of cargo tracing services has been identified as one of the most serious problems in China, and it could be attributed to the lack of telecommunication and information technologies needed to track cargo during delivery and transit.<sup>26</sup>

Growth of the sector will require particularly great sophistication in supply chain planning, product visibility, and end-to-end supply chain integration.

#### 6. *Managing Risk Effectively*

A company's ability to recognize the many risks of conducting business in China, and to plan for them, can spell the difference between success and failure. The companies that understand the baseline cost structure and motivations of their distribution and logistics operation, and track the total cost, will be in a better position to mitigate risks.

#### 7. *Building and Retaining Talent for Long-Term Success*

Finally, there will be an exceptional need to build and retain talent for long-term success. According to a survey by the Logistics Institute—Asia Pacific and The Logistics Institute of the Georgia Institute of Technology (2002), a premier obstacle to operating in China is lack of talent. Value-added services in distribution and logistics require more expertise than most PRC providers currently possess. In fact, some observers believe that 85–90 % of failed distribution initiatives were caused by workforce error. For the foreseeable future, training will be an integral part of any company's relationship with a PRC distribution service provider.<sup>27</sup>

## References

- Australia the Pulse of Chinese Logistics. 2002. Issued by Austrade (Australian Trade Commission), October 15, [http://www.pulse.com.au/news\\_detail.asp?NewsID=109&Source=News](http://www.pulse.com.au/news_detail.asp?NewsID=109&Source=News)
- Bolton, Jamie M. 2004. Supply chain management in China, July 2004. <http://www.accenture.com/xd/xd.asp?it=enweb&xd=industries%5Ccommunications%5Caccess%5Csc29.xml#top>

<sup>26</sup> Felix W.H. Chan, *supra* note 21 at p.63.

<sup>27</sup> Bolton and Wei (2003), pp. 13–17, See Bolton (2004)



- Bolton, Jamie M., and Yan, Wei. 2003. Distribution and logistics in today's China. *China Business Review*: 8–17.
- Chan, Felix W.H. 2002. The dynamic legal landscape for logistics management in China. *Asia Business Law Review* 37: 61–67.
- China to Fully Liberalize Its Distribution System. 2000. Business alert—China, Issue 06, June 15, <http://www.tdctrade.com/alert/cba-e0006b.htm>
- CNNIC 15th Statistical Survey Report on the Internet Development in China, published on January 15, 2005, <http://www.cnnic.net.cn/download/2005/2005012701.pdf>
- He, Mingke. 2004. Opportunities for the development of China's purchasing. Business Briefing: Global Purchasing & Supply Chain Strategies, pp. 8–17.
- Ho, H., and Lim, C. 2001. China logistics: spot the early bird. Morgan Stanley, pp. 20–21.
- Loo, David. 2002. China's logistics industry presents a golden opportunity. Feb 28. <http://www.tdctrade.com/imn/02022803/markettrends17.htm>
- Ng, Jimmy. 2004. Barriers to e-commerce logistics in China [Legal Aspects]. UNEAC Asia Papers No.7, pp. 1–18.
- Rosen, D. 1999. Hype versus hope for e-commerce in China. *China Business Review* 26(4): 38–42.
- Wei, Tan. 2004. Moving the goods. [http://www.bjreview.com.cn/200429/Business-200429\(C\).htm](http://www.bjreview.com.cn/200429/Business-200429(C).htm)
- World Trade Organization. 2001. Trading into the future: WTO The World Trade Organization, 2nd Ed.
- WTO Entry Unleashes Greater Opportunity and Competition in Logistics Sector. 2002. Business alert—China, Issue 08, August 15, <http://www.tdctrade.com/alert/cba-e0208sp.htm>
- Zhang, Jian Wei. 2001. Logistics in China. presented at WOF 2001, DBMJ, pp. 31–34.

# Chapter 7

## Barriers and Legal Solutions to e-Logistics in China

Yimeei Guo and Jinquan Tang

**Abstract** In 2004, the World Investment Report observes the trend of the changes of interest of foreign investment from manufacturing to service industry. In early 1970s, only 1/4 of foreign direct investment (FDI) went to the service industry. Now, it has soared to 60 %, or USD\$440 million. The structure of the FDI in the service industry has also changed. Traditionally focused on trade and finance, foreign capital now has developed better appetite toward power, telecommunication, water service, and various commercial sectors. China's logistics is certainly one of them and receives much more attention than ever after China's WTO entry. After December 11, 2004, China has opened up its logistics industry to overseas competition, in keeping with its WTO commitments. China's entering into the WTO has inspired a wave of reforms in existing laws and regulations, including laws in e-commerce. There is no formal, centralized regulation of e-commerce, but beginning from 2000, some government agencies and some local governments have begun to issue regulations specifically targeted at the Internet, but without coordination this effort is creating a patchwork of rules. On August 28, 2004, the Standing Committee of the 10th National People's Congress enacted the "Electronic Signature Law of the People's Republic of China" ("E-signature Law"), effective April 1, 2005, to boost electronic business, which for the first time legalizes increasing electronic deals. The law grants electronic signatures the same legal effect as handwritten signatures and seals in business transactions, and setup the market access system for online certification providers to ensure the security of e-commerce. While the Internet, and the need to regulate e-commerce via the Internet, has made the process of drawing up new laws more complex, it

---

(Published by "Proceedings of The KIECA International Conference 2005 on Trade, Investment, Logistics & E-Biz," Korea Internet e-Commerce Association (KIECA), 2005. 10.1, pp. 333~345.)

---

Y. Guo (✉)  
Management Science Department, Xiamen University, Xiamen 361005, China

J. Tang  
Management Science Department, Minjiang College, Fuzhou 350108, China

is also the case that the uneven use of the Internet in China may itself prove to be a barrier to the countrywide management of logistics. Therefore, this article plans to discuss some barriers to e-logistics in China, especially from legal perspectives and introduces some legal solutions thereafter. Finally, this article wants to conclude that China has to be sensitive and responsive to changes in rules and regulations that will cause uncertainties and lead to a decline in confidence in its information and communication technology (ICT) and logistics industries.

**Keywords** WTO · e-Commerce · Barriers to e-logistics · Legal solutions

## 7.1 Introduction

In 2004, the World Investment Report observes the trend of the changes of interest of foreign investment from manufacturing to service industry. In early 1970 s, only 1/4 of foreign direct investment (FDI) went to the service industry. Now, it has soared to 60 %, or USD\$440 million. The structure of the FDI in the service industry has also changed. Traditionally focused on trade and finance, foreign capital now has developed better appetite toward power, telecommunication, water service, and various commercial sectors.<sup>1</sup> China's logistics is certainly one of them and receives much more attention than ever after China's WTO entry.

Even though most of the companies are small in comparison with their overseas counterparts, and the whole industry is still in its early stages of development, the size of the mainland's logistics industry was worth around RMB 60 billion (US\$7.22 billion) in 2003 and is expanding at a rate of 30 % year-on-year.<sup>2</sup>

The value of China's logistics and related markets has exceeded RMB 2 trillion (US\$242 billion), and there are 730,000 logistics enterprises in operation. In 2003, China's logistics industry realized RMB 788 billion of added value, up 10.5 % over that of the previous year and 1.4 and 3.8 % higher than growth rates of gross domestic product and the service industry in the same period.

The International Monetary Fund (IMF) predicted the market share of the logistics industry in China will rise to RMB 1 trillion (US\$120 billion) in value by 2010, compared with the RMB 461.8 billion (US\$55.6 billion) in 1999.<sup>3</sup>

In 2003, the China Logistics Information Center (CLIC) reports, the highway transport sector grew 2.5 % to handle 11.4 billion tons of cargo; rail transport, 6.5 % to 2 billion tons; water transport, 10.6 % to 16 billion tons; and air transport, 7.4 % to 2.17 million tons.

---

<sup>1</sup> "China's better than its words on its WTO commitment," People's Daily Online, [http://english.people.com.cn/200409/23/eng20040923\\_158035.html](http://english.people.com.cn/200409/23/eng20040923_158035.html).

<sup>2</sup> Statement of Ministry of Commerce (MOCOM) vice minister Zhang Zhigang at a conference in Beijing in November 2004. See Nuo (2004).

<sup>3</sup> "Logistics business soaring in China," Xinhua, [http://www.chinadaily.com.cn/english/doc/2004-11/08/content\\_389561.htm](http://www.chinadaily.com.cn/english/doc/2004-11/08/content_389561.htm).

In addition, according to the “2004 Chinese Circulating Industrial Development Report” released by the Ministry of Commerce and the Development Research Center (DRC) of the State Council in Beijing on April 13, 2005, the circulating industry, which mainly consists of wholesale, retail, and other-related sectors, has played an important role in fueling the country’s economic development and has maintained rapid growth. Among them, the added value of China’s logistics industry accounts for 8 % of the country’s GDP.

However, in contrast, as Huang Hai, assistant to the Ministry of Commerce (MOC) Minister, puts it: “Low efficiency in the circulating industry is a hard nut to crack. China’s logistics cost is two times as high as that in developed countries. In addition, Chinese logistics companies are less well organized with few links and are seldom grouped, which prevents them from becoming internationally competitive. Few circulating companies have adopted advanced technologies, such as e-commerce.”<sup>4</sup>

For example, the high cost of logistics is a severe impediment to the growth in international investment and trade in Shanghai according to China Transport News. A recent survey of 170 Shanghai-based trading companies shows that, despite the mainland’s inexpensive labor, their costs in procurement, transport, and finance are higher than those for similar operations in the USA by as much as 40 %. The publication also reported that, by lowering its logistics costs by 1 % point per unit, Shanghai could gain more than US\$5 billion in import and export revenues.<sup>5</sup>

## 7.2 Impact of WTO on China’s Logistics and Distribution Industry

The complexity of the legal regime is always an issue in logistics management in China. Law and regulations relating to logistics management are enforced by more than one governmental ministry or bureau in China.<sup>6</sup> An outline of the status of the different services and their licensing authorities is given in Table 7.1.

On the one hand, bureaucracy is basically intended to resolve conflicts among different interest parties, i.e., consumers, entrepreneurs, labor, other producers, and environment. But on the other hand, it could create more hurdles for those parties. Multinational logistics operators may spend months, if not years, applying for the necessary operating licenses and permits, which are issued by different government ministries, departments, or bureaus. FDI will continue to be introduced into China only if foreign investors are protected from bureaucratic red tape and the uncertainty of political risks by an increasingly improved legal framework.<sup>7</sup>

<sup>4</sup> “China’s logistics cost twice that of advanced countries,” <http://61.135.142.194:89/gate/big5/www.chinanews.cn/news/2004/2005-04-14/3301.shtml>.

<sup>5</sup> You Nuo, *supra* note 2.

<sup>6</sup> See ‘Chap. 12—Distribution—Sect. 3: Transport options,’ Economist Intelligence Unit, 13 December 2001: Distribution sectors with foreign participation involve four different government departments in China.

<sup>7</sup> Chan (2001).

**Table 7.1** Regulatory framework for foreign participation in distribution

Sub-sectors	Foreign participation	Authority for license approval
International freight forwarding	Regulated	MOFCOM
Airfreight forwarding	Regulated	CAAC, MOFCOM
Logistics center	Encouraged	MOC, MOFCOM
Domestic trucking	Regulated	MOC, MOFCOM
Consolidation	Regulated	MOC, MOFCOM
Warehousing	Encouraged	MOC, MOFCOM
Customs brokerage	Heavily Regulated	CGA, MOFCOM
Shipping line	Regulated	MOC, MOFCOM
Airline	Heavily Regulated	CAAC, MOFCOM

*Abbreviations*

MOFCOM—Ministry of Commerce, CAAC—Civil Aviation Administration of China, MOC—Ministry of Communications, and CGA—Customs General Administration

*Source* Hong Kong Trade Development Council, EIU with some modifications by Yimeei, Guo

The goal of the rules under the WTO is to help producers of goods and services, exporters, and importers conduct their business, while allowing governments to meet social and environmental objectives. The overriding purpose of the system is to encourage trade flow as freely as possible, so long as there are no undesirable side effects. In part, this means removing obstacles or barriers. It also means ensuring that individuals, companies, and governments know what the trade rules are around the world, and giving them the confidence that there will be no sudden changes in policy. In other words, the rules have to be transparent and predictable.

The government's ambitions, as laid out in the Five-Year Plan, in accordance with the implementation of WTO and the Sino-US bilateral agreements, deem the next few years as crucial to the development of an integrated logistics and distribution industry. Accordingly, the central government continues to encourage state-owned firms to form alliances with both domestic and foreign partners (Table 7.2).<sup>8</sup>

On August 5, 2004, the National Development and Reform Commission (NDRC), MOFCOM, Ministry of Public Security, Ministry of Railways, Ministry of Communication, General Administration of Customs, State Administration of Taxation (SAT), Civil Aviation Administration of China, and the State Administration for Industry and Commerce (SAIC) jointly issued the "Opinions on Promoting the Development of a Modern Logistics Sector in China."

According to the opinions, a "logistics enterprise" refers to an economic organization that owns or rents transportation vehicles and warehousing facilities, contains in its business scope the provision of transportation and warehousing services, is able to provide integrated transportation, agency, warehousing, loading and unloading, processing and delivery services, and has the capacity to bear independent civil liability. The opinions set out preferential registration, tax, finance, and customs policies

<sup>8</sup> Wu (2003) at p. 14.

**Table 7.2** Market access restrictions in logistics services

Sector	Limitations on market access
Road	Foreign majority stake of up to 75 % in JVs currently permitted; wholly foreign-owned enterprises (WFOEs) permitted by 12/11/04 CEPA allows WFOEs from 1/1/04
Rail	From January 1, 2003, foreign majority stake permitted; WFOEs permitted from 1/1/06 CEPA allows WFOEs from 1/1/04
Maritime	Minority shares allowed in JVs, degree depends on sub-sector of maritime transport services CEPA allows WFOEs from 1/1/04 in most areas, depending on sub-sector
Storage and warehousing	WFOEs permitted by 12/11/04 CEPA allows WFOEs from 1/1/04
Freight forwarding	Foreign majority stake of up to 75 % in JVs currently permitted; WFOEs permitted by 12/11/05 CEPA allows WFOEs from 1/1/04

CEPA agreements apply to “qualifying Hong Kong service suppliers,” which can be taken to include Hong Kong permanent residents and juridical persons such as corporations, trusts, partnerships, joint ventures, sole proprietorships, or business associations organized under the relevant laws of the Hong Kong SAR

Source USA—China Business Council; Access Asia; Baker & McKenzie

to encourage the development of logistics enterprises. The opinions also encourage major foreign logistics enterprises to establish subsidiaries in China and domestic logistics enterprises to take advantage of foreign capital, equipment and technology.

In addition, after December 11, 2004, China has opened up its logistics industry to overseas competition, in keeping with its WTO commitments. In other words, China’s restrictions on geographic location, equity participation, and the number on foreign invested retail enterprises were removed.<sup>9</sup> Worldwide, the logistics services industry grew in all major markets, with management increasingly capable of expanding operations and making operations more economical.

## 7.3 e-Commerce in China

### 7.3.1 *The Meaning of e-Commerce*

Electronic commerce (e-commerce) includes any form of economic activity conducted via electronic connections.<sup>10</sup> E-commerce is the trading of goods and ser-

<sup>9</sup> “Complete opening-up of retail industry to foreign investors” Xinwen Morning Post, March 17, 2004, Edited by CS Shanghai, cited from China Commercial Brief—March 19, 2004, Vol. 2 No. 154, issued by the US Commercial Service—American Embassy, Beijing. <http://www.mac.doc.gov/china/CommBriefArchive.html>.

<sup>10</sup> Wigand (1997).

vice that takes place electronically, such as over the Internet.<sup>11</sup> E-commerce is the general term for the computer-to-computer processing of a growing variety of transactions, whether or not they take place using the Internet. These transactions range from electronic data interchange (EDI)—the well-established handling of business-to-business purchase orders, invoicing, remittance notices, and other routine documents—to electronic payment systems, credit cards, and consumer sales of goods and services.<sup>12</sup>

Baker and McKenzie (2000) pointed out that e-commerce is defined as the term used for commercial transactions involving the creation, advertising, sale, and distribution of products or services conducted by processing and transmitting digitalized data—including text, sound, and visual images—over open (e.g., Internet) or closed (e.g., Intranet) networks. The term generally includes transactions conducted through the Internet, Intranet, EDI, electronic mail (e-mail), and so forth.<sup>13</sup>

On March 28, 2000, the Beijing Municipal Administration for Industry and Commerce (“BAIC”) issued the “Notice of the Beijing Municipal Administration for Industry and Commerce Concerning E-Commerce Activities Registration” (the “Circular”). The Circular defines e-commerce to include using the Internet to sign contracts and conduct business, disseminate commercial advertising, promote products, provide Internet access, network technology services, graphic design or e-commerce or information services, or undertake any other profit-making activity.

Although e-commerce is not clearly defined in Chinese legislation, yet transactions using data messages are legally recognized under the “Contract Law of the People’s Republic of China,” which took effect on October 1, 1999. The data messages cover messages in the following formats: telegrams, telexes, facsimiles, EDI, and e-mails.

### *7.3.2 The Development of e-Commerce in China*

China is quickly embracing information and communications technology, including the Internet. The trend toward “informatization” in China is clearly growing very rapidly. In May of 2000, the Ministry of Information Industry (MII) published the “Outline of the 15<sup>th</sup> Plan on Information Industry,”<sup>14</sup> setting forth China’s strategic policies in directing the development of the information industry in China. As reflected in many official documents, e-commerce is considered part of the concept of “informatization,” so that the MII has a key role in the area of e-commerce development.

---

<sup>11</sup> Dolber et al. (1998).

<sup>12</sup> Anil (2001).

<sup>13</sup> Baker and McKenzie (2000).

<sup>14</sup> The whole text (Chinese version) is available at [http://www.chinaccia.org.cn/zcfg/qt/qt\\_02sw1.htm](http://www.chinaccia.org.cn/zcfg/qt/qt_02sw1.htm).

The State Administration for Industry and Commerce (“SAIC”), as name suggests, is the primary Chinese regulator of the economy and the market. The SAIC is responsible for the registration of enterprises and for regulating in the areas of advertising, trademark, unjust-competition, and consumer protection, etc. With the economic activities extending to Internet, the SAIC could theoretically extend its administrative functions to electronic commerce. The SAIC has not issued any important regulations to date dealing with e-commerce, although its local counterparts or departments have tried to regulate the virtual market (see the discussion below). It can be expected that the regulation function of the SAIC shall be inevitable move into online transaction.

It has been regarded by the Chinese government important to state security toward supervise information (news, public information, and information products) available on the Internet. A variety of government agencies have supervisory authority on what content is disseminated over the Internet. Among of them, the Ministry of Public Security, charged with overseeing Internet security, focuses on the dissemination of certain banned content as well as distribution and use of certain security products (including hardware and software); the others focus on regulation on an aspect or field of information transmitting over Internet.<sup>15</sup>

China’s online population has grown rapidly in recent years from just 620,000 in 1997. As of June 30, 2005, China has 103 millions Internet users according to the “16th Statistical Survey Report on the Internet Development in China” by CNNIC released on July 21, 2005 in Beijing. The figure consolidates China’s position as the second largest market in the world after the USA.<sup>16</sup>

E-commerce can be seen as a special industry in the national economy. Powerful and effective regulations to control and regulate the market environment are necessary to ensure that the newly emerging form of trade develops rapidly, safely, and in a healthy manner according to its own rules.<sup>17</sup> Policies and procedures should be created to promote an understanding of the potential legal risks.<sup>18</sup>

A research associate of the Program in Comparative Media Law & Policy at the University of Oxford, argued that while the Chinese market is attractive, developing Internet business in China is not easy and can be frustrating at times. Due to the different political, social, economic, and cultural conditions, foreign investors may face significant barriers to establishing Internet businesses in China.<sup>19</sup> A vivid example is that Chinese telecommunications laws forbid foreign participation in the Internet sector before China’s WTO entry.

In November 1999, China signed a bilateral accession protocol with the USA, laying out the terms for China’s accession to the WTO. Under this agreement,

---

<sup>15</sup> See *infra* note 28–30 and the accompanying text.

<sup>16</sup> “CNNIC 16th Report (2005).”

<sup>17</sup> Wu et al. (2001).

<sup>18</sup> Lightle and Sprohge (1992).

<sup>19</sup> Yu (2001).



China will allow 30 % foreign ownership of telecommunications firms upon accession to the WTO, 49 % after the first year, and 50 % after the second year. Despite the almost limitless growth potential of the Chinese telecommunications market, Professor Chan (2002a) maintained that the risk that foreign investors were facing remained very high in this politically sensitive sector of the economy.<sup>20</sup>

The rise in foreign competition in China expected after the country's accession to the WTO has led to pressure to adapt to the rules and possibilities of cyberspace as well. For example, the Shanghai Economic Commission has launched a plan aimed at helping Shanghai's industrial companies make full use of the Internet. It is expected that, by 2005, all major companies will be using the World Wide Web (WWW) to expand their business, both domestically and globally. About 80 % of their small- and medium-sized competitors will have launched a company Web site, as well.<sup>21</sup>

Realistically, China's taking up the Internet will be a slow process. One reason for this is that foreigners are not permitted to have a controlling stake in Internet Content Providers (ICPs) in the initial years after China's accession to the WTO.<sup>22</sup> In accordance with the concessions made by China in agreements reached with the USA in November 1999 and with the European Union in May 2000, in Internet, paging and other value-added services, foreign firms may immediately take 30 % stakes in Chinese companies in Beijing, Shanghai and Guangzhou, rising to 50 % in 2 years, when geographical constraints are lifted. Under WTO rules, benefits granted by China to one trading partner are extended to all.<sup>23</sup>

According to a report by the Ministry of Commerce (2004), logistics service is one of the three problems<sup>24</sup> which hindered China's e-commerce development. The report made an analysis of them. As to the limitation in the logistics system, among the corporations providing logistic services for e-commerce business in China, some 1,000 are traditional ones and their service quality is not good enough; therefore, the need to provide a speedy transaction and delivery regardless of space and distance can hardly be fulfilled.

---

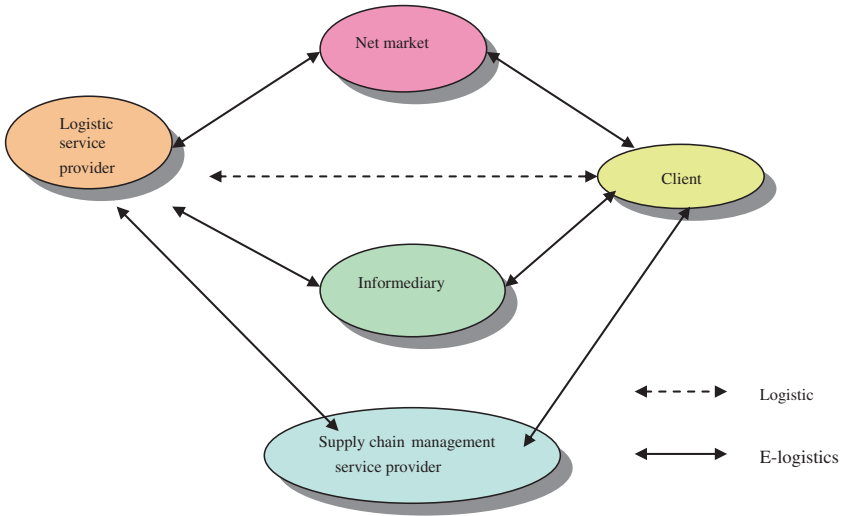
<sup>20</sup> Chan (2002a) at p. 65.

<sup>21</sup> China Business Information Center, "Industrial companies to face the age of Internet," China Daily, p 19. January 2001, <http://www.cbiz.cn>.

<sup>22</sup> China Business Information Center, "Opening Internet will be a slow process—lawyer," 24 November 2000, <http://www.cbiz.cn>.

<sup>23</sup> "Impact on Chinese sectors after WTO entry," China Daily, September 16, 2001, [http://www.chinadaily.com.cn/en/doc/2001-09/16/content\\_83547.htm](http://www.chinadaily.com.cn/en/doc/2001-09/16/content_83547.htm).

<sup>24</sup> Online payment and existing taxation are the other two problems. See "Three obstacles hinder e-commerce in China," China Daily, August 5, 2004, [http://www.chinadaily.com.cn/english/doc/2004-08/05/content\\_360031.htm](http://www.chinadaily.com.cn/english/doc/2004-08/05/content_360031.htm).



Sketch—E-logistics is driven by Internet. *Source* Tian (2002)

### 7.4 Barriers and Legal Solutions to e-Logistics in China

Although Internet penetration remains small judged on a per capita basis, statistics suggest a large and growing community of Internet users in China as above-mentioned.<sup>25</sup> However, the growth of e-commerce in China faces a number of practical and regulatory challenges.

McKenzie (2000) argued that at a practical level, Chinese consumers typically prefer to transact in cash or debit cards, and the rate of use of credit cards is low. Chinese consumers are also concerned about the security of e-commerce transactions. Internet access costs are highly compared with average personal incomes. China’s telecommunications infrastructure also needs to be upgraded in order to provide Chinese users with reliable high-speed access to the Internet. Delivery costs, due both to the use of courier services and China’s distribution infrastructure, also impede the development of China’s e-commerce sector.<sup>26</sup>

In order to encourage the development of commercial Web sites in China, and to anticipate an expansion of e-commerce in the post-WTO economy, China needs to focus on legal reform. China’s current system of laws and regulations does not create a particularly hospitable environment for the development of e-commerce. Much of the commercial legislation that has been issued as part of China’s economic and legal reforms since the 1980 s does not easily apply to the “new economy.”

<sup>25</sup> See supra note 16 and the accompanying text.

<sup>26</sup> McKenzie (2000).

There is no formal, centralized regulation of e-commerce, but beginning from 2000, some government agencies and some local governments have begun to issue regulations specifically targeted at the Internet, but without coordination this effort is creating a patchwork of rules.<sup>27</sup>

For example, in October 2000, an Internet regulation namely, “Measures for Managing Internet Information Services,” was promulgated by the Ministry of Information Industry (MII). But as Chan (2002a, b) indicated: The stringent reporting requirements toward Internet Information Services (IIS) providers, such as the time that subscribers accessed the Internet, subscriber account numbers, the address or domain names of the Web sites, and the telephones numbers they use,<sup>28</sup> will inevitably generate privacy concerns.

The captioned Measures will also handicap the development of Internet-based transportation logistics system, as the cargo owners, warehousing enterprises, and carriers using Internet logistics system may not wish to pass through the government-controlled servers and become subject to such strict censorship. In such a regulatory climate, the zeal and confidence of foreign investors might be significantly dampened.<sup>29</sup>

As mentioned afore, on a local level, the “BAIC” issued the “Notice of the Beijing Municipal Administration for Industry and Commerce Concerning E-Commerce Activities Registration” (the “Circular”) on March 28, 2000. The “Circular” requires any entity in Beijing engaging in e-commerce is to register with the BAIC, and to display a registration seal issued by the BAIC on the home page of its Web site. A registered e-commerce business desiring to alter or terminate its business activities must inform the BAIC.

In addition, the BAIC issued its “Interim Measures of Beijing Municipality for the Administration of Online Advertising” on April 10, 2001, mandating that providers of Internet information services publishing online advertisements must comply with “the Advertising Law” as well as the 1987 Regulations of the People’s Republic of China for the Administration of Advertising and other-related regulations. The Measures also require them to register with the BAIC and obtain an advertising license. It is not clear that whether the above measures will be adopted by the SAIC nationally.<sup>30</sup>

In general, there are more than one hundred promulgated laws, and related rules and regulations on electronic commerce in China. In 2003, these were administered by more than twenty different government bodies in China, including the State Council, ministries, a working party of the State Council, administrative units, commissions, and courts of judiciary, the People’s Bank of China, and local governments.<sup>31</sup>

---

<sup>27</sup> Ibid.

<sup>28</sup> See Article 14.

<sup>29</sup> See supra note 20.

<sup>30</sup> Gao (2004).

<sup>31</sup> Kua (2003).

So far, many cities in China such as Beijing, Shanghai, Tianjin, Chongqing, Shenzhen, Ningbo Guangzhou, Fuzhou and Xiamen, etc., are attempting to develop their logistics industries into pillar industries. They have treated logistics as central to their economic development and have established their own policies. However, overall, logistics services in China are still relatively undeveloped and struggling to keep pace with a rapidly changing economy.<sup>32</sup> In particular, regulators are required to take into account international approaches to laws surrounding logistics and e-commerce when reviewing their current laws.

For example, according to Article 63 of Chapter VI of the “Law of Civil Procedure of the People’s Republic of China,” evidence falls into the following categories: (1) documentary evidence, (2) material evidence, (3) video and audio material, (4) testimony of witnesses, (5) statements by litigants, (6) conclusion, and (7) records of inspection. It is not entirely clear whether an electronic bill of lading (B/L) is covered by Article 63 or not.

The United Nations Commission on International Trade Law (UNCITRAL) is attempting to develop uniform international rules that would validate the use of electronic data interchange (EDI). In 1995, the Commission adopted the “Model Law on Legal Aspects of Electronic Data Interchange and Related Means of Communication.” This law is intended to serve as a model for countries to create uniform law and practice involving the use of computerized system in logistics and international trade.

Article 4 of “the UNCITRAL Model Law on Electronic Commerce” (“the UNCITRAL Model Law”) provides that information should not be denied effectiveness, validity, or enforceability solely on the grounds that it is in the form of a data message. Article 8 also provides that nothing in the application of the rules of evidence shall prevent the admission of a data message in evidence on the ground that it is a data message, or if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

China has not yet adopted “the UNCITRAL Model Law” in its “Civil Procedure Law.” It is therefore strongly recommended by Professor Chan (2002b) that China should also incorporate the relevant provisions of “the UNCITRAL Model Law” into its “Law of Civil Procedure” to fill the legal vacuum.<sup>33</sup>

However, China’s entry into the WTO has inspired a wave of reforms in existing laws and regulations, including laws in e-commerce.<sup>34</sup> Among the various technologies available to authenticate identities online, digital signature technology appears to be preferred by the Chinese government. Robert Moskowitz, a US senior technical director at TruSecure Corporation said digital signature serves four legal functions: (1) evidence, (2) ceremony, (3) approval, and (4) efficiency and logistics.<sup>35</sup>

---

<sup>32</sup> “China logistic firms unable to meet foreign requirements,” SchedNet E-news, December 15, 2003.

<sup>33</sup> Chan (2002b).

<sup>34</sup> Cheung (2001).

<sup>35</sup> Cited from, Zhengping Song, “Making Electronic Contracts Reliable,” LLM Research Paper, <http://chinalawinfo.com/research/academy/details.asp?lid=3290>.

On August 28, 2004, the Standing Committee of the 10<sup>th</sup> National People's Congress enacted the "Electronic Signature Law of the People's Republic of China" ("E-signature Law"), effective April 1, 2005, to boost electronic business, which for the first time legalizes increasing electronic deals. The law grants electronic signatures the same legal effect as handwritten signatures and seals in business transactions, and set up the market access system for online certification providers to ensure the security of e-commerce.<sup>36</sup>

Perkinscoie (2004) pointed out that the PRC "Contract Law," in broad language, recognizes the validity of contracts consummated in the form of electronic data messages, but does not address a wide range of related issues. The "E-signature Law" fills some of the gaps by providing legal definitions of the terms "electronic data message" and "electronic signature," the requirements applicable to the communication and enforceability of electronic data messages, the legal effect and certification of electronic signatures, and the consequences of violating the "E-signature Law."<sup>37</sup>

The "E-signature Law" defines an electronic data message as information generated, sent, received or stored by electronic, optical, magnetic or similar means, and defines an electronic signature as data in an electronic form that can be used to identify the signatory to an electronic data message and to indicate the signatory's approval of the information contained therein. To be valid, an electronic contract must be capable of tangibly representing the content of the agreement, be accessible for subsequent reference at any time, be retained in a format that can demonstrably and accurately represent the information generated, sent or received, and enable the identification of the origin and destination of the electronic data message and the date and time when it was sent and received.<sup>38</sup>

Unless otherwise agreed, an electronic data message is deemed to have been derived from the originator if it was transmitted by a person authorized to act on behalf of the originator or by an information system programmed to operate automatically by or on behalf of the originator, or if the addressee ascertained that the electronic data message was transmitted by the originator after properly applying a procedure previously agreed to by the originator for that purpose.

Unless the parties agree otherwise, an electronic data message is deemed to have been dispatched at the time it passes outside the control of the originator and is deemed to have been received at the time it enters the information system of

---

<sup>36</sup> "China passes law legalizing electronic deals," China Daily, August 28, 2004, [http://www.chinadaily.com.cn/english/doc/2004-08/28/content\\_369759.htm](http://www.chinadaily.com.cn/english/doc/2004-08/28/content_369759.htm).

<sup>37</sup> "Electronic Signature Law," China legal Highlights, Volume 5 Issue 6, October 2004, <http://www.perkinscoie.com/content/ren/updates/china/chinallegalhighlights/2004october.htm#electronic>.

<sup>38</sup> Contracts regarding a personal relationship such as marriage, adoption or inheritance, the transfer of an interest in real property, the suspension of the supply of public utilities, or other situations prohibited by law or administrative regulation may not be formed through electronic communication. See Article 3 para. 3 of the "E-signature Law."

the addressee. If the parties designate a specific information system for the receipt of the message, however, the message is deemed to have been received at the time it enters the designated information system. The addressee must transmit an acknowledgement of receipt of an electronic data message where the parties have agreed that receipt must be acknowledged or where otherwise stipulated by law.

Under Article 13 of the “E-signature Law,” a “reliable” electronic signature has the same legal effect as a handwritten signature or chop. Unless otherwise agreed by the parties, an electronic signature is reliable (a) if the data used to create the electronic signature is in the exclusive control of the signatory for the purpose of creating the electronic signature and (b) if one can identify any change to the electronic signature or to the content or format of the underlying electronic data message that takes place after the issuance of the signature.

If a third party must certify an electronic signature, the signatory must obtain an Electronic Signature Authentication Certificate from a legally established supplier of electronic certification services. A provider of electronic certification services may certify an electronic signature and issue an Electronic Signature Authentication Certificate upon examination of an application submitted by the signatory that confirms the identity of the signatory and provides other-related information. The certificate must contain the name and code number of the signatory, the term of validity, the data concerning the signatory that has been verified, and the name of the service provider.

Upon approval from the Ministry of Information Industry (MII), and in accordance with a related bilateral or multilateral agreement or under the principal of reciprocity, the “E-signature Law” also recognizes certifications issued by foreign suppliers of certification services.

To obtain the authority to issue Electronic Signature Authentication Certificates, a supplier of electronic certification services must apply for approval from the MII. The application must demonstrate that the applicant has established an enterprise in China with a fixed place of business and possesses sufficient qualified personnel, capital, technology, and equipment. The “E-signature Law” obligates the MII to issue a decision within 45 days from receipt of the application. Successful applicants will receive an Electronic Authentication Permit Certificate from the MII and will be required to file Electronic Certification Practice Rules with the MII and publish certain other information on the Internet.

Later on, MII promulgated the “Measures on the Administration of Electronic Certificates Authentication Services” on February 8, 2005, which took effect from April 1, 2005. The Measures stipulate the conditions of becoming a service provider on electronic certificates authentication and govern the scope of services to be provided and the details of the electronic certificates, etc.

While the Internet, and the need to regulate e-commerce via the Internet, has made the process of drawing up new laws more complex, it is also the case that the uneven use of the Internet in China may itself prove to be a barrier to the countrywide management of logistics. A survey by the China Internet Network Information Center (CNNIC) showed that the number of www Web sites established in different provinces and municipalities as on July 21, 2005, varied greatly.

Beijing, the capital, had the highest number of Web sites in China at 123,033, i.e., 18.2 % of all Web sites in the country. This figure was 237.3 times that of Qinghai. The top ten places including Guangdong, Zhejiang, Shanghai, Jiangsu, and Fujian, etc., comprised 80.6 % of the total number of Web sites in China.<sup>39</sup>

## 7.5 Conclusion and Suggestions

Undoubtedly, China wants to see the continued inflow of FDI into the economy to give impetus to the modernization of the country. Apart from being able to invest more freely in China, foreign investors in the manufacturing, trading, or logistics industries expect that there will be more efficient channels to move their commodities and transfer information along with cargo into and out of China.

Influenced by its WTO accession, the legal environment of China is definitely one of the significant factors to analyze the logistics management in China. As mentioned above, the legislative system in China is complex. Logistics and e-commerce are under the jurisdiction of many government ministries and departments. This poses management hurdles for logistics operators in China, especially foreign enterprises.

To transform the freight transport sector into an efficient logistics management industry, China must start to strengthen its rule of law. Only a stronger legal framework can protect foreign investors from the political risks and bureaucratic red tape.

Added to the constantly changing laws on e-commerce is the much shorter life span of technologies, business models, or product cycles in e-commerce markets, which in turn influences the rules and regulations on e-commerce. Therefore, China has to be sensitive and responsive to changes in rules and regulations that will cause uncertainties and lead to a decline in confidence in its information and communication technology (ICT) and logistics industries.

## References

- Anil, S. 2001. Electronic commerce in Asia: The legal, regulatory and policy issues. *International Journal of Law and Information Technology* 2: 93–114.
- Baker & McKenzie. 2000. An overview of China's internet market and its regulation, April 4, 2000, updated August 22, 2000.
- Chan, F. 2001. Logistics management and its legal environment in China. *Hong Kong Law Journal* 3: 497–528.
- Chan, Felix W.H. 2002a. The dynamic legal landscape for logistics management in China. *Asia Business Law Review* 37:61–67.
- Chan, Felix W.H. 2002b. Logistics management in China: Barrier-hurdling and the outlook for legal solutions. UNEAC Asia Papers No. 5, at p. 13.

---

<sup>39</sup> CNNIC 16th Report (2005).

- Cheung, Ray. 2001. Law expert welcomes era of reform, South China Morning Post, November 14. CNNIC 16th Report: WWW Web Sites Number. 2005. July 21 2005, <http://it.people.com.cn/GB/8219/50653/3560135.html>
- Dolber, S., Cheema, S., and Sharrard, J. 1998. Resizing online business trade. The Forrester Report, pp. 1–13.
- Gao, Fuping. 2004. The outline of the electronic commerce legal environment in China: Status in quo and issues , 18 Temp. Int'l & Comp. L. J. 51.
- Kua, F., “Collection of law and regulations in e-Commerce and Internet in China” (in Chinese), Beijing: Legal Press, 2003.
- Lightle, S., and Sprohge, H. 1992. Strategic information system risk. Internal Auditing 6(1):31–36.
- McKenzie, Paul D. 2000. Electronic commerce law—People’s Republic of China, <http://www.perkinscoie.com/page.cfm?id=68>
- Ng, Jimmy. 2004. Barriers to e-commerce logistics in China [Legal Aspects], UNEAC Asia Papers No. 7.
- Nuo, You. 2004. Logistics industry is suffering from growing pains. China Daily, November 30 2004, (HK Edition) p. 20.
- Tian, Xuejun. 2002. E-logistics and its development in China. Logistics World, Special Edition.
- Wigand, R.T. 1997. Electronic commerce: definition, theory and context. 13 The Information Society 1, Special Issue: Theory and Practice of Electronic Commerce, pp. 1–16.
- Wu, Christina. 2003. China, Peoples Republic of Market Development Reports—China Logistics Profile 2003. USDA Foreign Agricultural Service, GAIN Report—CH3833, December 18 2003.
- Wu, J., Li, Q., and Han, F. 2001. The management of e-commerce. The United Nations Online Network in Public Administration and Finance, 27, at p 4.
- Yu, Peter K. 2001. Barriers to foreign investment in the Chinese internet industry, March 2001, <http://www.gigalaw.com/articles/2001-all/yu-2001-03-all.html>



**Part IV**  
**E-Privacy**

# Chapter 8

## E-privacy Protection—Centering on Global Main Legal Instruments and Prospects

Yimeei Guo and Ying Luo

**Abstract** The Internet also creates many threats to our personal privacy. Unless we know the “rules of the road,” our online activity may lead to significant privacy problems. For convenience, this article uses the term “e-privacy” to stand for our personal privacy in the Internet. To avoid an off-limit discussion, after discussing the definition of privacy and e-privacy, this paper analyzes the e-privacy issue and some legal instruments at international and national level with the concern on the collection of personally identifiable information (PII) by Web site operators from visitors to government and commercial Web sites, or by software that is surreptitiously installed on a user’s computer (“spyware”) and transmits the information to someone else, then discusses the captioned problems including a case study in China. Finally, as there is not any complete e-privacy rule for the Internet in China, this paper wants to make some suggestions to Chinese legislature for further specific regulations based on the analysis of the e-privacy in the conclusion.

**Keywords** E-privacy · Spyware · Legal instruments

### 8.1 Introduction

The Internet has created an entirely new legal dynamic as well as a new social and business one. From advertising to intellectual property to privacy and electronic-commerce (e-commerce), the online environment has generated novel legal issues and challenges. At the forefront is the subject of privacy.

---

Published by “Proceedings of 9th Academic Research Conference on Cross-Straits Chinese Culture and Operation Management”, July 8, 2006. pp. 300–308.

---

Y. Guo (✉) · Y. Luo  
Management Science Department, Xiamen University, Xiamen 361005, China  
e-mail: yimei\_guo@necmail.xmu.edu.cn

Y. Luo  
e-mail: yuhe\_ly@sina.com

Generally speaking, the Internet offers many benefits to netizens. Web sites provide a vast world of information, entertainment, and shopping at our fingertips. E-mail, instant message (IE), chat rooms, and ICQ enable us to communicate with friends, family, and strangers in ways we never dreamed of a decade ago.

But the Internet also creates many threats to our personal privacy. Unless we know the “rules of the road,” our online activity may lead to significant privacy problems. For convenience, this article uses the term “e-privacy” to stand for our personal privacy in the Internet.

E-privacy issues generally encompass two types of concerns. One is the collection of personally identifiable information (PII) by Web site operators from visitors to government and commercial Web sites, or by software that is surreptitiously installed on a user’s computer (“spyware”<sup>1</sup>) and transmits the information to someone else. The other is the monitoring of electronic mail and Web usage by the government or law enforcement officials, employers, or internet service providers (ISPs).

To avoid an off-limit discussion, after discussing the definition of privacy and e-privacy, this paper analyzes the e-privacy issue and some legal instruments at international and national level with the former type concern and discusses the captioned problems including a case study in China. Finally, as there is not any complete e-privacy rule for the Internet in China, this paper wants to makes some suggestions to Chinese legislature for further specific regulations based on the analysis of the e-privacy in the conclusion.

## 8.2 What is Privacy/E-privacy?

### 8.2.1 *The Right of Privacy*

The notion of privacy was first postulated in a Harvard Law Review article by Louis D. Brandeis, later to become a Justice of the Supreme Court of the USA, and Samuel D. Warren of the Harvard Law School, in 1890.<sup>2</sup> They described privacy as “the right to be let alone”<sup>3</sup> when they were offended by press coverage of their families, and by “recent inventions and business methods.”<sup>4</sup> It took almost 20 years before the American courts issued judgments which adopted that principle.<sup>5</sup>

---

<sup>1</sup> Spyware, a catch-all phrase for software that enables a person’s online movements to be tracked, has quietly become the latest threat to cyber security, affecting eight out of 10 computers. See Anita Kumar, “Can Congress get arms around spyware problem?”, [http://www.sptimes.com/2005/05/02/Technology/Can\\_Congress\\_get\\_arms.shtml](http://www.sptimes.com/2005/05/02/Technology/Can_Congress_get_arms.shtml).

<sup>2</sup> Brandeis and Warren (1890).

<sup>3</sup> Ibid.

<sup>4</sup> Id, at 195.

<sup>5</sup> Boufford (1998).

Later on, in another article by William Prosser, four different types of invasions of privacy were pointed out, including:

1. appropriating an individual's name or likeness for commercial benefit;
2. unreasonable intrusion or interference with an individual's interest in solitude or seclusion;
3. publicly disclosing private facts;
4. publicly placing an individual in a false light.<sup>6</sup>

### 8.2.2 E-privacy and “Fair Information Practices”

From an information technology (IT) perspective, a much better definition of privacy has been that of Alan Westin, where he described privacy as:

the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.<sup>7</sup>

This definition embodies the concept of “*fair information practices*” which forms the basis for many of the regulatory and voluntary data-protection schemes.<sup>8</sup>

In short, “privacy” is not just a matter of what is kept secret. In the context of e-commerce and e-government, the right to privacy, i.e., e-privacy is really “*the right to control the use of personal information*” that is disclosed to others.<sup>9</sup>

Throughout the world, the privacy of information about individuals is guided by the principles of “*fair information practices*.” These principles, which were authoritatively detailed by the Organization for Economic Co-Operation and Development (OECD),<sup>10</sup> represent basic guidelines for responsible information practices that respect the interests of individuals. They form the foundation of many national and local privacy laws, international agreements on data protection, and various industry codes of best practices.<sup>11</sup> It is these principles that provide the framework for privacy impact assessments and the reference point for the work of privacy commissioners.

---

<sup>6</sup> Prosser (1960). See also *Zacchini v. Scripps-Howard Broadcasting Co.*, 433 U.S. 562,571(1977), Note 7.

<sup>7</sup> Westin (1967) at 7.

<sup>8</sup> See supra note 4.

<sup>9</sup> See Privacy and E-Government (2003).

<sup>10</sup> See “*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*”, 1980, <http://www.oecd.org/EN/document/0,,EN-document-0-nodirectorate-no-24-10255-0,00.html>.

<sup>11</sup> See supra note 8.

As expressed by the OECD and other international bodies, fair information practices include:

- **Collection limitation:** No more information should be collected than is necessary to complete the transaction, and any such data collected should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data quality:** Personal data should be relevant to the purposes for which they are to be used, should be accurate and complete, and should be kept up-to-date.
- **Purpose specification:** When personal data are collected, the purpose for the collection should be specified and the subsequent use limited to the fulfillment of that purpose or such others as are not incompatible with the original purpose.
- **Use limitation:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the “purpose specification” except: (a) with the consent of the data subject; or (b) by the authority of law.
- **Security:** Personal data should be protected by reasonable security safeguards against loss or unauthorized access, destruction, use, modification or disclosure.
- **Openness:** In general, there should be no secret collections of data. As a matter of general policy, there should be openness about data practices and policies. Means should be readily available to individuals to establish the existence and nature of databases, the main purposes of their use, and the identity of the entity responsible for the database.
- **Individual participation:** An individual should have the right to obtain access to any data about him held by a data controller. This includes: (a) confirmation of whether or not an entity has data relating to him; (b) to obtain copies of data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, or corrected or completed.
- **Accountability:** Entities collecting data should be subject to enforcement measures that give effect to the principles stated above.

There are obvious exceptions to some of these principles in specific applications. For example, in the context of law enforcement investigations, it is not always possible to give notice to a suspect or to give him access to the information that the police are collecting. Nevertheless, these principles provide a framework for thinking through the privacy issues raised by any government collection of personal information.<sup>12</sup>

---

<sup>12</sup> “Personal (or personally identifiable) information” is data that can be associated with an individual. Notably, a person’s name need not be attached to the information for it to qualify as “personal information.” For example, data categorized by a unique numeric identifier is considered personal information even where no name is attached to it, since the numeric identifier can be used to determine the name.

## 8.3 Main Legal Instruments Dealing with Data Privacy

### 8.3.1 *International Instruments*

#### 8.3.1.1 The 1980 OECD Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data

The Guidelines contain a set of data privacy principles similar to those stipulated in “*the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.*”<sup>13</sup> The Guidelines have been very influential on the drafting of data privacy laws and standards in non-European jurisdictions, such as Australia, New Zealand, and Canada.<sup>14</sup> They have also been formally endorsed—though not necessarily implemented—by numerous companies and trade associations in the USA.<sup>15</sup> Further, they constitute an important point of departure for ongoing efforts by the Asia-Pacific Economic Cooperation (APEC) to draft a set of common data privacy principles for jurisdictions in the Asia-Pacific region.<sup>16</sup>

#### 8.3.1.2 The Montreux Declaration

In terms of other international legal instruments, there does not exist a truly global convention or treaty dealing specifically with data privacy. The call to the United Nation (UN) was made in a declaration adopted at the 27th International Conference of Data Protection and Privacy Commissioners in Montreux in early September of 2005.

In what they have called “the Montreux Declaration,” the commissioners also call for governments to encourage the adoption of legislation in line with recognized data protection principles and to extend it to their mutual relations; and for the Council of Europe to invite non-member states of the organization to ratify the Convention for the protection of individuals with regard to automatic processing of personal data and its additional protocol.

International organizations have been asked to commit themselves to complying with data protection rules; international non-governmental organizations

<sup>13</sup> European Treaty Series No. 108; adopted Jan 28, 1981; in force Oct 1, 1985. Further on the Convention, see, e.g., Henke (1986), Bygrave (2002), especially p. 32.

<sup>14</sup> Reference to the Guidelines is made in the preambles to both Australia’s federal “*Privacy Act of 1988*” and New Zealand’s “*Privacy Act of 1993*”. Further on the Guidelines’ importance for Australian policy, see Ford (2003). In Canada, the Guidelines formed the basis for the Canadian Standards Association’s “*Model Code for the Protection of Personal Information*” (CAN/CSA-Q830-96), adopted in March 1996. The Model Code has been incorporated into Canadian legislation as Schedule 1 to “*the Personal Information Protection and Electronic Documents Act of 2000*”.

<sup>15</sup> See, e.g., Gellman (1993).

<sup>16</sup> See generally the documentation collated at [http://www.apecsec.org.sg/apec/documents\\_reports/electronic\\_commerce\\_steering\\_group/2004.html](http://www.apecsec.org.sg/apec/documents_reports/electronic_commerce_steering_group/2004.html).

(NGOs) have been asked to draw up data protection standards; and hardware and software manufacturers have been asked to develop products and systems that integrate privacy-enhancing technologies.

The nature of the legally binding instrument to be adopted by the UN is not prescribed; but Swiss data-protection commissioner Hanspeter Thür told SwissInfo.org that it could be a text adopted by the UN in the same way as human-rights provisions.

Progress in implementing the objectives will be subject to a regular assessment. The first such assessment will be carried out at the 28th International Conference, due to take place in September 2006 in Argentina.

The commissioners also adopted a resolution presented by Germany on the use of biometric data in passports, ID cards, and travel documents. In it, the commissioners call for effective safeguards to be built in so as to limit the risks inherent in biometrics. They also adopted a resolution from Italy on the use of personal data for political communication purposes.<sup>17</sup>

### 8.3.1.3 The European Union

Within the European Union (EU), several Directives on data privacy have been adopted, the first and most important of which is “*Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*” (hereinafter “*EU Directive*”).<sup>18</sup> This instrument is binding on EU member states. It is also binding on non-member states (Norway, Iceland and Liechtenstein) that are party to the 1992 Agreement on the European Economic Area (EEA). While the Directive is primarily a European instrument for European states, it exercises considerable influence over other countries not least because it prohibits (with some qualifications) transfer of personal data to those countries unless they provide “adequate” levels of data privacy (see Articles 25–26).<sup>19</sup> Many non-European countries are passing legislation in order, at least partly, to meet this adequacy criterion.<sup>20</sup>

Furthermore, the Directive stipulates that the data privacy law of an EU state may apply outside the EU in certain circumstances, most notably if a data

<sup>17</sup> See “Global data protection law needed, say regulators,” OUT-LAW News, 19/09/2005, <http://www.out-law.com/page-6132>.

<sup>18</sup> Adopted Oct. 24, 1995, O.J. L 281, Nov. 23, 1995, p. 31 et seq. Two sectoral Directives on data privacy have also been adopted. The first of these was “*Directive 97/66/EC of Dec.15, 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector*”, O.J. L 24, Jan. 30, 1998, p.1 et seq. This has now been replaced by “*Directive 2002/58/EC of July 12, 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*”, O.J. L 201, July 31, 2002, p. 37 et seq.

<sup>19</sup> See e.g., Kuner (2003), Chap. 4.

<sup>20</sup> Further on this influence, see Swire and Litan (1998), Shaffer (2000), Waters (2003).

controller,<sup>21</sup> based outside the EU, utilizes “equipment” located in the state to process personal data for purposes other than merely transmitting the data through that state (see Article 4 <1> <c>).<sup>22</sup> All of these provisions give an impression that the EU, in effect, is legislating for the world.<sup>23</sup>

Although the Directive establishes what a company can and cannot do with the data they hold, yet it does not make any specific provisions with regard to e-mail or more specifically, e-mail marketing. Unsolicited e-mail, i.e., “spam” is becoming a growing problem that is costing business worldwide a staggering £6bn per year in online connection costs.<sup>24</sup> As the European Parliament and the Council of the European Union conceive: the Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services, publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy. So-called spyware, Web bugs, hidden identifiers, and other similar devices can enter the user’s terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.<sup>25</sup>

Therefore, a new EU anti-spam law—*Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*<sup>26</sup> came into force on December 11, 2003, and is already having a dramatic effect on the amount of spam sent to computer users. Under the Directive, spyware becomes illegal software.<sup>27</sup> This Directive’s implementation glorifies the formal stepping in the global anti-spam war of EU and is an important weapon to enhance the consumer’s confidence on Internet and e-communication as well.<sup>28</sup>

---

<sup>21</sup> A “data controller” is a person or organization who/which determines the purposes and means of processing personal data: see E.U. Directive, Article 2(d).

<sup>22</sup> See further Bygrave (2000); Kuner, *supra* note 14, Chap. 3.

<sup>23</sup> See further Bygrave (2000); Kuner, *supra* note 17, Chap. 3.

<sup>24</sup> See “EU Directive on e-mail marketing”, <http://www.extravision.com/eudirective.cfm>.

<sup>25</sup> “Preamble, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)”, O.J.L 201, 31/07/2002, pp. 0037–0047.

<sup>26</sup> *Ibid.*

<sup>27</sup> Article 13 provides that: the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

<sup>28</sup> See “EU implements Anti-spam Act, spyware becomes illegal software,” Dec. 3, 2003, [http://news.cidnet.com/pub/article/c951\\_a69660\\_p1.html](http://news.cidnet.com/pub/article/c951_a69660_p1.html).



## 8.3.2 National Instruments

### 8.3.2.1 The USA

By contrast, the US legal regime for data privacy is much more atomized. While there is fairly comprehensive legislation dealing with federal government agencies,<sup>29</sup> omnibus legislative solutions are eschewed with respect to the private sector. Legal protection of data privacy in relation to the latter takes the form of ad hoc, narrowly circumscribed, sector-specific legislation, combined with recourse to litigation based on the tort of invasion of privacy and/or breach of trade practices legislation.<sup>30</sup> European-style data privacy agencies do not exist.

At the same time, though, a “safe harbor” agreement has been concluded between the USA and EU allowing for the flow of personal data from the EU- to US-based companies that voluntarily agree to abide by a set of “fair information” principles based loosely on the EU Directive. The scheme, which so far has attracted over 500 companies,<sup>31</sup> has been held by the European Commission to satisfy the Directive’s adequacy test in Article 25.<sup>32</sup>

Today, much of the privacy regulation in the USA occurs at the state level, where many of the 50 states have enacted privacy laws that govern specific industries, issues, or practices. Often, these laws are inconsistent, so that a set of business practices that is legal and commonplace in one state may be prohibited just across the state line. In addition, the *number* of state privacy laws is increasing quickly—for example, more than 20 states have passed separate financial privacy laws just since the beginning of 2004.

At the same time, Congress has enacted federal privacy legislation specific to certain industries. For instance:

- *The Gramm-Leach-Bliley Act* applies to financial institutions;
- The Health Insurance Portability and Accountability Act (HIPAA) of 1996<sup>33</sup> applies to health care providers;
- The privacy provisions of *the Cable Act* apply to cable operators;

<sup>29</sup> Most notably *the Privacy Act of 1974* and *Computer Matching and Privacy Protection Act of 1988*. Note also the limited protection of data privacy afforded under the Constitution as construed by the Supreme Court: see especially *Whalen v. Roe*, 429 U.S. 589 (1977). See further Schwartz and Reidenberg (1996), Chap. 4.

<sup>30</sup> See generally the overview in Schwartz and Reidenberg, *supra* note 13, especially Chaps. 9–14.

<sup>31</sup> See “<http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>” (accessed July 6, 2004).

<sup>32</sup> Decision 2000/520/EC of July 26, 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (O.J. L 215, 25th Aug. 2000, p. 7 et seq.). However, the scheme is presently under review by the Commission.

<sup>33</sup> 42 USC § 201 et seq. (42 USC 1320d-2).

- The privacy provisions of *the Communications Act* apply to telecommunications carriers<sup>34</sup>;
- Specific privacy laws address children’s online privacy,<sup>35</sup> spam, telemarketing, and junk faxes<sup>36</sup>;
- *The Identity Theft Penalty Enhancement Act (ITPEA)* increases criminal penalties for phishing and other forms of identity fraud. This measure, signed by the President in July 2004, establishes punishment guidelines for anyone who possesses someone else’s personal information with intent to commit a crime.<sup>37</sup>
- And concerns over spyware are now prompting an array of federal legislative proposals.<sup>38</sup>

Finally, a bill announced on February 8, 2006, in Congress would require every Web site operator to delete information about visitors, including e-mail addresses, if the data is no longer required for a “legitimate” business purpose.<sup>39</sup>

While all of these are well-intended efforts, this ad hoc approach to privacy legislation has many drawbacks. It has led to an overlapping, inconsistent, and incomplete patchwork of state and federal laws that creates compliance chaos for businesses and uncertainty for consumers.

Consumers and businesses alike are often faced with the daunting task of determining whether one or more of the existing laws applies. The answer may depend on the type of data involved, the kind of company that collects it, where and how it is collected, and how it might be used.

For example, personal information collected by a bank is covered by one privacy standard, but that same information collected by a hospital is covered by a different standard. If that information is from a child under the age of 13, it is protected by yet another standard if it is collected online, but it may not be protected at all if it is collected offline. And each of those standards may be affected by state law, but in a different way from state to state. Yet, despite all of these legal

<sup>34</sup> Part I of title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) is amended by adding at the end the new section 231: (d) Privacy Protection Requirements.

<sup>35</sup> “*Child Online Privacy Protection Act (COPPA)*”, 15 USC 6501-6506.

<sup>36</sup> *The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act)*, 18 USC 1037.

<sup>37</sup> On Sept. 30, 2005, California Governor Arnold Schwarzenegger signed the Anti-Phishing Act of 2005 into law. The first-of-its-kind bill makes Internet phishing a punishable offense. The new law will permit victims to seek recovery of actual damages or up to \$500,000 for each violation, whichever is greater. See Walaika K. Haskins, “California Passes Nation’s First Antiphishing Law”, Oct. 4, 2005, [http://www.newsfactor.com/story.xhtml?story\\_id=38456](http://www.newsfactor.com/story.xhtml?story_id=38456).

<sup>38</sup> So far, the anti-spyware legislation has been enacted in twelve states. For example, in 2004, California has enacted “*the Consumer Protection Against Spyware Act*”, to “protect California consumers from the use of spyware and malware that is deceptively or surreptitiously installed on their computers.” See “Schwarzenegger Signs California Anti-Spyware Bill”, Sept 28, 2004, <http://www.reuters.com/newsArticle.jhtml?storyID=6359582>.

<sup>39</sup> Declan McCullagh, “Bill would force Web sites to delete personal info”, February 8, 2006 [http://news.com.com/2100-1028\\_3-6036951.html](http://news.com.com/2100-1028_3-6036951.html).

distinctions, the consequences of misuse of that information could be exactly the same in each scenario.<sup>40</sup>

### 8.3.2.2 Canada

Across the Atlantic, Canada comes closest of the North American countries to embracing the European approach. There is now federal legislation in place to ensure comprehensive protection of data privacy in relation to both the public and private sectors, such as *Privacy Act of 1982*, *Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000*.

The PIPEDA came into full effect on January 1, 2004, which would apply to all businesses in Canada that use direct marketing and/or data mining, that collect, store and communicate personal information respecting employees and/or customers, and businesses with partners and business allies, or outsource company functions of this nature. The Act specifically requires that businesses disclose the purposes for the collection of personal information and that they obtaining consent for such use. The Act also contains restrictions against repurposing or publishing/sharing that information.<sup>41</sup>

Some provinces have already enacted data privacy legislation in relation to provincial and local government agencies and/or the private sector.<sup>42</sup> Data privacy agencies exist at both federal and provincial levels. The Commission of the European Communities has formally ruled that, in general, Canada offers “adequate” protection for data privacy pursuant to Article 25 of the EU Directive.<sup>43</sup>

### 8.3.2.3 The Asia-Pacific Region

In this region, there exist a handful of relatively comprehensive legislative regimes on data privacy—most notably those in Australia, New Zealand, Hong Kong, Korea, and Japan.<sup>44</sup> The bulk of these jurisdictions—but not Japan—has also

<sup>40</sup> Brad Smith, “*Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation*”, Nov. 2005, <http://www.cdt.org/privacy/20051103microsoftprivacy.pdf>.

<sup>41</sup> Brent Krause, “*An Overview of the Canadian Personal Information Protection and Electronic Documents Act*”, Feb. 2001, <http://www.gigalaw.com/articles/2001-all/krause-2001-02-all.html>.

<sup>42</sup> See, e.g., Quebec’s Act on Protection of Personal Information in the Private Sector of 1993.

<sup>43</sup> Decision 2002/2/EC of Dec. 20, 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (O.J. L 2, Jan. 4, 2002, p. 13 et seq.).

<sup>44</sup> Further on Australian law, see, e.g., Hughes and Jackson (2001); on New Zealand law, see Longworth and McBride (1994) and Roth (1994)—(looseleaf, regularly updated); on Hong Kong law, see Berthold and Wacks (2003); on Korean law, see Yi and Ok (2003) and Chung (2003); on Japanese law, see Case and Ogiwara (2003).

established data privacy agencies. New Zealand has been the fastest and perhaps most ambitious of these jurisdictions in the data privacy field; it was the first to enact data privacy legislation applying right across the public and private sectors.<sup>45</sup>

Australian, Korean, and Japanese legislation in the field was initially limited largely to regulating the data-processing activities of government agencies,<sup>46</sup> but has recently been extended to cover the private sector as well.<sup>47</sup> However, some of these extensions still leave large gaps in private sector coverage.<sup>48</sup> Other aspects of the laws in question also diverge from the EU model(s).<sup>49</sup> Not surprisingly, none of the countries concerned has yet been formally recognized by the European Commission as offering adequate protection pursuant to the EU Directive. By contrast, India is reported to be considering enactment of a data privacy law modeled on the EU Directive largely due to a fear that its burgeoning outsourcing industry will flounder without such legislation in place.<sup>50</sup>

Data privacy regimes in other Asia-Pacific jurisdictions tend to be rather patchy in coverage and enforcement levels. Thailand, for instance, has inserted data privacy rules covering the government sector, in legislation dealing primarily with freedom of government information.<sup>51</sup> Singapore has so far decided to establish a data privacy regime based on voluntary, self-regulatory schemes that are linked with its national trust mark programmer.<sup>52</sup> The primary catalyst for the schemes appears to be commercial concerns.<sup>53</sup>

---

<sup>45</sup> See Privacy Act of 1993.

<sup>46</sup> For Australia, see Privacy Act of 1988; for Japan, see Act for Protection of Computer-Processed Personal Data Held by Administrative Organs of 1988; for Korea, see Act on Protection of Personal Information Maintained by Public Agencies of 1994.

<sup>47</sup> For Australia, see Privacy Amendment (Private Sector) Act of 2000; for Japan, see *Privacy Law of 2003*; for Korea, see *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. of 1999*. Note too that several of the Australian States have enacted data privacy laws covering their respective government agencies and, to a lesser extent, the health sector. See, e.g., *Victoria's Information Privacy Act of 2000 and Health Records Act of 2001*.

<sup>48</sup> For example, with a few exceptions, the Australian legislation does not apply to "small business operators"; i.e., businesses with an annual turnover of AUD\$3 million or less [see federal Privacy Act, sections 6C(1), 6D, 6DA & 6E]. Another major gap is that the legislation does not cover the processing of data by employers about their present and past employees (as long as the processing is directly related to the employment relationship) [Section 7B(3)].

<sup>49</sup> The Japanese laws, for example, do not formally operate with a distinction between sensitive and non-sensitive data, and they make relatively extensive use of "opt-out" consent mechanisms.

<sup>50</sup> See Pedersen (2003).

<sup>51</sup> See Official Information Act of 1997, described in Opassiriwit (2002).

<sup>52</sup> See "Model Data Protection Code for the Private Sector of 2002"; Industry Content Code of 2002.

<sup>53</sup> For criticism of the schemes, see Greenleaf (2002).

## 8.4 E-privacy Protection in China

### 8.4.1 Current Situation and Development

China's laws and regulations do not generally provide comprehensive rights and protections to Internet users. There is often tension between formal legal rights and those recognized in actual cases. Considering a right to privacy, Article 38 of China's Constitution refers to a fundamental right of personal dignity, believed by most Chinese legal scholars to incorporate a right of privacy.<sup>54</sup> Article 40 provides for the freedom and privacy of citizens' communications, and bars other organizations and individuals from infringing on those rights. The same Article, though, contains restrictions on or permits deprivation of a citizen's privacy or correspondence rights by public authorities to "meet the needs of state security" or "investigate criminal offenses"—broad, ambiguous exceptions. Some of China's legislation alludes to a similar right of privacy. However, Chinese constitutional jurisprudence does not recognize a fundamental right of privacy in action.

Legislation governing Internet users contains the same dichotomy. Certain regulations partially recognize a right to privacy. For example, Internet users' personal information is protected against unauthorized public disclosure by electronic messaging service providers.<sup>55</sup> Users whose personal information is disclosed, in violation of this provision, can sue for damages and injunctive relief.<sup>56</sup> Similarly, it is illegal to use computer information systems to steal or disrupt others' information or jeopardize the lawful interests of citizens; violators risk civil penalties.<sup>57</sup>

User communications also enjoy protection, at least in theory. Regulations affirm the freedom and privacy of users' e-mails and ban others from infringing upon their privacy. Violators who illegally intercept, modify, or delete others' e-mails face criminal liability.<sup>58</sup> Even compulsory seizure of e-mails and other private telecommunications by the state is limited, according to the laws, to instances where the public security authority, public procurator authority, or the national security authority must do so to investigate a national security threat or criminal

---

<sup>54</sup> Art.101 of the China's "General Principles of Civil Law" protect both personal dignity and the "right of reputation" and have been construed by the Supreme People's Court to include the right to privacy. Most likely, Chinese legal scholars extrapolate this conclusion from the relevant SPC decisions. See *Privacy Protection in China's Cyberspace*, China Law and Practice, February 2003.

<sup>55</sup> Art.12, *Administration of Internet Electronic Messaging Service Provisions*.

<sup>56</sup> Art.19, *Id.*

<sup>57</sup> Art.25, *Protection of the Safety of Computer Data Systems Regulations*; Article 58(2), *Telecommunications Regulations*.

<sup>58</sup> Art.4.2, *Internet Security Decision*.

conduct.<sup>59</sup> Such seizures are formally governed by specific criminal procedure requirements.<sup>60</sup>

However, the state possesses the power to regulate Internet content and to demand that ISPs and Internet Content Providers (ICPs) turn over personal information of Internet users who violate the laws or post prohibited content (a term defined broadly). Upon official request, an ISP or ICP must provide the user's name, IP address, e-mail address, user name, information on any changes in IP address and use, and all data saved by the service provider's computer when the prohibited content or illegal conduct took place, including time, content, originating source, and system logs.<sup>61</sup>

Thus, while China ostensibly provides some protection to users in the form of legally guaranteed rights, these safeguards rarely function in practice.

Nevertheless, South China's Guangxi Zhuang Autonomous Region has already banned unauthorized publication or forwarding of the applicants' personal information by administrative permit authorities in a set of regulations that took effect on February 1, 2005.

Recently, in Chinese booming market economy, many people leave their personal data when filling out applications. But some data holders—hospitals, realtors, telecom, and ISPs—sell the information to others who will later come up with unwelcome phone calls or visits.

New mothers in Beijing, for example, find they have to answer many unexpected calls shortly after they are home with the babies—infant formula suppliers, baby haircutters, and insurance agents have already got a long list of potential customers from the delivery room. Also, a gang in Shanghai was recently found to have stolen other people's personal information, applied for credit cards in their names and made vicious overdraft amounting to RMB ¥ 470,000 (US\$56,600).<sup>62</sup>

Therefore, it should be noted that the draft of *the Law for Personal Information Protection of the People's Republic of China*, completed in January 2005, after 2 years' deliberation, has been submitted to the Information Office of the State Council for processing. With a definition of personal information that is broader than just including privacy, the drafted law places a wide range of information under protection, including cell-phone numbers, family addresses, medical records, and occupation. Once the law is proclaimed, violators of personal information will be charged with administrative, civil, and even criminal responsibility.<sup>63</sup>

---

<sup>59</sup> Art.66, *Telecommunications Regulations*.

<sup>60</sup> Art.116, *Criminal Procedure Law*.

<sup>61</sup> Ministry of Public Security, *Questions Relevant to the Implementation of the Circular*.

<sup>62</sup> See "Lawmaker Urges Legislation to Curb Rampant Privacy Infringement", Xinhua News Agency March 6, 2005. It is also available at <http://www.china.org.cn/english/2005lh/121920.htm>.

<sup>63</sup> "Do We Need Legislation to Protect Personal Information?", Beijing Review, March 24, 2005, Vol. 48, No. 12, at Col. 44.

## 8.4.2 *Ucloo.com Case Study*

### 8.4.2.1 The Fact

Since early December 2005, Ucloo.com—an Internet portal that is said to hold personal files on 90 million people—has provided a service nicknamed “souren,” meaning searching for a specific person. By paying RMB 1 (12 US cents) through one’s mobile phone, it is possible to find personal information such as telephone numbers, addresses, and even details of marital status and credit ratings. A student was surprised that someone he had never met called him and knew what he had written in his schoolmate address book. Later on, he was told the man obtained his contact details from Ucloo.com.

Another portal called 5460.net has been accused of leaking its pool of 90 million data files on users to Ucloo.com. But those concerned from 5460.net said the company had never authorized Ucloo.com to use its data and it had no idea how the portal had obtained the files.

5460.net, which has a collection of schoolmate address information covering 90 million people, has said it may take Ucloo.com to court.

Under pressure, Ucloo.com has canceled the charged service and said netizens can use the service through e-mail and apply for corrections of the personal information kept by the portal.<sup>64</sup>

### 8.4.2.2 A Brief Comment

The primary concern is how the portal obtained the data in the first place. Those in charge of Ucloo.com said they had obtained the data through legal channels and all of the personal information they held had appeared somewhere on public Web sites. They admitted only a portion of their data came from 5460.net.

If what they said is true, we have reason to remind ourselves that we must use caution whenever we are required to fill in forms on the Internet, such as providing an e-mail address, because that is how personal information enters the public domain.

Personal information is often required if surfers wish to view certain documents or apply for an e-mail address, but Web sites should have an obligation to keep personal information secret.

Another concern is whether the portal has the right to use the data at all, even if it has obtained contact details by legal means. Apparently, when such information as a person’s phone number, address, or even his or her family background or

---

<sup>64</sup> Zhu Yuan, “Web users worry about ease of obtaining personal data”, China Daily Jan. 16, 2006 at p. 4. It is also available at [http://www.chinadaily.com.cn/english/doc/2006-01/16/content\\_512461.htm](http://www.chinadaily.com.cn/english/doc/2006-01/16/content_512461.htm).

marital status is involved, the person should be contacted for consent before the information is used.

As many reports in China have revealed, it is obvious those whose personal information has been put on the Web site have never given consent. If anyone gets into trouble because of the information provided on the Web site, the portal will be liable for legal penalties.

Although a notice on the Ucloo.com Web site says the firm is registered in the USA, yet, this does not mean it has the right to provide the service. This incident indicates that more detailed rules are urgently needed for the management of information on the Internet. The rise of the Internet has made life and work more convenient, but the risk of invasion of privacy has also increased because of the free flow of information.<sup>65</sup>

## 8.5 Conclusion and Suggestions

Internet privacy, without doubt, presents significant issues for consumers, industry, and the government. It is also without doubt that these issues have increasingly become the subject of private and governmental attention in the form of lawsuits and proposed legislation.

There are serious questions, however, whether such attention is, in fact, effectively addressing the risks of abuse that exist in connection with the use of personal information obtained from Internet activity, and what the costs may be for such attention.

As to China, the Internet development is still in the initial stage, regulations need posit the suitable stand to both promote the Internet evolvement and guarantee the user's interests. Regulations shall consider difference between countries while taking foreign laws as reference. Regulations shall also differentiate various Internet services while taking responsive measures.

Finally and overall, as the government has to ensure a better awareness among the citizens about the privacy risk of Internet and the adequate solutions the technical tools and the interactivity of the network provide. It is quite clear that the Internet's user is himself his own better identity protector. He might decide to prevent the arrival of cookies, to erase them, or block their sending; he might through techniques of encryption of anonymous protect the confidentiality of his message or its anonymity; he might reveal or not certain data, decide to communicate only with rated Web sites and use his access right to control their activities.<sup>66</sup>

---

<sup>65</sup> Ibid.

<sup>66</sup> Yves Poullet, Internet and privacy: any conclusions, <http://www.droit.fundp.ac.be/textes/conclusions.pdf>.



## References

- Berthold, M., and Wacks, R. 2003. *Hong Kong data privacy law: Territorial regulation in a borderless world*, 2nd ed. Hong Kong: Sweet & Maxwell Asia.
- Boufford, John G. 1998. Privacy on the information highway. *U.N.B.L.J.* 47: 219.
- Brandeis, L.D., and S.D. Warren. 1890. The right to privacy. *Harvard law review* 4: 193.
- Bygrave, L.A. 2000. Determining applicable law pursuant to european data protection legislation. *Computer Law and Security Report* 16: 252–257.
- Bygrave, L.A. 2002. *Data protection law: Approaching its rationale, logic and limits*. The Hague/London/New York: Kluwer Law International.
- Bygrave, Lee A. 2004. Privacy protection in a global context—a comparative overview. *Scandinavian Studies in Law* 47: 319–348. [privacy%20in%20global%20context.pdf](#).
- Case, D., and Y. Ogiwara. 2003. Japan's new personal information protection law. *Privacy Law & Policy Reporter* 10: 77–79.
- Chung, H.-B. 2003. Anti-spam regulations in Korea. *Privacy Law & Policy Reporter* 10: 15–19.
- Ford, P. 2003. Implementing the EC directive on data protection—an outside perspective. *Privacy Law & Policy Reporter* 9: 141–149.
- Gellman, R.M. 1993. Fragmented, incomplete, and discontinuous: the failure of federal privacy regulatory proposals and institutions. *Software L. J.* 6: 199, 230.
- Greenleaf, G. 2002. Singapore takes the softest privacy options. *Privacy Law & Policy Reporter* 8: 169–173.
- Henke, F. 1986. *Die Datenschutzkonvention des Europarates*. Frankfurt am Main/Bern/New York: Peter Lang.
- Hughes., and Jackson, M. 2001. *Hughes on data protection in Australiam*, 2nd ed. Sydney: Law Book Co. Ltd.
- Kuner, C. 2003. *European data privacy law and online business*. Oxford: Oxford University Press.
- Longworth, E., and T. McBride. 1994. *The privacy act: a guide*. Wellington: GP Publications.
- Opassiriwit, C. 2002. Thailand: a case study in the interrelationship between freedom of information and privacy. *Privacy Law & Policy Reporter* 9: 91–95.
- Pedersen, A. 2003. India plans EU-style data law. *Privacy Laws & Business* (68): 1, 3.
- Privacy and E-Government. Privacy impact assessments and privacy commissioners –two mechanisms for protecting privacy to promote citizen trust online. 1 May 2003, <http://www.internetpolicy.net/practices/030501pia.pdf>.
- Prosser, William. 1960. Privacy. *Cal. L. Rev.* 48: 383.
- Roth, P. 1994. *Privacy law and practice*. Wellington: Butterworths/LexisNexis.
- Schwartz, P.M., and J.R. Reidenberg. 1996. *Data privacy law: a study of united states data protection*. Charlottesville: Michie Law Publishers.
- Shaffer, G. 2000. Globalization and social protection: the impact of e.u. and international rules in ratcheting up of U.S. privacy standards. *Yale J. of Int'l Law* 25: 1–88.
- Smith, Brad. Protecting consumers and the marketplace: The need for federal privacy legislation. <http://www.cdt.org/privacy/20051103microsoftprivacy.pdf>.
- Smith, Marcia S. 2004. Internet privacy: Overview and pending legislation. Updated 6 July 2004, CRS Report for Congress. <http://fpc.state.gov/documents/organization/35133.pdf>.
- Swire, P.P., and R.E. Litan. 1998. *None of your business: world data flows, electronic commerce, and the european privacy directive*. Washington, DC: Brookings Institution Press.
- Waters, N. 2003. The European influence on privacy law and practice. *Privacy Law & Policy Reporter* 9: 150–155.
- Westin, A.F. 1967. *Privacy and freedom*. New York: Atheneum.
- Rice, Denis T. Privacy in cyberspace: A primer. [http://www.howardrice.com/uploads/content/privacy\\_cyber.pdf](http://www.howardrice.com/uploads/content/privacy_cyber.pdf).
- Yi, C.-B., and K.-J. Ok. 2003. Korea's personal information protection laws. *Privacy Law & Policy Reporter* 9: 172–179.

# Chapter 9

## Monitoring Employee's E-mail: An E-privacy Concern

Yimeei Guo and Ying Luo

**Abstract** Monitoring employees is a standard practice in many workplaces, although the reasons for monitoring can vary greatly. While there is no doubt that employee monitoring is becoming a standard practice, companies need to ensure that it complies with legal requirements and does not unduly affect the employment relationship. Viewing from the protection of e-privacy in the workplace, this article discusses the notion of privacy and e-privacy at first, then examines law governing employee monitoring in various jurisdictions mainly in Germany, USA, and China as well. Finally, this article provides corporate operators some practical guidance on achieving compliance.

**Keywords** Employee monitoring · E-privacy · Practical guidance

### 9.1 Introduction

Monitoring employees is a standard practice in many workplaces, although the reasons for monitoring can vary greatly. Some company monitors to protect employees, for example, where they work in hazardous environments, and it is essential to ensure that safe working practices are being followed. Others may be under legal or regulatory obligations to monitor, for example, in the financial services sector. Most companies, however, primarily monitor to check their employees' performance. Monitoring may also be specifically targeted, for example, to detect misconduct or to ensure compliance with certain company policies and procedures.

---

(Published by "Proceedings of the 3rd international conference on innovation & management", Vol. II, 2006.12.1-3, pp.1011–1098, <ISSHP indexed>).

---

Y. Guo (✉) · Y. Luo  
Management Science Department, Xiamen University, Xiamen 361005,  
People's Republic of China

According to a most recent investigation involving 406 US and British companies which have more than 1,000 employees (*Proofpoint, 2006*), over 1/3 of such companies appointed personnel to monitor their employees' e-mail. Although the advantages to the company may be obvious, the adverse impact of monitoring employees is perhaps less apparent. A company may view employee monitoring as essential to the effective and efficient running of its business. However, if employees are permitted to use telephones, e-mail and Internet for personal use, it may be difficult for companies to draw a distinction between work and private information and activity, and limit monitoring to the former. On the contrary, even though employees may expect and accept the monitoring of their work, monitoring of their private information and activity is likely to be much less welcome.

A company's failure to consider the adverse impact of monitoring on employees can interfere with, or ultimately destroy, working relationships; it can also amount to a criminal offense. For instance, in May 2005, the former CEO and five other executives of Sonera, the Finnish telecom company, now TeliaSonera, were given fines or between 6 and 10 month suspended sentences by a Finnish court for illegally keeping logs on e-mails and telephone numbers dialed by employees, in an effort to identify who had leaked information about management disputes to mass media (Wugmeister et al. 2005).

Viewing from the protection of e-privacy in the workplace, this article discusses the notion of privacy and e-privacy at first, then examines law governing employee monitoring in various jurisdictions mainly in German, USA, and China as well. Finally, this article provides corporate operators some practical guidance on achieving compliance.

## 9.2 What Is Privacy/E-privacy?

The notion of privacy was first postulated in a Harvard Law Review article (Warren and Brandeis 1890), which described privacy as "the right to be let alone" when they were offended by press coverage of their families, and by "recent inventions and business methods." It took almost 20 years before the American courts issued judgments which adopted that principle.

Later on in another article (Prosser 1960), four different types of invasions of privacy were pointed out, including:

- appropriating an individual's name or likeness for commercial benefit;
- unreasonable intrusion or interference with an individual's interest in solitude or seclusion;
- publicly disclosing private facts; and
- publicly placing an individual in a false light.

From an information technology (IT) perspective, a much better definition of privacy has been that of Alan Westin, where he described privacy as: "The claim of individuals, groups, or institutions to determine for themselves when, how, and to

what extent information about them is communicated to others.” This definition embodies the concept of “*fair information practices*” which forms the basis for many of the regulatory and voluntary data protection schemes.

In short, “privacy” is not just a matter of what is kept secret. In the context of e-commerce/e-business and e-government, the right to privacy, i.e., e-privacy is really “*the right to control the use of personal information*” that is disclosed to others.

## 9.3 E-mail Monitoring Regulations in Various Jurisdictions

### 9.3.1 Germany

In Europe, the general right to privacy is derived from the European Convention on Human Rights, which governs Council of Europe member states, and the Data Protection Directive (95/46/EC), applying to EU member states. There are differences, however, in the way that EU member states such as France, Germany, Sweden, and the UK have implemented the provisions of the Directive. To save the length, this paper chooses Germany as an example.

The monitoring of employees' Internet use is governed by employment law, collective agreements, data protection legislation, constitutional and human rights law, and telecommunications law. The result is complex, and whether the Internet use can be monitored depends on a number of individual circumstances.

As the constitutional and human rights law overlays all other regulation, the general view is that blanket monitoring infringes an employee's rights and, because they cannot be waived, collective or individual agreements to monitor Internet use are unlikely to be valid.

The Telecommunications Act 2004 (*the Act*) specifically provides for the privacy of electronic communications. It is largely thought that, by expressly or impliedly permitting private use of the Internet by employees, a company becomes a provider of telecommunications services to them. The privacy right under *the Act* can be waived, within the limits of constitutional boundaries, but a company that has tolerated private Internet use at work without an express written policy may find itself in a difficult position, because it would already be bound by *the Act*, and a change of policy might be met with resistance from the workforce or the works council.

Where a company has expressly forbidden private use of the Internet at work, data protection law, employment law, and the constitutional principles combine to form a set of complicated rules. In essence, where there is no express Internet monitoring agreement, individually with the employee or collectively with the works council, monitoring is only allowed to the extent that it is based on a concrete suspicion against an individual employee for breaching the Internet policy, or it is necessary to assess the employee's performance due to the nature of his job. Any monitoring must be kept to the necessary minimum and must be announced in advance. If a works council exists, it must expressly consent to each individual monitoring measure.

Because of the limited rights of companies to monitor, express agreements with employees or works councils are advisable. However, there is a risk that agreements will be void on the basis that they were obtained under duress, especially if they are wide-ranging and presented as a condition of employment. An express detailed agreement with the works council on a policy for the use of technology and its enforcement is usually the best way forward.

### 9.3.2 US

US law generally allows monitoring of employees provided they have no reasonable expectation of privacy. As a result, if companies have given employees clear notice that they will monitor public areas and technology resources, employees generally will have no reasonable expectation of privacy and a company can monitor.

Under federal law, corporate monitoring of e-mails is governed primarily by the Electronic Communications Privacy Act of 1986 (*18 USC §§ 2510 et seq.*) (*ECPA*). What a company can monitor turns on whether the employees' messages are intercepted during transmission or are retrieved from storage on the company's server.

Interceptions of online communications (that is, monitoring messages as they are transmitted) are subject to the most stringent restrictions of *ECPA* and are permitted only in limited circumstances. For employers' purposes, the exceptions most likely to apply are as follows:

- Prior consent is given by at least one party to the communication.
- Interception is necessary to provide the service or to protect the rights or property of the service provider.

Employee communications stored on a company's server can be read by it regardless of whether either of the above exceptions applies. The company is therefore relatively free to monitor stored e-mails as long as the expectation of privacy has been removed (*Fraser v Nationwide Mutual Insurance Company*, 352 f.3d 107 <3rd Cir 2003>).

Similarly, if a company provides, in its technology use policy, that it reserves the right to, and will in fact, monitor employees' Internet use, there are few legal impediments to that monitoring.

### 9.3.3 China

The law on employee monitoring varies significantly between different Asia-Pacific jurisdictions. Several have adopted a model similar to the USA, where giving notice to the employee is a necessary and sufficient requirement for the company to monitor. Others, such as Hong Kong and Japan, have adopted

far-reaching guidelines supplementing the legislative framework and imposing strict requirements on data collected from employees. South Korea's approach is more similar to that taken in Europe. Here, this article takes China including Hong Kong, Mainland China, and Taiwan as a sample for discussion.

According to a Web@Work survey (*Websense, 2005*), across eight regions of the world, 83 % of respondents said they surfed non-work-related Web sites during office hours. Chinese office workers are the worst, concludes the survey, because they spend more than 1 h a day on personal usage. Specifically, Chinese employees spend 5.6 h per week on personal Internet usage in the workplace, 1.4 h more than the average of 4.2 h for companies in the Asia-Pacific region.

But employers in China are taking notice. For instance, Ruideng Communications, a Sichuan company, recently installed eight micro-cameras in the ceiling, overlooking all the office's computers. Productivity has shot up, but some employees feel uneasy about the surveillance and have complained about a "loss of privacy." TCL, the world's largest TV maker, has a strict policy on Web access. Its IT department uses specially designed software to track and record all online activities of all employees. TCL R&D staffs are not allowed to use third-party instant messenger (IM) platforms such as MSN.

As pointed out by one legal expert (Zhao 2003), whether or not business security or employee's privacy is indeed more important is not clearly provided by law in Mainland China. By referring to foreign legislative examples, it is the basic solution to solve such problem to award a right for business to monitoring its employee's e-mail under certain conditions and make a clear cut between infringing citizens privacy right and maintaining business' sound interest.

In Hong Kong, the Personal Data (Privacy) Ordinance 1997 (*the Ordinance*) applies to employee monitoring and allows the Privacy Commission for Personal Data to adopt guidelines. In December 2004, the Privacy Commissioner adopted guidelines on employee monitoring of e-mail, Internet, and telephone use and CCTV monitoring.

There are potentially serious consequences if *the Ordinance* requirements are not met. A company may be exposed to:

- Civil compensation to individuals who suffer damage.

Enforcement notices served by the Privacy Commissioner (for example, when an aggrieved party complains). Non-compliance with an enforcement notice carries a penalty of between HK\$25,001 (about US\$3,200) and HK\$50,000 (about US\$6,400) and 2 years' imprisonment.

As to Taiwan, although there is a constitutional right to privacy (*Article 12, Constitution 1946*) and detailed data privacy legislation has been in place since 1995, the clearest statement of employee privacy law is found in Taipei district court case law in 2003 adopting the reasonable expectation test.

Under this test, one company can only monitor employees' e-mails if they do not have a reasonable expectation of the privacy of their work e-mails (for example, where employees have been provided with a clear e-mail monitoring policy).

## **9.4 Conclusion and Suggestion**

Even where companies can justify monitoring employees' activities, it may still be advisable for them to strike a balance between the legitimate need to run their businesses in the best way they see fit and respect for their employees' private information and activities. While there is no doubt that employee monitoring is becoming a standard practice, companies need to ensure that it complies with legal requirements and does not unduly affect the employment relationship. Here, this article tries to put down some tips for companies' compliance as follows:

### ***9.4.1 Providing Notice by Implementing and Disseminating a Technology Use Policy***

Notify employees of any anticipated intention to monitor. This overcomes any employee expectation of privacy in using the company's e-mail or accessing the Internet while at work. If a halfway approach is taken (for example, by allowing employees limited personal use of IT equipment), a company policy should be clearly set out.

### ***9.4.2 Stating the Reasons for the Monitoring***

Include in any e-mail or Internet use policy a statement of the reasons for monitoring (for example, to ensure compliance with company policies or the proper functioning of the computer systems, or to monitor an employee's performance).

### ***9.4.3 Proportionality of the Monitoring***

Be clear about the reasons for monitoring. In principle, monitoring should be limited to the extent necessary to achieve a certain legitimate aim. If it can be carried out on a less intrusive basis (for example, monitoring only the number of e-mails sent or amount of time spent on the Internet), then this should be used. Ensure that local laws can be complied with once the personal data has been collected (see below).

### ***9.4.4 Complying with Local Laws***

Provisions vary dramatically between jurisdictions. Do not ignore local laws and adopt, for example, a US approach across jurisdictions. Such an approach runs a serious risk of non-compliance.

As well as complying with any notice requirements, remember that many jurisdictions require a legal basis for monitoring, such as employee consent, or conducting a balance of interest test where the company's interest in monitoring outweighs the employee's right to privacy. Verify whether there are any applicable exceptions for employee monitoring.

### 9.4.5 Conduct Training

Once a policy is implemented, conduct training sessions to raise employees' awareness of monitoring and its purposes.

### 9.4.6 Audits

Conduct regular audits at least annually to ensure that policies are current, applicable, and being followed (Wugmeister et al. 2005).

## References

- 1/3 of US and British companies stole a Glance at their employees' E-mail, Beijing Youth Times, <http://www.yynet.com/view.jsp?oid=9647857>, 6 June 2006.
- Boufford, John G. 1998. Privacy on the information highway. *University of New Brunswick Law Journal* 47: 219.
- Prosser, William. 1960. Privacy. *California Law Review* 48: 383.
- Wugmeister, Miriam, Ann, Bevitt, Peter J. Edlind, and Ritter, C. 2005. *Employee monitoring: Highlighting the issue*, <http://www.mofo.com/news/updates/files/update02051.html>, Aug 2005.
- Warren, S., and Brandies, L. 1890. *Privacy*, *Harvard law review*. pp. 207–208.
- Westin A.F. 1967. *Privacy and freedom*. New York: Atheneum, at 7.
- Zhou, Raymond, and Zhuoqiong, Wang. 2005. Chinese office workers world's worst in cyber slacking, China Daily page 1. [http://www.chinadaily.com.cn/english/doc/2005-08/18/content\\_469947.htm](http://www.chinadaily.com.cn/english/doc/2005-08/18/content_469947.htm). 18 Aug 2005.
- Zhao Limei. 2003. *Analysis and research on legal problems about E-mail (in Chinese)*. <http://tech.sina.com.cn/news/review1/2000-04-21/23363.shtml>, 13 May 2003.



# Chapter 10

## Privacy Concern in CRM Service

Yimeei Guo and Haiyu Huang

**Abstract** Customer relationship management, known as CRM, is a concept for increasing companies' profitability by enabling them to identify and concentrate on their profitable customers. Electronic commerce customer relationship management or ECCRM chiefly relies on Internet or Web-based interaction of companies with their customers. As a tool of CRM, the purposes and methods of data mining for firms are manifold and often help the firms to analyze business-critical data including person-related information. Indeed, there are norms in the USA and European Union that should be taken into account when implanting a CRM system. This paper reviews the US and EU CRM service-related legal regimes with emphasis on privacy protection at first. Then, it discusses the privacy concern in CRM service by doing some case study, mainly in the States. Finally, this paper probes into some practical suggestions for enterprises' better CRM service reference.

**Keywords** CRM · ECCRM · Data mining · Privacy concern

### 10.1 Introduction

Customer relationship management, known as CRM, is a concept for increasing companies' profitability by enabling them to identify and concentrate on their profitable customers. From a strategic point of view, CRM closely combines the most advancing information technologies (IT) together: Internet and electronic

---

Published by "Proceedings of Int'l Symposium on China Hospitality Management & Business Information 2007", August 7–9, 2007, pp. 533–538.<ISTP indexed>

---

Y. Guo (✉)  
School of Law, Xiamen University, Xiamen, China

H. Huang  
School of Management, Xiamen University, Xiamen, China

commerce, multimedia technology, data warehouse, and data mining, expert system and artificial intelligence, etc. Briefly speaking, CRM provides for the field of companies' sales, customer service center, decision-making support, etc., a solution to business automation.

CRM can be viewed from two perspectives. *Operational CRM* refers to the business strategy that focuses on the day-to-day management of the customer relationship across all points of customer contact and is enabled by sales and service technologies. *Analytical CRM* is the part of the CRM business strategy that drives increased customer intelligence and makes information actionable across all touch points. It encompasses a host of data mining applications (e.g., marketing, forecasting, and budgeting) that enable companies to develop greater customer intelligence and accordingly customer-specific strategies.

In analytic CRM, data miners often analyze customer data with the specific intent of understanding individual behavior and instituting sales campaigns based on this understanding. Researchers in economics, demographics, medicine, and social sciences are trying to understand the relationships between behaviors and outcomes (Edelstein and Millenson 2003). For example, if an employer has access to medical records, they may screen out people with diabetes or have had a heart attack. Screening out such employees will cut costs for insurance, but it creates ethical and legal problems.

As to ECCRM, it chiefly relies on Internet or Web-based interaction of companies with their customers. The prospect of higher profitability has lured many companies into launching CRM initiatives and, in particular, ECCRM projects as a central element of their electronic commerce activities. Market projections at the time of the Internet hype saw corporate investments into CRM in general grow at annual rates as high as 50 %, eventually matching and surpassing expenditure on ERP systems (Meta Group 2000). Even after the end of the hype, there are projections still predict double-digit growth rates for the years to come (Forrester Research 2002).

The fast progress in networking technologies has led to an enormous amount of digital information stored all over the world. This process has been accompanied by a rise of tools, e.g., data warehouse and data mining that are able to collect data, add them to databases and find information that could not be discovered in an obvious way. The analysis of huge data amounts is of particular relevance in e-commerce, where companies are given the opportunity to learn more about their customer profitability and customer segmentation. While yielding benefits to the companies (marketing, etc.), these analyses of customer behavior, preferences, and interests may provoke the fear of privacy breaches (Kobsa 2002).

Therefore, the legal aspects of CRM including ECCRM, the laws affecting it among others, cannot be forgotten. Indeed, there are norms in the USA and European Union that should be taken into account when implanting a CRM system. This paper reviews the US and EU CRM service-related legal regimes with emphasis on privacy protection at first. Then, it discusses the privacy concern in CRM service by doing some case study, mainly in the States. Finally, this paper probes into some practical suggestions for enterprises' better CRM service reference.

## 10.2 US and EU CRM Service-related Legal Regimes with Emphasis on Privacy Protection

As a tool of CRM, the purposes and methods of data mining for firms are manifold and often help the firms to analyze business-critical data including person-related information. The knowledge about customers is a valuable asset for the company in a competitive landscape no matter online or offline. However, data privacy protection regulations rightfully limit the use of person-related data.

### 10.2.1 The USA Data Privacy Laws and Regulations

Although the USA had no comprehensive privacy law, Congress had passed *the Children's Online Privacy Protection Act (COPPA)* in 1998. It had also passed regulation of online privacy practices in health and financial services, namely, *the Gramm-Leach-Bliley Act of 1999* applying to financial institutions and *the Health Insurance Portability and Accountability Act (HIPAA) of 1996* applying to health care providers. The Federal Trade Commission (FTC) and the National Telecommunications and Information Administration (NTIA) are the two bodies charged with monitoring online privacy.

Currently, the FTC has taken the lead in enforcing privacy rules in the USA. The FTC requires companies to follow evolving privacy rules labeled “*Fair Information Practice Principles*” (FIPPs) including:

- **Notice/Awareness:** Web site is required to provide consumers notice of their information practices, such as what information they collect and how to use it.
- **Choice/Consent:** Web sites are required to offer consumers choices as to how that information is used beyond the use for which the information was provided (for example to consummate a transaction). In other words, customers must be able to “opt-out” or must affirmatively “opt-in” to information collection practices.
- **Access/Participation:** Web sites are required to offer consumers reasonable access to that information and an opportunity to correct inaccuracies.
- **Security/Integrity:** Web sites are required to take reasonable steps to protect the security and integrity of that information.

### 10.2.2 US Safe Web Act of 2006

On December 9, 2006, Congress approved S. 1608, *the “Undertaking Spam, Spyware, And Fraud Enforcement with Enforcers beyond Borders Act of 2006”* (known as *the US Safe Web Act of 2006*). *The Act* amends *the Federal Trade Commission Act (FTCA)* and improves the FTC’s ability to protect consumers from international fraud by: (1) improving the FTC’s ability to gather information

and coordinate investigation efforts with foreign counterparts; and (2) enhancing the FTC's ability to obtain monetary consumer redress in cases involving spam, spyware, and Internet fraud and deception.

### ***10.2.3 The European Union***

The roots of European data protection law lie in the European Convention of Human Rights. The Convention aims to find a balance between the privacy of individuals and freedom of expression, including the economic rights of companies to market. By the 1980s, many European Community (EC) states (notably Germany and the United Kingdom) had data protection laws designed to protect citizens' privacy. The EC felt it needed to regulate to ensure that there were similar rules in every country in the EC, so as to allow free movement of data across Europe. This move was both pro-consumer and pro-trade. EC law therefore evolved to afford some basic protections to individuals concerning how personal data about them is collected and used.

So far, the European Union (EU) has developed privacy regulations much stricter than the mostly voluntary approach for most US entities. Violations of *European Data Protection Directive* (1995/46/EC) may result in civil monetary fines, criminal sanctions, and injunctive measures such as blockage of data transfers and injunctions against violated data practices. Also, a new EU anti-spam law—“*Directive 2002/58/EC*” came into force on December 11, 2003, and is already having a dramatic effect on the amount of ‘spam’ sent to computer users.”

In addition to legislative measures, the European Commissioner for Information Society encouraged greater international cooperation and development of technological solutions to move toward eliminating spam. The Commission also called on greater cooperation among the OECD countries, including self-regulation.

## **10.3 Case Study on CRM Service Provoking Privacy Breaches**

### ***10.3.1 CVS and Giant Food***

In 1998, the Washington Post reported that CVS drug stores and Giant Food were disclosing patient prescription records to a direct mail and pharmaceutical company. The company was using the information to track customers who failed to refill prescriptions and then sending them notices, encouraging them to refill and to consider other treatments.

Due to public outrage and perhaps the concern expressed by senators crafting legislation on the issue of health privacy, CVS and Giant Food agreed to halt the marketing disclosures.

### ***10.3.2 Amazon.com***

The purchase circles, which Amazon.com introduced on Aug. 20, 1999, comprised thousands of best-seller lists that enabled customers to browse and see what books, music, and videos were popular among various groups of people—by categories that include geography, employer, university, or professional organization.

To generate the lists, Amazon mined the data that all of its customers provided when they shopped: a shipping address, an e-mail address, and the list of items bought. The shipping addresses let it create its best-seller lists based on geographic areas like towns or foreign countries. Using the Internet domain name in the e-mail address, Amazon can often identify a customer's employer or college, for example. The lists gave no actual sales figures. Nor did the purchase circles identify individual buyers, even though Amazon.com's database was capable of doing so.

Whatever Amazon.com motivated, once word began circulating of Amazon.com's new program, privacy-rights advocates began sounding alarms. Finally, Amazon.com said that it would adjust the program by letting customers request that their buying habits not be included in the "purchase circles," as the listings are known.

### ***10.3.3 Toysmart***

Toysmart, an Internet retailer, closed its doors in the summer 2000 because it could not meet its financial obligations. The firm placed an ad in the Wall Street Journal seeking a buyer for its 250,000-name customer file, which contained customers' names, addresses, billing information, shopping preferences, and even data about children such as their birthdays. Other customer lists, such as the 200,000-name list from Living.com, was selling for \$100 per 1,000 names; at that price, Toysmart would only receive \$25,000 for its customer list.

Customers, state attorney generals, and the FTC objected to the sale of its customer list because Toysmart's privacy policy explicitly stated that it would not sell customer information to third parties. Toysmart reached an agreement with the FTC that enabled it to sell the customer list to a company in a similar business that would agree to abide by Toysmart's privacy policy.

However, Toysmart did not receive an offer from any such company, and the Walk Disney Company that owned a 60 % share in Toysmart through the Buena Vista Internet Group purchased the customer file for \$50,000 so that the list could be destroyed.

### ***10.3.4 DoubleClick***

DoubleClick is an Internet advertising company that is one of the leaders in developing online banner advertising. On November 23, 1999, DoubleClick consummated its acquisition of Abacus Direct Corporation. Abacus is in the business of providing specialized consumer information to direct marketers. This acquisition would have allowed, for the first time, an Internet advertiser to match actual names with other personal information that is “anonymously” collected online.

DoubleClick’s announcement of its intention to merge the databases elicited a firestorm of criticism. On March 2, 2000, DoubleClick announced that it would delay its plan to merge its databases with those of Abacus. There is little question that the DoubleClick fiasco contributed to the willingness of the Network Advertising Initiative, an industry group of which DoubleClick is a member, to reach a compromise with the FTC in July 2000. Ultimately, in January 2001, the FTC closed its investigation of DoubleClick without taking action, concluding that DoubleClick had not violated its privacy policy.

In sum, the DoubleClick incident provides ample evidence that the public concern over Internet privacy has real-world implications for any business.

### ***10.3.5 Cingular v. Data Find Solutions et al.***

According to Atlanta’s US District Court filings, Tamarac, Fla.-based First Source Information Specialists Inc. had used several Web sites to provide cell phone numbers, reverse lookups for cell phone numbers (which provide the names of callers using such phones) and—for prices ranging from \$110 to \$195—records of calls made from a particular cell phone number.

Atlanta-based Cingular Wireless, the complaint accused that the defendants “engage[d] in deceit, trickery, and dishonesty to obtain private information from Cingular’s (customer service representatives) through ‘social engineering,’ improper hacking and/or through unauthorized access to online account information stored on Cingular’s database.” (The term “social engineering”—once used to describe governmental or cultural policies aimed at influencing public behavior—has acquired a new meaning as data miners and “phishers” seek to obtain information by gaining the confidence of targets through trickery.)

Among the techniques used to gather the proprietary, confidential information, Cingular said, were instances of the defendants or their employees using customers’ passwords to access their accounts, pretending to be Cingular customers seeking information about their own accounts or posing as “fellow [Cingular] employees facing an urgent access problem in accessing a customer account.”

Following up on an earlier default judgment, on Nov. 9, 2006, Judge Clarence Cooper ordered that data miners—First Source and company principals Kenneth

W. Gorman and Steven Schwartz disgorge all profits and pay Cingular compensatory and punitive damages and attorney fees at the amount of \$1,135,00.

Finally, it is noteworthy that Expedia.com, the largest US online travel agency, and other five Web sites were judged in 2003 on their privacy and security policies, customer service, and clear disclosure of advertising relationships, usability and content. The winners were praised for promising to maintain customer privacy, enabling easy navigation through the site and providing a satisfying online experience. Also, Customer Respect Group analyzed privacy policies of 464 major companies in 2005. Expedia is one of the top 10 companies rated for privacy.

## 10.4 Conclusion and Suggestions

From the captioned case study, we can find out that privacy had become the No. one policy issue affecting customer relationships on the Internet. Proper handling of personal information was not just a moral and ethical requirement; it was a strategic necessity if not a strategic advantage in e-commerce. And it was not just a concern to Internet firms selling to consumers; privacy affected any enterprise operating on the Internet that came in contact with personally identifiable information.

Nevertheless, purchasing a CRM system is a complex and high profile corporate activity. Companies must address the business case, systems implementation challenges and change management issues. Against this background, it is unsurprising that customer privacy concerns often take a back seat role.

Yet some major corporations do take the privacy issue seriously because of legal compliance requirements and corporate governance repercussions—and because consumer privacy has become a customer relationship issue in itself. Customers often cite unsolicited telephone calls, sale of mailing lists, and unsolicited emails (i.e., spam) as their top information privacy concerns.

Comparatively speaking, the EU legislation calls for a transparent and consent-based approach to handling personal data, whatever the purpose is. The US regulation avoids blanket legislation but addresses some privacy concerns with focused laws (for instance aimed at the banking sector, or currently, cutting out spam). Without EU-style government intervention, US companies have often self-regulated, appointing chief privacy officer (CPO) in response to the customer trust issue.

For instance, IBM, Microsoft, HP, and many other major players in the technology industry have appointed CPO. Even before its acquisition of Abacus incident, DoubleClick had been one of the first firms to appoint a CPO, and one of the very few firms where such a person reported directly to the Chairman and not to a legal counsel. Surprisingly, European companies have been less quick to follow the US example. This is despite Europe's far more protective, pro-consumer data protection laws.

As to data miners, they should solicit people's cooperation. Every organization gathering data can ask people to sign a form granting permission to use the data

(known as opt-in) or acquire their permission implicitly when they do not revoke it (opt-out). They could also respond with regulations about what data may be collected and how it can be used. In the EU states, there are already strict laws that prohibit the use of personal data without the individual's explicit opt-in.

Notably, in the USA, health-related companies and researchers are constrained by *HIPAA* as mentioned above, which provides a national standard for the protection of information relating to an individual's health. *HIPAA* provides for some limited use of the data collected for marketing purposes. For many purposes, however, the data must be stripped of all fields that would enable an individual to be identified, such as name, address, date of birth, and Social Security number.

Therefore, data miners must be sensitive to these worries when collecting or using data, or else they risk burdensome and counter-productive regulation just as shown in the *Cingular's* case. Although the captioned US companies have created the role of CPO to oversee the protection and use of data, yet, this charter should be extended to explain how the data would be used to the ultimate advantage of the people whose personal information is captured in the database.

Finally, viewing that the USA and EU have clear and definite legal guidelines on privacy breaching problem arising from CRM service, it is suggested by this paper that the task of the greatest urgency at present for other countries be to endeavor to resolve such problem. For instance, whether or not utilizing CRM will definitely infringe one's privacy in China is still without a general rule, since there is no law explicitly regulating the relationship between privacy right and CRM.

## References

- Amazon Tries to Ease Privacy Worries. 1999. <http://www.taborcommunications.com/dsstar/99/0907/100984.html>.
- Berman, Jerry, and Mulligan, Deirdre. 1999. Privacy in the Digital Age: Work in Progress. *Nova Law Review* 23(2): 551.
- Briskman, Simon. 2004. *CRM: Don't forget about privacy*. <http://management.silicon.com/government/39024677,39124925,00.htm>.
- Dong, Jinxiang, Gang, Chen, and Yin, J. 2002. *Customer Relationship Management*. Zhejiang, China: Zhejiang University Publishing Co.
- Edelstein, Herb and Millenson, Janet. 2003. *Data mining in depth: Data mining and privacy*. DM Review Magazine.
- European Commission Continues to Combat Spam. 2004. [http://europa.eu.int/comm/research/headlines/news/article\\_04\\_03\\_11\\_en.html](http://europa.eu.int/comm/research/headlines/news/article_04_03_11_en.html).
- Forrester Research. 2002. *Forrester Research Predicts Growth for Customer Relationship Management (CRM) Market Through 2007*. <http://www.forrester.com>.
- Greg, Land. 2006. *Cingular Wins \$1.1 M Victory over Data Miners*. Fulton County Daily Report. <http://www.law.com/jsp/article.jsp?id=1164636901736>.
- Jarvenpaa, Sirkka L., and Tiller, Emerson H. 2001. *Online Consumer Privacy: DoubleClick, Amazon, and eCustomers*. <http://btl.mccombs.utexas.edu/IBM%20Course%20modules/IBMPrivacy10.pdf>.
- Kobsa, Alfred. 2002. Personalized Hypermedia and International Privacy. *Communications of the ACM, Special Issue on Adaptive Web-based Systems and Adaptive Hypermedia* 45(5): 64–67.
- Lefons, Ezio, Silvestri, Alberto, and Tangorra Collins, K. 2001. 'Analytical CRM: Driving Profitable Customer Relationships'. *Strategic Planning*. SPA-12-7120.



- Meta Group. 2000. Meta Group Sees Continued Strong Growth for Customer Relationship Management (CRM) Initiatives: Projects a 50 % Annual Growth Rate for Global CRM Market. Press release available at <http://www.metagroup.com>.
- Paula Crouch Thrasher. 2003. *Expedia, Travelocity get top consumer marks*, Cox News Service. <http://www.jsonline.com/story/index.aspx?id=125502>.
- Privacy Concerns May Tame Internet. 1998. <http://www.cbsnews.com/stories/1998/04/08/tech/main6851.shtml>.
- Privacy-ch2: Why Business Cannot Afford to Disregard Consumer Privacy Concerns. 2002. <http://www.law.com/pdf/sfb/PrivacyCh02.pdf>.
- Schoder, Detlef, and Nils Madeja. 2004. Is Customer Relationship Management a Success Factor in Electronic Commerce? *Journal of Electronic Commerce Research* 5(1): 38–53.
- Top privacy policies: Intel, Expedia, e-Loan. 2005. <http://www.itfacts.biz/index.php?id=P4373>.

# Chapter 11

## Internet Industry's Legal Risk and Solution to Personal Privacy Infringement

Yimeei Guo, Weiwei Hu and Zhengzheng Fang

**Abstract** In recent years, Internet industry has borne the legal risk to infringe users' personal privacy. This article wants to figure out some plausible solutions to help Internet industry to prevent the legal risk in advance.

**Keywords** Personal privacy · Internet industry · Legal risk · Solutions

### 11.1 Introduction

Following the day after day evolution and popular usage of Internet and mobile communication, the service category and function provided by Internet operator also becomes more and more various, from news, multimedia visual sound, Street View to book and material research, etc. The users only need moving fingers; then, they can easily obtain relevant messages which they want to understand. Those services provided for free are quite super valuable welfares for the users.

However, at the same time, the users will confront the risk of their personal privacy being infringed as well. For example, Google's Street View photographing vehicle took a picture on personal privacy scenery. It also collected e-mails, URLs, and passwords from unsecured wireless networks around the world. As to Internet operators, this means the legal risk of being sued by privacy infringement. For instance, on December 23, 2010, the US iPhone and iPad users collectively filed a lawsuit in federal court in San Jose, California, against Apple's revealing personal information. They asked the court to prohibit such action without their permission and award damage (Legaldaily 2010). Therefore, how to use personal information and effectively protect personal privacy by Internet industry is worthy for us to pay attention to and put it into consideration. Finally, this article hopes to figure out some plausible solutions to help Internet industry to prevent the legal risk in advance.

---

Y. Guo (✉) · W. Hu · Z. Fang (✉)  
Law School, Xiamen University, 361005 Xiamen, China  
e-mail: ymguo@xmu.edu.cn

## 11.2 Recent Emerging Online Personal Privacy Infringement Disputes

Firstly, there are emerging disputes regarding personal privacy infringed by Internet industry in several countries, which tend to increase more and more. Here are selected examples as follows:

- In July 2010, a researcher of American Network Security Consulting Firm “Skull Security” utilized “spider software” to collect 0.1 billion user data of not amended privacy setting from Facebook (Du Tianqi 2010).
- On October 18, 2010, the Wall Street Journal (WSJ) had reported that the 10 most popular Facebook applications, including Farmville and Texas HoldEm Poker, were sending user identifications to 25 companies, some of which were advertising firms and some of which built behavioral tracking databases containing information about users’ behavior, which is against Facebook’s rules. The WSJ reported that the user ID data were passed on even in the case of users whose privacy settings were set to maximum, meaning that users could do nothing to stop it happening (Du Tianqi 2010).
- On October 22, 2010, WSJ alleged that the MySpace ad transferred the Web address of the originating page, and that Web address contained the user ID of the user. Some apps are also transferring user IDs, the Journal’s report found. The apps included BitRhymes Inc.’s TagMe, WonderHill Inc.’s GreenSpot, and RockYou Inc.’s RockYou Pets (Mark Hachman 2011).
- WSJ conducted a similar investigation earlier in the same week with Facebook, also concluding that many of its top apps were also transferring personal identification information (Mark Hachman 2011).
- On December 2010, Qihoo 360, a China’s online security provider, has been accused by Kingsoft Network Technology of collecting and leaking the private information of its users, igniting rounds of recrimination between the two Chinese Internet companies (Zhang 2011).

Secondly, there were some pending or decided cases overseas involving Internet industry’s infringing users’ privacy as follows:

- On October 18, 2010, the Spanish Agency for Data Protection (AEPD) has opened disciplinary proceedings against Google for alleged violation of the country’s data protection laws, following an investigation launched in May and forwarded its findings to a Madrid court. It said it had evidence of five offences committed by Google involving the capturing and storing of data from users connected to Wi-Fi networks while collection photographs for Street View, and the transfer of such data to the United States (Spanish agency sues Google over Street View 2010).
- On May 17, 2010, Oregon and Washington residents file class action lawsuit against Google over alleged Google street view (“GSV”) WI-FI invasion of privacy and seeks injunctive relief barring Google from destroying or altering payload data collected in Oregon and/or Washington (GSV 2010).

- On August 20, 2010, the operator—YU Wusen of Campax English Consulting Firm in Taichung, Taiwan—directed program designer Xu Shengwei to steal Columbia Group.com's 24,307 clients' data for promoting business. After Columbia Group brought the lawsuit for damage compensation, Taichung District Court ordered Campax, YU Wusen, and Xu Shengwei to pay Columbia Group NT\$15,000,000 severally (Campex 2010).

Besides, there are foreign investigated or prosecuted cases related to Internet industry's infringing users' privacy and settled finally as follows:

- In the US Federal Trade Commission's first case against a social networking site, Twitter agreed to establish a security program that will be audited by another company. According to an FTC news release issued around late June 2010, Twitter "will be barred for 20 years from misleading consumers about the extent to which it maintains and protects the security, privacy and confidentiality of nonpublic consumer information." (Natasha Watkins et al. 2010)
- On September 3, 2010, Google has agreed to pay \$8.5 million to settle a number of cases alleging that its Buzz social networking service violated their privacy rights. The money will be paid out to Internet privacy activists to use in their education and policy work (Google 2010).
- On November 30, 2010, the US FTC said it has reached a settlement with EchoMatrix over charges that it failed to inform parents that information it was collecting about their children would be disclosed to third-party marketers. As part of the settlement, EchoMatrix has agreed not to share or use information it has obtained from its Sentry program or any other program for purposes other than allowing registered users to access their accounts. It also requires the company to destroy information it has transferred from the Sentry program to its Pulse database (Gruenwald 2010).

### 11.3 An Overview of Foreign Precaution Against Online Privacy Infringement

The Internet has brought new concerns about privacy in an age where computers can permanently store records of everything: "where every online photo, status update, Twitter post and blog entry by and about us can be stored forever," writes law professor Jeffrey Rosen in New York Times on July 19, 2010. To control online personal privacy infringement, many countries have adopted some measures, e.g., The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) relating to data privacy. It governs how private-sector organizations collect, use, and disclose personal information in the course of commercial business. In addition, the Act contains various provisions to facilitate the use of electronic documents. PIPEDA became law on April 13, 2000, to promote consumer trust in electronic commerce. The Act also established the Privacy Commissioner of Canada as the ombudsman for privacy complaints.

In the United States, a variety of federal and state laws govern the collection and use of personally identifiable information such as the Children's Online Privacy Protection Act (COPPA), the Gramm–Leach–Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA). The European Union (EU) requires all member states to legislate to ensure that citizens have a right to privacy, through directives such as the “1995 Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.” It is regulated in the United Kingdom by the Data Protection Act 1998, and in France, data protection is also monitored by the CNIL, a governmental body which must authorize legislation concerning privacy before them being enacted.

In Asia, Japan has been hit by a raft of scandals involving the loss of personal data. Both Japanese and foreign firms operating in Japan have been hit. Alarmed at these problems, the Japanese government took measures to try to prevent such problems as well as cracking down criminally on particularly egregious cases. In April 2005, a law to protect personal information went into effect. The law requires a new regulatory infrastructure for the appropriate protection of personal information by businesses and the government. Each ministry will be required to come out with guidelines to cover the industries over which they have jurisdiction (Seeman 2003).

Besides, South Korea has adopted a data protection regime similar to the United States and Japan, with one act covering the public sector and sector legislation for the private sector. In July 2010, South Korea government pronounced that it would promote new ID which only revealed personal picture, birthday, and name to prevent personal data and privacy from infringement, and the personal sensitive information such as ID number, address, and fingerprints would be kept in the chip inside the ID to protect the card holder from leaking personal information while losing his or her ID.

## **11.4 The Status Quo of China's Online Privacy Protection Legislation**

Owing to historical reason, there is no strong sense of privacy protection in China; thus, there is no perfect and intact legal framework being established in China. As to online privacy protection, the legislation in China appears evidently scant. China still lacks a comprehensive legal framework to regulate the use and disclosure of personal data. Notable recent developments include the following:

- The promulgation of an amendment to the national Criminal Law in February 2009 to criminalize the sale or other unlawful disclosure of personal data by government officials and employees in key industries and
- The promulgation of the Torts Liability Law on December 26, 2009, and becoming effective on July 1, 2010, a long-debated measure with potentially important privacy implications.

In detail, on February 28, 2009, the Standing Committee of the National People's Congress ("NPC") promulgated the seventh Amendment to the Criminal Law of China. The Amendment, which also updates the Criminal Law in a variety of areas such as tax evasion and insider trading, makes it a criminal offense:

- (i) for employees of government institutions or private organizations in the financial, telecommunication, transportation, education, or medical sectors to sell or otherwise unlawfully provide to third parties the personal data of any citizen that has been obtained in the course of performing duties or services by their employers; or
- (ii) for any person to obtain such information by means of theft or other unlawful means.

If the violation is "severe," the individuals found guilty of either offense will be subject to imprisonment of up to 3 years and/or a monetary fine. The Amendment also specifically provides that organizations (such as corporate entities) that commit either offense shall be liable for a monetary fine and the responsible officers may be personally liable for criminal charges.

The Amendment is vaguely drafted. It does not define personal data, leaves unclear what types of disclosure will constitute "unlawful provision," whether and to what extent any authorization by the employer and/or consent by the data subject are relevant, and what factors will be relevant in determining whether a violation is "severe." Major national-level China's laws are often broadly drafted, and subsequent implementing regulations or interpretations of the Supreme People's Court may provide guidance on these questions in due course.

In the meantime, companies operating in China's financial, telecommunications, transportation, education, or medical sectors would be well advised to review their internal systems for preventing unauthorized disclosure of customer data, and all companies looking to acquire customer databases in China should take care to conduct thorough due diligence about the sources of such information.

The Tort Liability Law being effective on July 1, 2010, contemplates a wide-ranging reform and modernization of China's tort law. In addition to extensive provisions governing areas such as product liability and environmental pollution that are unrelated to data privacy, the law contains several novel provisions with potentially far-reaching data privacy implications. The Tort Liability Law appears to recognize an independent right of privacy. Unfortunately, little further detail is provided in the law; it will be necessary to wait for the Supreme People's Court to add flesh to these bare bones.

In addition to this potential elevation of the right of privacy, the Tort Liability Law provides that a party whose right to privacy is infringed is entitled to claim from the tortfeasor the profits arising from the breach. In addition to the right to claim damages for "emotional harm" (see Article 22) and actual loss that arises under the existing General Principles, a Web site operator who either acknowledges that a party's privacy or other rights are being infringed through content posted on its Web site, or who is warned of such infringement by an affected party and fails to remove the content or adopt other corrective measures, is jointly and

severally liable with the party having posted the content, and if an affected party requests registered information about the party that had posted infringing content and the Web site operator refuses to divulge such information, the Web site operator itself becomes liable for the infringement (see Article 36).

Notably, in 2005, the draft Personal Information Protection Measure (“Protection Measure”) was published and provided as follows: entities undertaking the commercial processing of personal data would require a permit from a new “personal data administrative authority” prior to collection of personal data; collection of personal data by non-government entities would generally require prior consent from the data subject; and the administrative authority would have the power to restrict the cross-border transmission of personal data to any jurisdiction that did not provide sufficient protection to such data.

The draft Protection Measure was merely a consultative document and has not been formally adopted by any part of the China government. Indeed, since the publication of the draft measure, attempts to introduce a national privacy law appear to have remained in limbo. Proposals for such a law have been submitted to the NPC several times since 2005. However, none of these proposals have yet come to fruition and it seems likely that the introduction of any such national privacy law remains some way off.

## 11.5 Suggestions and Conclusions

Generally speaking, the effect of preventing online personal privacy from infringing is not apparent. The British “Daily Electronic Message” reported that it was because people in the past did not form consensus against the seriousness of “online privacy revealing everywhere” and the development of network technology was too fast, whereas relevant laws could not catch up with. As to this phenomenon, the expert in this field suggests that there are two aspects concerning protecting personal privacy:

- Individual should have the sense of protecting privacy: should not easily reveal personal information and
- Some agencies and departments should also pay high attention on network security involving personal privacy and severely punish the party leaking other’s information.

As to China, to effectively protect online personal privacy, this article suggests that we can refer and adopt foreign legislative models by way of combining those two models of self-regulation (e.g., the USA) and heteronomy (e.g., EU). At the initial developing stage of network technology, China government may let the industry sectors make their own business regulation to protect the users’ privacy and apply such regulation as the minimum standard. If the Internet industry operators comply with such regulation, they can immune from liability. Meanwhile, China’s legislative body should enact some relevant laws to supplement the defect of weaker

binding force of self-regulation. With the combination of two captioned legislative models, China can take care of mutual benefit of Internet industry operators and users and can take care of mutual benefit of country and individuals and therefore make personal privacy be protected as it should be.

## References

- Campex was judged to compensate 15,000,000 for stealing personal data (in Chinese). <http://udn.com/NEWS/SOCIETY/SOC6/5799531.shtml>. Accessed 21 Aug 2010.
- Du Tianqi. To protect privacy becomes big difficulty (in Chinese) [N]. <http://www.chinaeclaw.com/News/2010-08-19/17120.html>.
- Google agrees \$8.5 m Buzz settlement as lawyers fail to find monetary damage. <http://www.out-law.com/page-11353>. Accessed 6 Sept 2010.
- Google Street View (“GSV”) Wi-Fi Privacy Class Action Lawsuit [N]. <http://classactionlawsuit.sinthenews.com/class-action-lawsuits/google-street-view-gsv-wi-fi-privacy-class-action-law-suit-filed>. Accessed 21 May 2010.
- Gruenwald Juliana, FTC Reaches Settlement With Firm Over Use Of Children’s Data. <http://techdailydose.nationaljournal.com/2010/11/ftc-reaches-settlement-with-fi.php>.
- Mark Hachman. 2011. Report: MySpace Exposes User IDs Via Apps, Ads [N]. <http://www.pcmag.com/article2/0,2817,2371359,00.asp>.
- Natasha Watkins, Twitter and FTC Settle Over Privacy Breaches. <http://redmondmag.com/articles/2010/06/28/twitter-and-ftc-settle-over-privacy-breach.aspx>June.
- Seeman Roderick H. PRIVACY PROTECTION—2003 Japan Law. [http://www.japanlaw.info/law2004/JAPAN\\_LAW\\_2004\\_PRIVACY\\_PROTECTION.html](http://www.japanlaw.info/law2004/JAPAN_LAW_2004_PRIVACY_PROTECTION.html). (Published by “Education and Education Management 2011”, June 1, 2011, pp. 6–10).
- Spanish agency sues Google over Street View[N]. [http://www.google.com/hostednews/afp/article/ALeqM5hJZnbsG01RaPfgcyWgV3Ff\\_mFgA?docId=CNG.f19d7e6bde86784c402b-796cf62d955d.381](http://www.google.com/hostednews/afp/article/ALeqM5hJZnbsG01RaPfgcyWgV3Ff_mFgA?docId=CNG.f19d7e6bde86784c402b-796cf62d955d.381). Accessed 18 Oct 2010.
- The U.S. iPhone and iPad users collectively prosecuted Apple’s revealing personal information (in Chinese) [N]. [http://www.legaldaily.com.cn/economical/content/2010-12/29/content\\_2421391.htm?node=21507,2010-12-29](http://www.legaldaily.com.cn/economical/content/2010-12/29/content_2421391.htm?node=21507,2010-12-29). See also Joel Rosenblatt. Apple Sued Over Applications Giving Information to Advertisers [N], <http://www.businessweek.com/news/2010-12-30/apple-sued-over-applications-giving-information-to-advertisers.html>.
- Zhang Xusheng. Qihoo Accused of Privacy Breach by Rival (in Chinese) [N]. <http://english.caing.com/2011-01-04/100213747.html>Jan.



**Part V**  
**M-Commerce Security**

# Chapter 12

## Security Problem and Solutions to M-commerce

Yimeei Guo and Ying Luo

**Abstract** Mobile e-commerce (hereinafter m-commerce) is a new shiny spot for enterprise's informatization. It will be broadly put into practice in the coming years. Currently, because consumers lack confidence on security problem of the mobile networks, it becomes the biggest challenge of the development of m-commerce. Therefore, this article wants to explore the security problem in mobile business in general and in particular. Then, it discusses some feasible solutions. Finally, this article brings out the conclusion.

**Keywords** M-commerce · Security · Solutions

### 12.1 Introduction

Mobile e-commerce (hereinafter m-commerce) is a new shiny spot for enterprise's informatization. It will be broadly put into practice in the coming years. Many commentators believe that m-commerce services will be the next biggest growth area in the telecommunications market, representing the fusion of two of the current consumer technologies: mobile communications and e-commerce. Whether the ambitious forecasts will be realized is immaterial; as an industry, telecommunications is being driven rapidly toward this goal.

For example, according to the data from Ministry of Industry and Information Technology of the People's Republic of China, till the end of June 2008, the number of China's mobile phone users reaches 601 million (China 2008). Also, in accordance with "the 22nd Statistical Report on the Internet Development in

---

Y. Guo (✉)

School of Law, Xiamen University, 361005 Xiamen, China

e-mail: yimei\_guo@necmail.xmu.edu.cn

Y. Luo

Management Science Department, Xiamen University, 361005 Xiamen, China

e-mail: yuhe\_ly@sina.com

China” by China Internet Network Information Center (CCNIC) released in July 2008, surfing the Internet with cell phone has become an important development orientation for network applications and will inevitably accelerate the popularization of the Internet. At present, 28.9 % of the Chinese netizens accessed the Internet with cell phone in the past half year, and the amount of cell phone netizens has reached 73.05 million (CNNIC 2008).

Mobile communications is now considered a relatively mature technology with the move from second to third generation systems and with its high consumer acceptance. However, older network technologies are still present in many parts of the world with the associated problems of cloning and eavesdropping, while services that are badly designed and implemented, together with new attack methods, combine to result in continued reports of loss, even where the security of the underlying technology is relatively sound.

E-commerce is a relatively new technology that is slowly gaining consumer acceptance, despite a background of fears surrounding security issues. An informal poll at a recent telecommunications conference revealed that around 30 % of delegates had made use of e-commerce services, but only around 10 % used them regularly, demonstrating that even those in the business made little use of them. Although the reasons for the lack of uptake are many and varied, at least part of the problem can be attributed to security fears, reinforced by the media attention surrounding every failure.

M-commerce is bringing together these two technologies with a history of security problems. Coupled with the convergence of voice and data communications, interconnection with external data networks and issues surrounding the transactions themselves, the potential risks are possibly very large indeed (Messham xxx).

Generally speaking, currently, because consumers lack confidence on the security problems of the mobile networks, it becomes the biggest challenge of the development of m-commerce. Therefore, this article wants to explore the security problem in mobile business in general and in particular and discusses some feasible solutions. Finally, this article brings out the conclusion.

## **12.2 Security Problem in Mobile Business**

### ***12.2.1 General Description***

Fundamental to the concept of e-commerce is a commercial transaction between two parties carried out by electronic means. The applications of this concept are almost limitless but may involve anything from a few cents to thousands of dollars in value. In the m-commerce domain, the boundaries will be similarly wide-ranging, although with a greater focus on location-based and information services, the distribution of transaction value may differ. Experience has shown that wherever something is of value, it will be targeted for attack; even small value transactions are worth attacking if there are enough of them. For instance, Taiwan

Criminal Investigation Police Office successfully detected the first case of illegally using other peoples' credit card by means of utilizing wireless excessive wave and found out the suspect—Shiyu Zhuang with the nickname of “originator of wireless excessive wave,” organized a crime gang with his girlfriend and other pals and utilized portable computer appliance to intercept other people's wireless excessive wave, illegally use their credit card and do money laundry (Tao 2006). A key element of ensuring security of m-commerce services must, therefore, be of securing the transaction itself.

Not all attacks will, however, focus on the transaction. Other attackers may target the underlying infrastructure supporting the service. For example, the world's first mobile phone virus “Cabir” has spread to the United States from its birthplace in the Philippines in July 2004. “Cabir,” found in about 15 variations so far, is draining mobile phone batteries, said Mikko Hypponen, director of Finnish anti-virus research company F-Secure (FSC1 V.HE: Quote, Profile, Research) on February 18, 2005. “Cabir” has been found in countries ranging from China to the United Kingdom. In November 2004, another virus program known as “Skulls” aimed at advanced mobile phones was sent to security firms, not to consumers, as a so-called proof of concept to alert them of the virus writer's capability (Swartz 2005).

Notably, according to an investigation conducted by McAfee Corporation in 2008 which picked up 2000 persons' samples from the United Kingdom, the United States, and Japan, only 21 % people stated that their cell phones were infected by virus, 11.6 % people told that they have heard some people nearby were invaded by virus, and 86.3 % people stated that they never heard whose cell phone was infected by virus. Nevertheless, 72 % people cared about their own cell phone' security very much. In Japan, with its vigorously developed cell phone industry, there are 89.1 % people who highly concern cell phone security problem. They stated that they have many experiences of virus invasion (Pang 2008).

Besides, it is reported in early 2008 that there was a multimedia messaging service (MMS) virus “Commwarrior,” which mainly infected the cell phone applied the SymbianS60 system. “Commwarrior” has made many cell phone batteries out of work and caused their users' communication fee increased suddenly (Cell Phone Infected by MMS Virus and Was Stolen RMB 100 a Day 2008).

The attacker's motivation may be for profit, for kudos or merely malicious, but all have the potential for significant damage. As infrastructure is opened up through interconnection, the risks multiply. In protecting the infrastructure, it is also important to consider customer data (including the confidentiality of information about customers) and ensure that appropriate measures are taken to ensure that it is adequately protected.

Clients, whether they are customers in the traditional sense or partners in hosted m-commerce environments, must also be taken into account. The opportunities for malicious code attacks, such as viruses, against client terminals and interconnected systems will become significant. Although the end user may assume ultimate responsibility, they will also look to network operators to provide some level of protection.

### ***12.2.2 The Different Levels of Involvement that the Network Operator May Take in an M-Commerce Transaction***

The exact nature of the security issues faced will depend on the operator's level of involvement in the transaction. Issues of responsibility and liability will be fundamental in establishing services and managing exposure to loss. The question of who is responsible for a particular aspect partly derives from the different levels of involvement that the network operator may take in an m-commerce transaction:

- At the simplest level, the network operator provides a means of transport and network interconnection for a transaction between two independent parties, the customer and an m-commerce service provider
- At a higher level of involvement, the network operator may provide a hosted m-commerce environment for service providers or may actually manage a branded service on the part of a retailer
- At the highest level, the operator may act as an intermediary in the transaction and take responsibility for mutual authentication of the parties and, potentially, for facilitating the settlement of financial exchange.

Clearly, as the level of involvement increases, so does the responsibility and potential liability for loss. The security concept built and applied around the service will depend on how the service is configured, but must also ensure that liability is established where an interface occurs with another party.

Bearing this in mind, the three basic security components are as follows:

- Transaction: protecting the transaction parties and their data by providing an acceptable level of security
- Information: protecting valuable and sensitive information about customers
- Infrastructure: protecting the network infrastructure from attack.

These are considered separately, but it is worth explaining at the outset that the exact nature of the service implemented will influence the involvement of the operator in the financial transaction. Various payment models have been proposed, ranging from credit card transactions between customer and vendor, through billing of services directly to the customer's telephone bill for collection by the network operator. These have different impacts on the liability of the operator.

As operators become involved in transactions, either by processing payments, by extending credit, or by acting as clearing houses, their roles will increasingly evolve toward acting as financial institutions and they will need to emulate many of the process and security controls of such institutions (Messham xxx).

## **12.3 Some Feasible Solutions**

### ***12.3.1 Managing the Security Risks***

Managing the security risks in m-commerce services will require a combination of controls, both technical and procedural. One of the biggest challenges facing operators will be ensuring the coordination of these controls in a strategic manner to ensure complete coverage. Understanding and applying the controls effectively will demand a combination of skills from different security backgrounds, ranging from technical solutions through secure process design to physical security. Ongoing operational management of the various processes and systems will also be fundamental to success.

### ***12.3.2 Monitoring and Detection***

Fraud monitoring and detection have become part of the established voice telephony infrastructure. Most operators have some form of monitoring, ranging from billing system-based reports through to dedicated fraud detection systems and monitoring teams. These systems are largely rule or threshold based and analyze switch-based signaling or call detail records. In an environment based on data where packets and messages have replaced voice calls, and networks may carry many types of communication, including financial transactions, where will the next generation of monitoring come from? There will be requirements on operators to monitor behavior, of their customers, of service usage and access, and of content itself. To do so, clearly requires a much broader understanding of the security risks and of the nature of the services being used by customers. Without this understanding, it will be impossible to distinguish between legitimate and non-legitimate or unwanted traffic. Again, this will require cooperation between operators, service, and content providers to define responsibilities and requirements and to ensure appropriate coverage and protection.

### ***12.3.3 Relationship Management***

Traditionally, network operators have had relatively few relationships with other organizations: network interconnection and roaming being the two main examples. However, even in these environments, problems have arisen with definition of responsibilities and consideration of fraud and security issues when making

agreements. In the new era of data services, operators will potentially be confronted by many more interfaces to many more organizations such as customers, service providers, and content providers. Potential security weaknesses arise from poor cooperation, a failure to communicate, or a lack of clearly defined responsibilities. All operators should consider these issues alongside legal and regulatory concerns in defining service interfaces and drawing up agreements (Messham xxx).

## 12.4 Conclusions

Undoubtedly, fraudsters and hackers will actively target all m-commerce services, service providers, and the underlying infrastructure. Among every operator's first customers will be individuals and organizations attempting to identify weaknesses that can be exploited. Although security standards have been defined surrounding the underlying technology of the mobile communications infrastructure, it is essential that these be implemented and their limitations were recognized. The supporting infrastructure must also be appropriately secured through a combination of technical controls and procedural and process security.

At the same time, it is also necessary to consider the new risks surrounding convergent and value-added services. Operators must think laterally to adapt existing countermeasures, adding new ones where emerging risks are not adequately covered. Above all, in a constantly changing and still evolving product environment, they must continue to be one step ahead and proactively manage security issues before they arise.

Finally, although the "Electronic Signature Law of the People's Republic of China" was enforced on April 1, 2005, which validates the legal effect of electronic signature, there are no laws and regulations directly addressing the aspect of m-commerce, and the traditional ones cannot applied for m-commerce, such as the physical authentication of m-commerce devices, billing, and invoicing. (Messham xxx). Therefore, it is hoped that China enact and revise relevant laws and regulations so as to keep m-commerce's prosperous and orderly development.

## References

- China has 601 million mobile phone users and China Mobile's users reaches 414.6 million (Chinese version). <http://cn.ibtimes.com/articles/20080725/shoujiyonghu.htm>. Accessed 25 July 2008.
- Cell Phone Infected by MMS Virus and Was Stolen RMB 100 a Day. [http://news.dayoo.com/tech/news/2008-01/30/content\\_3282456.htm](http://news.dayoo.com/tech/news/2008-01/30/content_3282456.htm). Accessed 30 Jan 2008.
- CNNIC. The 22nd Statistical Report on the Internet Development in China. <http://www.cnnic.cn/uploadfiles/doc/2008/7/23/170424.doc>. Accessed 23 July 2008.
- Lv Xin. 2005. Security and privacy problems of M-commerce (Chinese version), Computer Security, Volume 9. (Published by Proceedings of 2008 International Conference of Production and Operation Management, 2008.12.8-10. < ISTP indexed >).

- Messham James. M-commerceSecurity,[http://www.tdap.co.uk/uk/archive/billing/bill\(fml\\_0012\).html](http://www.tdap.co.uk/uk/archive/billing/bill(fml_0012).html).
- Pang Ligeng. Cell phone is hot online with virus becoming a big problem. <http://220.160.107.163/cgi-bin/login?token=ATD1CVMRSpB7TW3tAoQ3BA%3d%3d>. Accessed 14 Feb 2008.
- Swartz Spencer. Mobile phone virus found in United States. <http://www.reuters.com/newsArticle.jhtml;jsessionid=VN05MLNXO3Y5OCRBAELCFFA?type=topNews&storyID=7678694&pageNumber=1>. Accessed 18 Feb 2005.
- Tao Huanchang. Risk of Illegally Using Credit Card Exits in Wireless Online (Chinese version), United Evening News, available at <http://times.hinet.net/news/20060214/headline/7e4b335b25be.htm>. Accessed 14 Feb 2006.



**Part VI**  
**Online IPR Protection**

# Chapter 13

## IPR Management Strategies for Enterprises in the e-Commerce Era

Yimeei Guo, Dongsheng Yan and Weiwan Zhang

**Abstract** The new era of e-commerce has changed the way we conduct business affairs. First, the rapid development of innovative technologies has promoted the global economy to an era dominated by knowledge and information. Secondly, fast exchanges in investment and technical transfer have created a boundary-free global economy. Lastly, the rapid development of the Internet and e-commerce has radically changed the pattern of traditional economic activities. Meanwhile, in the rapid changing and highly competitive global market, IPR management has already become the most important topic while facing the challenges from competitors. How enterprise could practice the best knowledge strategy and integrate IT platform to facilitate the ability of managing intellectual assets are the critical issues nowadays. Therefore, this article introduces the overall IPR protection and development of e-commerce in China separately at first. Then, it discusses the importance of IPR management and some IPR management strategies for enterprises in the e-commerce era. Finally, this article brings forth the conclusion with the hope to promote innovation development in China in the e-commerce era.

**Keywords** E-Commerce · IPR management · Strategies innovation

---

(Published by “Proceedings of the IASTED International Conference on Modeling, Simulation, and Identification (MSI 2009)”, 2009-10-1. <EI indexed>)

---

Y. Guo (✉) · D. Yan · W. Zhang  
Center for Economic Law, Law Department, Xiamen University, Xiamen 361005, China  
e-mail: yimei\_guo@necmail.xmu.edu.cn

D. Yan  
e-mail: ydsxmu69@126.com

W. Zhang  
e-mail: luckyall970@hotmail.com

## 13.1 Introduction

The new era of e-commerce (EC) has changed the way we conduct business affairs. First, the rapid development of innovative technologies has promoted the global economy to an era dominated by knowledge and information. Secondly, fast exchanges in investment and technical transfer have created a boundary-free global economy. Lastly, the rapid development of the Internet and e-commerce has radically changed the pattern of traditional economic activities.

Meanwhile, in the rapid changing and highly competitive global market including e-commerce market, intellectual property right (hereinafter IPR) management has already become the most important topic while facing the challenges from competitors. How enterprise could practice the best knowledge strategy and integrate IT platform to facilitate the ability of managing intellectual assets are the critical issues nowadays. Therefore, this article introduces IPR protection and the development of e-commerce in China at first, and then, it discusses the importance of IPR management and some IPR management strategies for enterprises. Finally, this article brings forth the conclusion with the hope to promote innovation in China in the e-commerce era.

## 13.2 IPR's Protection in China

Since the 1980s, China has developed a body of laws and regulations on IPR protection, namely the *Copyright Law*, *Patent Law*, *Trademark Law*, and *Regulations on the Protection of Layout-Designs of Integrated Circuits* and administrative regulations for the implementation of these laws. Upon accession to WTO, China became a signatory to the *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs)* and amended the related IPR laws to provide a stronger and wider scope of protection for IPR holders.

However, given the country's vast geography and population and its rapid economic growth, implementation and enforcement of IPR laws remains weak. In recognition of this, the central government has stepped up to its efforts in IPR protection. As early as in 2003, the Chinese government instituted the Mechanism of Regular Communication and Coordination with Foreign-Invested Enterprises to further improve the enforcement of IPR protection and the foreign investment environment. In August 2004, a high-power National Working Group of Intellectual Property Protection was established under the aegis of the States Council. Recently, after more than three years of preparation work, the revised PRC Patent Law ("New Patent Law") was finally promulgated on December 27, 2008, and will enter into force on October 1, 2009.

With concerted efforts from all parties concerned, improvements in IPR protection can be achieved, but this will be a gradual process. Foreign investors are well advised to develop a more proactive approach in IPR and brand protection in

China, such as forming allies with all stakeholders, including domestic enterprises (Coppers 2005).

## 13.3 The Development of EC in China

### 13.3.1 Overall Situation

Since the first e-mail is delivered over the Great Wall by Internet on September 20, 1987, the history of development of the e-commerce has had over 20 years. China's fast-growing population of Internet users has risen to 298 million after passing the United States in 2008 to become the world's largest, a government-sanctioned research group said (China Daily 2009). Besides, the market research company IDC has published a white paper about China's e-commerce industry, and it states the total trade scale of China's e-commerce industry reached RMB 1.951 trillion yuan in 2008, increasing over 20 % compared with the RMB 1.608 trillion yuan in 2007, forming a big contrast with the macroeconomic downturn. Of this revenue, e-commerce that targeted individual consumers increased by about 30 %. The report further points out that China's e-commerce industry will maintain a rapid growth in the next five years and by 2010, its total trade is expected to reach RMB 3.22 trillion yuan (IDC 2009).

### 13.3.2 Current Legal System Concerning EC in China

On June 25, 2007, the National Development and Reform Commission (NDRC) with The State Council Informatization Office of PRC (now incorporated in MIIT) jointly published *The Eleventh Five-Year Plan on E-commerce Development*. Thereafter, many local governments began to set up new service mechanism to improve the development of e-commerce. As early as on May 8, 2001, the Former President Jiang Zemin pointed out in the opening speech of the Fortune Global Forum 2001 in Hong Kong that "China will work hard on e-commerce, accelerate the process of informatization, and support enterprises in applying modern information network technology and international co-operation and exchanges." Chinese government has always paid much attention to the development of e-commerce.

In order to achieve the goal of the "Eleventh Five-Year Program," in the following years, Chinese Government had further promoted the development of e-commerce and created a good development environment in the field of technology, network, commerce, and legal rule. These policies, laws, and regulations concerning taxation, tariff, e-payment, electronic signature, identification authentication, network intellectual property rights, etc., will be stipulated, which are suitable to the development of e-commerce.

Inter alia, as the only law related to e-commerce in China currently, the *Electronic Signature Law* effective on April 1, 2005, was to boost electronic business, which for the first time legalizes increasing electronic deals. Also, the issuance of “*Electronic Payment Guideline*” by People’s Bank of China on October 26, 2005, provides policy authority for e-commerce macroenvironment’s perfection and advancement.

### 13.3.3 IPR Laws and Regulations Related to EC in China

In China, the dispute between the holder of domain name and the owner of trademark is the major issue. Other trademark protection issues in cyberspace are seldom reported in China. Recently, the People’s Court in Beijing and Shanghai has issued a number of decisions in high-profile domain name dispute cases involving foreign companies such as Ikea, P&G, and Dupont. In all three cases, i.e., *Ikea v. Guowang*, *P&G v. Guowang*, and *P&G v. Shanghai Chenxuan*, the owner of the trademark won; however, the basis for the decision seems straightforward, logical, and reasonable, but it relies more on the spirit of the underlying Chinese law, i.e., the principle of “fairness, honesty and credibility” provided by Clause 1, Article 2 of the Law against Unfair Competition rather than its terms.

In all, China’s current trademark legislation and competition legislation also prohibits “passing off” and has regulations on well-known trademarks, like *Lanham Act* in the USA, but the legislation was drafted without consideration of domain names. Thus, it is difficult to find a specific provision in this legislation that would prohibit use of a domain name. In order to provide more effective trademark protection on the Internet, the new amendment should address these issues seriously.

While cases involving conflicts between domain names and trademarks are still in their infancy in China as elsewhere, China’s administrative bodies have not been slow to grapple with the difficult legal issues. On February 14, 2006, the China Internet Network Information Center (CNNIC) promulgated a new version of the *CNNIC Domain Name Dispute Resolution Policy (CNDRP)*, which governs disputes relating to “.cn” domain names and all Chinese domain names (CNNIC domain names). The new *CNDRP* came into force on March 17, 2006. The *CNDRP* provides a set of efficient and cost-effective procedures for resolving ownership disputes involving CNNIC domain names.

According to Article 8, to succeed, the complainant in a *CNDRP* proceeding must satisfy three conditions: (a) The disputed domain name is identical or confusingly similar to the complainant’s name or mark, (b) the disputed domain name holder has no legitimate interest in the domain name, and (c) the respondent has registered or has been using the domain name in bad faith. While these basic tenets remain the same under the 2006 Policy, certain new rules highlighted below will make the recovery of CNNIC domain names more difficult.

The 2006 Policy contains three key changes. First, if a domain name has been registered for more than two years, a CNNIC dispute resolution service provider will not accept a *CNDRP* complaint to protect the stability of domain name registrant's right and legitimate interest. Second, mere registration for the purpose of selling, renting, or otherwise transferring a CNNIC domain name by itself is no longer sufficient proof of bad faith. Such acts must be done with a view to obtain unjustified benefits from the complainant or its competitors to constitute bad faith. Third, a respondent is presumed to enjoy rights and legitimate interest in the disputed domain name if, prior to receiving a complaint, it has made *bona fide*, legitimate or fair use of the same, or it has come to be known by the disputed domain name even if it has acquired no corresponding trademark right.

Besides, three cases separate from the Courts of China in Beijing, Guangzhou, and Shanghai in 2008 have again raised questions relating to keyword advertising programmers. The issue at stake is whether the purchase or sale of keywords that constitute the whole or part of another party's registered trademark can be classified as trademark infringement under Chinese law.

Among them, the Shanghai district court at the outset examined the fact pattern regarding "keyword advertising" or "sponsored links" involved in Jijia case, and eventually held in the plaintiff's favor and awarded damages of Rmb100,000 to Jijia. In the other case from Guangzhou Baiyun District, the court found Google innocent of trademark infringement in the context of a keyword service.

Ironically, in an even earlier case, another large search company, Baidu, had confronted the completely opposing stand of Shanghai No. 2 Intermediate Court. The Shanghai Court concluded that in the case where a third party used another's trademarked words without authorization, Baidu did not duly perform its duty of care and hence should be imposed with a civil liability. In addition to the injunction order, the Court awarded damages of Rmb50,000 against Baidu for its joint infringement.

The examination of the three cases above reveals that the Chinese courts have not yet reached consensus on issues including the duty of care of a search engine which provides a keyword service, and the application of joint infringement theory to relevant cases. In the absence of guidance from a higher level, some lessons can be learned on the basis of court practices observed until now in China (Hong 2009).

Article 10 of the *Copyright Law* amended in 2001 specifies the sixteen rights of a copyright owner. Inter alia, added as a new kind of property to the copyright owners in accordance with *WIPO Copyright Treaty (WCT)* and *WIPO Performances and Phonograms Treaty (WPPT)*, the right of communication through information networks is the right to communicate to the public a work, by wire or wireless means in such a way that members of the public may access these works from a place and at a time individually chosen by them [See Art.10 (xii)].

On May 18, 2006, China State Council issued the *Ordinance on the Protection of the Right to Network Dissemination of Information (the Ordinance)* and took effect on July 1, 2006. The *Ordinance* sets forth regulatory guidelines for the protection of the "right of communication over information networks" in respect of

text, images, performances, sound recordings, video recordings, and other works in which copyright subsists (collectively, works). One significant aspect of *the Ordinance* is that it addresses the legal uncertainty highlighted in a 2005 lawsuit involving illegal MP3 downloads (i.e., *Shanghai Busheng Music Culture Media v. Baidu* case. On September 16, 2005, the People's Court of Haidian District in Beijing ordered Baidu to pay ¥68,000 to Shanghai Busheng for unauthorized downloads of 46 songs), namely the legal liability of Internet service providers (ISPs) that provide search engine or linking services which indirectly allow Internet users to access copyright-infringing works. Thus, *the Ordinance* stipulates, for the first time in China, some of the specific liabilities that ISPs could face for providing online search and Web-linking services and sets forth guidelines for ISPs to follow in order to avoid such liability.

According to *Art.15 of the Ordinance*, ISPs will not be liable for infringing the right of communication if the providers ensure the prompt removal of infringing content and any links thereto upon receipt of an infringement notice with supporting evidence from a copyright holder. If the individual or entity that was providing that work issues a "non-infringement statement" with supporting evidence, then the ISP must promptly repost the relevant content or link upon receipt (*See Art.17*).

Therefore, Baidu met the chance to turn its fate around in another case. On November 7, 2006, in *IFPI v. Baidu case*, Beijing's First Intermediate Court ruled that Baidu's service, which provides Web links to the music, does not constitute an infringement as all the music is downloaded from Web servers of third parties.

## 13.4 IPR Management Strategies for Enterprises in the e-Commerce Era

### 13.4.1 *The Importance of IPR Management*

IT Researcher Kevin Zhu at University of California-Irvine Graduate School of Management once pointed out that companies that want to take advantage of the opportunities posed by e-commerce will have to do a better job managing dynamic pricing strategies, intellectual property rights, and partnership relationships. By developing their management techniques in those areas, traditional manufacturing firms will improve their standing with high-tech firms. Inter alia, UC Irvine found the management of intellectual property rights is critical to e-business success. Examples of intellectual property accomplishments by e-commerce firms include the patents obtained on [www.Priceline.com](http://www.Priceline.com)'s reverse auction and [www.Amazon.com](http://www.Amazon.com)'s 1-Click shopping system. Using an e-business patent has become the weapon of choice for Internet giants, with a series of patent cases between powerhouses determining who can—and who cannot—use certain e-commerce shopping technologies (Vigoroso 2001).

### ***13.4.2 IPR Management Strategies***

According to the discussion above, this article suggests that some strategies be adopted by the companies for meeting various techno-legal requirements pertaining to IPR protection in cyberspace.

#### **13.4.2.1 Enterprises Should Attach Much Importance to Technology Advancement and IPR Protection**

Some unimaginable technologies before Internet rose to power have emerged nowadays just as the spring bamboos after raining and overthrown the rule of game of traditional industries. For example, MP3 music format broadcasting and P2P/BT file sharing and swapping software made the music and movie industries confronting tremendous challenges. Even though most of the litigations brought by US big record labels or movie companies against ISPs or software companies worldwide had prevailed, yet the whole music and movie industry went down gradually to the bottom ever since 2000 and the revival of prosperity seems fairly remote. This is simply owing to companies' IPR protective means inadequate with technology improvement.

Whereas, in another aspect, the upheaval of business method patent, ever since Signature Financial Group, Inc., obtained the patent of the business model of financial management and accounting calculation of mutual fund, [www.Amazon.com](http://www.Amazon.com), [www.Priceline.com](http://www.Priceline.com), and [www.Doubleclick.com](http://www.Doubleclick.com) have utilized business method patent separately to accuse their competitors intending to block them outside the wall, hence has arisen another wave of IPR possibly caused by IPR over protection to some degree.

Nevertheless, based on the captioned explanation, we can realize the gigantic impact of technology advancement toward IPR management in the e-commerce era. This is also one of the most important challenges to IPR management personnel.

#### **13.4.2.2 Enterprises Should Transform Employees' Knowledge and Experience to Corporate Assets**

"Employee is an enterprise's biggest asset!" This proverb reveals much more meaning in the knowledge economic age. While employee holds the strongest production tool—knowledge, which is the enterprises' biggest asset—but from the lawyer's point of view, such asset should be more or less depreciated. Once the employee leaves his job, such knowledge will also be moved away. Therefore, the above-mentioned proverb cannot be spoken out freely from anxiety while lacking sound legally protected employment relationship, because if there is no clear right



of asset, how can an enterprise have any claim on such asset? This also belonged to part of IPR management.

Besides, after the right of asset is made clear, we shall see how to utilize the asset effectively. Right now, the very prevailing “knowledge management (KM),” viewed from the lawyer, is to transform employees’ knowledge to corporate intangible assets, less an enterprise loses its valuable resources owing to employees’ departure or something happened.

#### **13.4.2.3 Enterprises Should Take Care of Both Information Transmission and Protection of Themselves**

In the e-commerce era, no matter employees or consumers have the opportunity to take charge of more information than ever, and enterprises also would like to utilize such way of information transmission to stimulate employees to innovate and bestow employees power of decision making by various layer, and increase consumers’ confidence toward the whole enterprise. However, as enterprises look up information transmission, they should not forget that giving information to the suitable person at appropriate time is the correct method of use.

It is believed that how an enterprise controls the circumstances related to information transmission and utilization is a big challenge to information technology (IT) and legal personnel. For instance, the attached file brought by e-mail may be one of the quickest channels to cause IPR loss, whereas whether monitoring employees’ e-mail should be allowed or not has been a controversial issue so far. Also, taking trade secret protection as an example, via e-mail the R&D documents, efforts, direction, discussion paper, etc., can be sent to the competitor’s enterprise and through enterprise’s customer service center direct line, some secret related to enterprise’s development can be overheard, not to mention revealing enterprise’s operational secret by MSN or QQ.

In fact, such incidents rely one enterprise’s drawing up precise rules of Internet usage and IPR protective guideline to meet the trend of information fast transmission and information control ability enhancement.

#### **13.4.2.4 Enterprises Should Adapt Themselves into Technology and Legal Environment Changes**

How an enterprise adapts themselves into technology and legal environment change is no longer solved by setting a unit or a managerial system, but is a prompt response toward the captioned change by the enterprise’s decision-making status. Presently, every country in the world is in an effort to add or modify IPR and trade laws and regulations. In the near future, relevant rules will be necessarily reshuffled within a great range adding the borderless character of e-commerce; enterprises cannot isolate themselves from foreign IPR’s development.

It is possible that a newly risen service filled with lots of commercial opportunities today becomes illegal activity because of change of rules. It is also probable that a highly profitable industry becomes nonprofitable at all under competition owing to deregulation. Those are something that enterprises have to pay attention particularly to engage in IPR management.

Besides, every country's including China's court in practice continually makes judgments against Internet or e-commerce disputes including copyright infringement by [www.MP3.com](http://www.MP3.com), Napster and Grokster, trademark infringement by domain name cybersquatting, deeplink and metatags, and copyright infringement and trespassing by data mining, etc. Taking *StreamCast* case as an example, a US judge has said that the Morpheus software produced by StreamCast breaks the law in September 2006. The ruling is another victory for the entertainment industry, which has had a string of recent victories and concessions. Just weeks ago before *StreamCast* judgment, Sharman Network—owner and provider of Kazaa software—settled with Universal, Sony BMG, UMI, and Warner, four international big labels for \$100 million (File-sharing software firm loses US case 2006).

In addition to P2P software companies, music- and movie-publishing companies, *StreamCast* case is looked attentively in particular by companies developing P2P transmission technology. This is because when e-commerce-related regulation is unclear or its development step lags behind, the court's judgment will be the best reference to define various legal issues. To meet changes of legal environment (from ambiguous to clear and definite is also a kind of change) and proceed enterprises' operational and managerial as regarding IPR management is also a very important issue.

For example, viewing the increasing maturity of P2P technology, Google bought YouTube at an amazing price on the latter half of 2006. Contemporarily, YeMusic.com—a subordinate of Yahoo!—and online music P2P leading Web site Kuro in Taiwan reached settlement. Kuro officially transformed to become legal online music provider. Besides, Oracle criticized computer software patent award unjust in the one hand, but when such patent system has become operational in reality, Oracle also began to apply software patent immediately in order not to fall behind. Those facts told us there are few absolutely unchangeable strategies in the e-commerce era. Companies which can meet technology and legal environment's fast change will be the last survivor.

## 13.5 Conclusion

Over the past 20 or more years, China has created IP laws that generally adhere to international standards. As Premier Wen Jiabao points out, "IPR protection is not only for the need of establishing international credibility and broadening international cooperation, but more importantly, for the need of stimulating innovation within China. The protection of IPR is, in essence, the respect for labor, for

knowledge, for talents and for creation (Yi 2007).” Thus, as to Chinese enterprises, it is indispensable for them to have IPR management strategies to enhance their competitive leverage so as to catch up all potential opportunities in the e-commerce era.

## References

- Coppers, Price Water House. 2005/2006. *From Beijing to Budapest—winning brands, winning formats*. London: PricewaterhouseCoppers, 4th edn, 35–49. Available at [http://www.pwc.com/extweb/pwcpublishations.nsf/docid/814235FAABCCFD678525708B00597DF7/\\$File/China.pdf](http://www.pwc.com/extweb/pwcpublishations.nsf/docid/814235FAABCCFD678525708B00597DF7/$File/China.pdf).
- China Daily. 2009. *China internet users soar to 298 million*. Beijing: China Daily, 14 Jan 2009. Available at [http://www.chinadaily.com.cn/china/2009-01/14/content\\_7396500.htm](http://www.chinadaily.com.cn/china/2009-01/14/content_7396500.htm).
- IDC. 2009. *China's e-commerce scale increased 20 %*. In 2008, China Tech News, 2009. Available at <http://www.chinatechnews.com/2009/01/07/8432-chinas-e-commerce-scale-increased-20-in-2008/>.
- Hong, Luckie. 2009. *Internet search engines and trademark rights*. 3 Apr 2009. Available at <http://www.blawdog.com/article/Publication/831.htm>.
- Vigoro, W., Mark. 2001. *Study: winning at e-commerce requires evolved management style*. E-Commerce Times, 20 July 2001. Available at <http://www.ecommercetimes.com/story/12150.html>.
- File-sharing software firm loses US case, 29 Sept 2006. Available at <http://www.out-law.com/page-7343>.
- Yi, Wu. Address of Vice Premier Wu Yi at the Conference of Enterprise IPR Protection and Self-initiated Innovation. Available at <http://english.mofcom.gov.cn/column/print.shtml?/translators/garden/famouspeech/200706/20070604809574>.

# Chapter 14

## How Would the Domain Name Dispute—Ikea “Cybersquatting” Case Be Decided Under American Law?

Yimeei Guo

### 14.1 Introduction

Domain name can be considered the addresses of the Internet, e-mail is sent, and Web pages are found through the use of domain names. As an example, the Web address for the Perkinscoie Web sites is [www.perkinscoie.com](http://www.perkinscoie.com) while e-mail to Sui-Yu Wu (Attorney at Law in Taipei Branch) is sent to [wusuy@perkinscoie.com](mailto:wusuy@perkinscoie.com) (both using the “perkinscoie.com” domain name). Domain names are more than just address, however, since they can be selected by the “addressee” and are usually closely associated with a particular service or product.

Because of the increasing popularity of the internet, companies have realized that having a domain name that is the same as the company or product name can be important part of establishing an Internet presence. To obtain a domain name, an application must be filed with an appropriate register. However, when companies attempt to obtain their desired domain name, they may discover that their desired domain name is already taken. When this happens, the company can either choose a different name (e.g., china\_airline instead of china airline) or fight to get the domain name it really wanted (e.g., McDonald, MTV). These fights are called domain name disputes.<sup>1</sup>

---

(Published by “(Taiwan) Proceedings of 2000 National Science and Technology Law Conference”, November 23, 2000, pp. 779–790)

---

<sup>1</sup> Some well publicized examples of domain names disputes can be found in <http://www.bitlaw.com/internet/domain.html>).

---

Y. Guo (✉)  
S.J.D., Tulane University, New Orleans, USA  
e-mail: [yimei\\_guo@necmail.xmu.edu.cn](mailto:yimei_guo@necmail.xmu.edu.cn)

Y. Guo  
Net and Law Institute, Peking Law School, Beijing, China

When a dispute over a domain name occurs, the parties can always turn to the courts. For example, in the states, companies that do bring a court action must present legal arguments on why a domain name registered to someone else should be canceled or transferred to an organization who was not fast enough to register the name first. Historically, those arguments were based on trademark law or dilution law (the latter will be discussed in II of this article). It was sometimes difficult to present a strong case under the traditional principals of trademark law, especially when the party seeking to obtain a domain name either could not prove a likelihood of confusing (which is required under trademark law)<sup>2</sup> or was a famous individual who never technically established trademark rights in their name.

In response to intense lobbying from trademark owners and famous individuals, Congress passed the Anticybersquatting Consumer Protection Act<sup>3</sup> in November, 1999. This act made it easier for individuals and companies to take over domain names that are confusingly similar to their names or valid trademark. To do so, however, they must establish that the domain name holder acted in bad faith (Detail discussion on ACPA and the relevant cases will also be in Part II of this article).

“Cybersquatting”—the practice of registered a domain name that matches another company’s trademark—may have begun in the USA as mentioned afore, but it is now a world wide issue. In China, it is not so difficult to register a domain name (the presiding organization is CNNIC. It also open the experimental system of Chinese domain name on January 18, 2000), but it is more difficult to pursue cybersquatters because of the lack of laws that address this problem than to do so in the states.

For example, in the PDA domain name preemptive registration case,<sup>4</sup> one of the grounds of the court to reject the plaintiff’s accusation is as follows. Registration of domain name is not the right enjoyed by the right holder of the mark, and meanwhile, registration as a domain name of other’s trademark is not one of the trademark infringing acts under Art.38 of the Trademark Law and Rule 41 of its Implementing Regulations.<sup>5</sup> This article will explain the legal status of cybersquatting in China by analyzing the recent decision of *Inter-Ikea Systems B.V. v. Beijing CINET Inf. Co. Ltd.*<sup>6</sup>

---

<sup>2</sup> Section 32 of the Lanham Act provides remedies for the infringement of federally registered trademarks. Section 43(a) provided remedies for false designation and descriptions (that is, unfair competition).

<sup>3</sup> 15 U.S.C. §1125(d). For the full text, see <http://www.cs.utah.edu/classes/cs5965/cybersquatting.html>. See also <http://www.mama-tech.com/antipiracy.html>.

<sup>4</sup> *Fulande Development Corp. from Shijiazhuang City v. Beijing Mitian Jidye Technology and Trade Co., Ltd.*, Civil Judgment of Beijing 1st Intermediate People’s Court (1999) Yi Zhong Zhi Chu No. 48.

<sup>5</sup> For a thorough discussion of the PDA case, see Ma, Laiker, *The Analysis of Handling Principals on Domain Name Preemptive Registration Cases from the PDA Case* (<http://www.chinaiplaw.com/fgrt/fgrt19.htm>).

<sup>6</sup> See Civil Judgment of Beijing 2nd Intermediate People’s Court (2000) Er Zhong Zhi Chu No.86. Note: But it was revoked by Beijing High People’s Court in November 2001. See Civil Judgment of Beijing High People’s Court (2000) Gao Zhi Zhong Zi No.76.

Finally, this article tends to make some suggestions for Chinese better solution to the “cybersquatting” problems as the conclusion.

## 14.2 How to Fight Against “Cybersquatting” Under American Law

### 14.2.1 *The Federal Trademark Dilution Act*

In addition to claims of trademark infringement, domain name disputes often include an allegation that use of the domain name dilutes a famous mark owned by the plaintiff. The legal authority can be found in the Federal Trademark Dilution Act of 1995 (15 U.S.C. §1125(c))(hereinafter the anti-dilution statute), added dilution as a cause of action available to trademark owners. The Act provides:

“The owner of a famous mark shall be entitled...to an injunction against another person’s commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark.....”

Senator Leahy, who supported the anti-dilution statute, said: “that this anti-dilution statute can help stem the use of deceptive Internet address taken by those who are choosing marks that are associated with the products and reputations of others.”<sup>7</sup> Therefore, the courts had already applied such statute to the domain name disputes, according to the above-mentioned words.

Under the anti-dilution clause, the plaintiff would have to show the mark was “famous” and that the use of the domain name actually dilutes this famous mark. Since the anti-dilution clause does not require showing a likelihood of confusion, plaintiffs may find this prescription a helpful aid in obtaining domain names “stolen by others.” On the other hand, the requirement that the mark be famous should limit these types of domain name disputes to those circumstances involving marks which are immediately associated to a single source.<sup>8</sup>

The notable application of the anti-dilution statute in practice was in the case of Panavision Int’l LP. v. Toeppen.<sup>9</sup> Panavision involved the best known cybersquatting defendant, Dennis Toeppen who reserved hundreds of domain names corresponding to well-known trademarks, such as Delta Airline, Neiman Marcus, Eddie Bauer, Lufthansa, Intermatic, and Panavision. Both the district court and the Ninth Circuit held that because Toeppen had attempted to extort \$13,000.00 from Panavision, this was sufficient use “in commerce” to bring the Federal Dilution

---

<sup>7</sup> See cong. Rec. S19312.

<sup>8</sup> E.g. in *Hasbro, Inc. v. Clue Computing, Inc.*, 66 F. Supp. 2d 117 (C.D. Mass. 1999), court held that mere registration of clue.com domain name did not automatically dilute “clue” mark, and that those was insufficient evidence that mark met standard for protection as famous or that defendant’s use would cause dilution.

<sup>9</sup> 945 F. Supp. 1296, 1303, 40 USPQ 2d 1908 (C.D. Cal. 1996), affirmed, 141 F. 3d 1316, 46 USPQ 2d 1511 (9th Cir. 1998).

Act into play. This was consistent with the ruling in *Intermatic, Inc. v. Toeppen*, 947 F. Supp. 1227 (N.D. Ill. 1996), which found that Toeppen's intention to arbitrage the "intermatic.com" domain name constituted a commercial use.<sup>10</sup>

### ***14.2.2 Anti-Cybersquatting Consumer Protection Act***

On November 29, President Clinton signed into law the Anti-cybersquatting Consumer Protection Act which amends the Lanham Act to provide a cause of action against cybersquatters. The act provides a cause of action where, without regard to the goods or services, a person: (i) Has a bad faith intent to profit from a protected mark, and (ii) registers, traffics in, or uses a domain name that (I) is identical or confusingly similar to a distinctive mark; (II) is identical or confusingly similar or dilutive of a famous mark; or (III) is a trademark protected by reason of section 706 of Title 18, U.S.C., or Section 220506 of Title 36, U.S.C..

In determining whether a person has a bad faith intent, the legislation lists nine factors which a court may consider (but is not limited to). These factors include (I) the trademark rights of the person in the domain name, (II) the extent to which the domain name consists of a legal name of the person, (III) the person's prior use of the domain name in connection with goods or services, (IV) the person's noncommercial or fair use of the mark in a site accessible under the domain name, (V) the person's offer to sell the domain name for financial gain without having used the domain name or (VI) the person's prior conduct indicating a pattern of such conduct, (VII) the person's providing false contact information when applying for the domain name, (VIII) the person's acquisition of multiple domain names which are identical or confusingly similar to the marks of others, and (IX) the extent to which the domain name is distinctive or famous.

Courts are given the remedy of being able to order forfeiture or cancellation of a domain name to the owner of the mark, as well as statutory damages of between \$1,000 and \$100,000 for each domain name, as the court considers just. The owner of a mark is given the option of filing an in rem civil action against the domain name itself, such as Porsche tried in *Porsche v. Porsche.com*, 51 USPQ2d 1461 (E.D. Va. 1999). This can prove very helpful to famous mark owners, especially where the cybersquatters are located overseas.

The act also provides for a cause of action when a person registers a domain name that consists of a name of another living person with intent to profit by selling the domain name to that person or a third party.

So far, there has been numerous domain name disputes involving "cybersquatting" brought to the courts. In *United Greek, Inc. v. Klein d/b/a Greek 101*, 00-cv-0002 (N.D. N.Y., May 2, 2000), the court entered a default judgment awarding statutory damages and attorneys fees against a defendant who failed to respond to a complaint under the ACPA. The plaintiff sought the transfer of the domain names

---

<sup>10</sup> Id. at 1239. *Contra*, *Academy of Motion Picture Arts & Sciences v. Network Solutions Inc.*, 45 USPQ 2d 1463, 1466 (C.D. Cal. 1997), and *Lockheed Martin Corp. v. Network Solutions, Inc.*, 985 F. Supp. 949 (C.D. Cal. 1997), affirmed, 52 USPQ 2d 1481 (9th Cir. 1999).

somethinggreek.com, united greeks.com, and united greek.com in addition to statutory damages of \$10,000. The court awarded plaintiffs \$15,950, including attorney's fees. In *Morrison and Foerster LLP v. Wick*, 94 F. Supp. 2d 457 (D. Colo. 2000), the law firm of Morrison and Foerster alleged that the defendant's registration of [www.morrisonfoerster.com](http://www.morrisonfoerster.com) and similar domain names violate the APCA. The court ruled in favor of Morrison and Foerster holding that the name creates initial interest confusion and that the defendant acted in bad faith. The defendant used the site to ridicule lawyers in general and MOFO in particular in what the court found was an attempt to "get even" with the firm (that the defendant alleged reneged on a contract).

In addition, in *Cello Holdings, L.L.C. v. Lawrence-Dahl Co.*, 89 F. Supp. 2d 464 (S.D. N.Y., 2000), Cello Holdings alleges trademark dilution and infringement based on the defendant's registration of the domain name "cello.com." A federal district court judge for the Southern District of New York denied summary judgment to both Cello Holdings and Lawrence-Dahl. The court suggested that Cello must show a specific intent to extort or blackmail in order to meet ACPA's bad faith requirement. Although the defendant registered, advertised, and attempted to sell numerous domain names, he registered "cello.com" during an attempt to register twenty other common names of musical instruments.<sup>11</sup>

## 14.3 A Comment on the Ikea "Cybersquatting" Case

### 14.3.1 Domain Name Dispute in China

It was until 1996 did China enter into the Internet officially. As reported by the news, when a number of well-known enterprises of inland China were trying to enter the Internet, they found that their corporate names had already been preemptively registered as domain names by others. There are as many as 400 enterprises in this predicament. Also preemptively registered are names of some well-known inland cities. What's more, this kind of activity is still going on unchecked.<sup>12</sup> Besides, many famous foreign enterprises have encountered the same fate in recent years, but they chose to seek legal remedy from the court to combat Chinese cybersquatters. It is learned that the Ikea case as mentioned before is the first proceedings of the kind instituted by a foreign enterprise in China.<sup>13</sup>

---

<sup>11</sup> For many other APCA cases, (see <http://www.perkinsoie.com/Internet> case Digest).

<sup>12</sup> See Zhu Qichao & Zhu Bin, *Domain Name and Trademark* (China Patents & Trademark No.1, 1998) p.59.

<sup>13</sup> Currently, there are other three domain name preemptive registration cases pending in the courts which all are against the same defendant. One is *U.S. Dupont Corp. v. CINET* (alleging trademark infringement and unfair competition), the second is *U.S. P&G Co. v. CINET* (requesting the court to order the defendant to desist from its infringing act and to revoke its registered domain name). The third one is *U.S. Dow's Chemicals Inc. v. CINET* (maintaining that the defendant's act has constituted preemptive registration of domain name in bad faith and requesting the court to order the defendant to stop using and revoke the preemptively registered domain name and to bear the fees paid by the plaintiff and the fees relating to this lawsuit).



### ***14.3.2 The Ikea “Cybersquatting” Case Summary***

In July 1999, the Ikea Systems B.V. from the Netherlands instituted proceedings in the Beijing No.2 Intermediate People’s Court against the Beijing CINET Inf. Co. Ltd. For an act of unfair competition by preemptive registration of its registered trademark “IKEA” as a domain name, petitioning the court to adjudicate the case, to order the defendant to stop using and to bear the litigation fees, and to revoke the domain name [www.ikea.com.cn](http://www.ikea.com.cn). The Beijing No.2 Intermediate People’s Court has accepted the case.

On June 20 2000, the court made the decision. The court made it clear that the defendant’s registration of the plaintiff’s “ikea” well-known trademark, as its own domain name had not only violated relevant provisions of Administration for Registration of Domain Names on the Internet in China, but also contravened the spirits of the “Paris Convention on Protection of the Industrial Property” and the fundamental principles of PRC Anti-unfair Competition Law. The defendant infringed the legal right and benefit as the owner of a well-known trademark and should undertake the corresponding civil law liability. Therefore, the defendant can no longer use the domain name “ikea.com.cn,” and the registration of such domain name should be revoked. The court held as follows in accordance with para.1, article 2 of ACL:

- The defendant’s domain name registration of “ikea.com.cn” is invalid. The defendant should immediately stop using and revoke such domain name within 10 days after this ruling goes into effect.
- Acceptance fee of this case 1,000 RMB should be paid by the defendant (to be rendered with 7 days after the coming into force of this judgment).

### ***14.3.3 Comment***

Before the Ikea cases, there have already been several domain name disputes brought to the courts. For example, in Guangdong Kelon Group Ltd. V. Yong’an Clothes Making Factory (Beijing Haidian Dist. Basic Level People’s Ct. 1999), Kelon found that Yong’an had registered “kelon.com.cn” as domain name and asked for a large amount of compensation fee for its domain name transference to Kelon. Kelon then filed a lawsuit in the court, claiming that Yong’an’s registering trademark “kelon” as domain name constituted its trademark infringement. In March 1999, Yong’an applied for cancellation of “kelon.com.cn” which it registered as domain name with ICCAN. Kelon finally withdrew its lawsuit against Yong’an.

In another PDA case, the plaintiff pleaded that the defendant preemptively registered the domain name “pda.com.cn” in bad faith, an act constituting an infringement of its trademark and unfair competition, hence petitioning the court to order it to desist from its use of the domain name. The court rejects the plaintiff’s

accusation in the case mainly on these grounds: (1) Registration of domain name for one's own registered trademark is not the right enjoyed by the right holder of the trademark, and meanwhile, registration as a domain name of other's trademark is not one of the trademark infringing acts under Article 38 of the Trademark Law and Rule 41 of its Implementing Regulations. (2) Since PDA trademark is not a well-known trademark and, likewise, "PDA," a name for lap top computer in the industry, does not specifically stand for the entity and products of the plaintiff. In this situation, it is not possible for the public, upon seeing the domain name, to mistake that the Web site with this domain name is specifically related to the plaintiff. The defendant's act to have registered the domain name does not cause any confusion among the public; there does not exist the fact that the reputation of the plaintiff's trademark is exploited to seek interests. And, according to Article 2 of the Anti-Unfair Competition Law, the accusation of the plaintiff that the Defendant's act constitutes an unfair competition is groundless.

The PDA case shows that, within the current legal framework, it is unworkable to resolve conflicts between trademarks and domain names by actions against trademark infringement. If the right holder of a trademark desires to resolve such a conflict by action against unfair competition, it should first of all prove that this is a well-known trademark, that registration by another party of the same trademark as domain name would cause public confusion and misrecognition, or that the defendant's act violates the principle of voluntariness, equality, honesty, and good faith, runs counter to the accepted social ethics, impairs its own lawful rights and interests, and disrupts the socio-economic orders.<sup>14</sup>

In the Ikea case, just as Prof. Liu Chuntian (also the director of the Institute of Intellectual Property of Ren Min University) pointed out<sup>15</sup>: "It is obvious that the court tries to use its independent judicial authority to make up the weakness of "provisional Rules on the Ascertainment and Administration of Well-Known Trademark," (hereinafter the Provisional Rules) which is enforced by State Administration for Industry and Commerce and is criticized by scholars in the following aspects:

(1) As to domestic trademarks, they can only be protected as well-known trademark after being decided by State Trademark Office. This makes trademark acquiring well-known trademark protection very limited. Whereas foreign well-known trademarks need not national uniform decision, they can be particularly protected, according directly to the relevant provisions of Paris Convention on Protection of Industrial Property<sup>16</sup> no matter this trademark is registered or unregistered trademark, just as the "Ikea" court does, it applies the relevant well-known trademark protection provision of Paris Convention directly to deal with the domain name preemptive registration problem, according to article 142 of Chinese

---

<sup>14</sup> See Shan Yan, Basic Court Approach to Handling IP Disputes on the Internet (China Patents & Trademarks No.1, 2000) p.85.

<sup>15</sup> This was based on an interview with Prof. Liu on Sep. 7, 2000 in his research room.

<sup>16</sup> Art.6 bis (1).

General Principles of Civil Law, thus creates man-made domestic/foreign dual standard for trademark protection.<sup>17</sup>

(2) According to the provisional rules, the misappropriated well-known trademark registrant may apply for executive relief within two years from the date he knows or should know. But this prescription can not be completely applied to continuous infringing conducts. No matter that such infringement did not come to an end, he should be entitled to legal protection. (3) According to the Provisional Rules, the well-known trademark right holder can only ask the SAIC to prohibit the infringing conduct, but have no right for damage.

The captioned problems can be solved by adjusting the current mechanism, but there are some problems cannot be solved by doing so. In accordance with the provisions of the Provisional Rules, when a well-known trademark is used by others on dissimilar products or services, the legal protection standard is decided by whether or not there is confusion and whether or not it cause mistaken recognition by the consumers.<sup>18</sup> Therefore, only when it suggests such products or services exist some kind of association with the well-known trademark registrant, and probably make the right and benefit of the well-known trademark registrant being impaired, then constitutes injury to such trademark right. Conclusively, the Chinese well-known trademark protection mechanism is limited to the trademark infringement range provided by Trademark Law and does not involve the “dilution” problem.

Even though Chinese Trademark Law is amending, some commentators advocate adequate regulation on “dilution” problem to enhance well-known trademark protection and deal with domain name disputes. But a much too high trademark protection standard is not necessarily fit for practical situation a developing country such as China. Therefore, some scholar suggests the “dilution” content can be of added into the Anti-Unfair Competition Law depending on the future development.<sup>19</sup>

Finally, it should be noted that the Ikea court addresses the “cybersquatting” problem which has not been regulated by the existing Trademark Law or the

---

<sup>17</sup> Concretely speaking, here exists this situation: “Chinese Law only protects registered trademark as to domestic trademark, but protects registered foreign trademark, and unregistered trademark as to foreign trademark (of course is the well-known trademark decided by such country). Therefore, it provides “super national treatment” for foreign trademark, whereas the domestic unregistered trademark can not be afforded the right derived from the Paris Convention. The reason is in China only the registered trademark can be well-known trademark (See Trademark Law Enforcement Rule Art.12). See Song Sun Lin, *The Challenge on Chinese Trademark Exclusive Right System by Trademark Preemptive Registration* (published by Hebei Law Review (Shijiazhuang) in May, 1998) at p.49.

<sup>18</sup> It should be noted that para.3 of Art. 16 of TRIPs Agreement extends its protection on well-known trademark to dissimilar products or service, so long as such products or services would indicate a connection between those goods or serving and the owner of the registered trademark, and thus does damage to the interest of the well-known trademark owner.

<sup>19</sup> See Xue Hong, *The Net Law is Spacious Also—The Punishment on Domain Name Infringing Acts under Chinese Legal Mechanism* (published by Int’l Trade (Monthly), No.6, 1999) at 50.

relevant provisions of Anti-Unfair Competition Law, by accepting the plaintiff's evidence as true. During the hearing, the plaintiff, Inter-Ikea Co., has showed evidence proving that besides "Ikea," the defendant has also registered many other worldwide famous trademarks or brand names, such as amex/bacardi/boss/cartier/dupont/carlsberg/coia/dunhill/hertz/lancom/lv/marriott/ omega/phillips/polo/rolex/whisper as its domain names, and has not used them on Internet since those domain names was registered.

Though the defendant has made a homepage of vocal forum under this domain name, no practical use has been made pertinent to the purpose of such a homepage. It has also been proved by further inquiry and evidence that many of other trademarks of certain degree of fame have been registered as domain name by the defendant, and no positive use has been made of them either. The court states that to register a great deal of domain name but just to wait for the favorable price to sell, instead of making any positive use of them is obviously a conduct in bad faith. Even though there is no counterpart of US ACPA in China, it seems that the Ikea court has adopted the same approach against "cybersquatting" coincidentally.<sup>20</sup>

#### 14.4 Some Suggestions for Chinese Better Solutions to "Cybersquatting"

According to the previous discussion, the domain name disputes especially involving preemptive registration in bad faith, i.e., the "cybersquatting" problem is not only a personal conduct of the business operator, but also it touches off the deeper layer content of Chinese legal system, thus stir a challenge on the trademark Law Mechanism. Therefore, to amend and enhance trademark, exclusive right system has something to do with the direct benefit of both enterprise and country and is the requisite condition for the enhancement of Chinese industrial property system and healthy development of market economy under socialism as well.

Besides, since China is not a "precedent law" country, we can not rely on the court to solve the increasing "cybersquatting" problem case by case. Even though there has been an opinion entitled "Some Guiding Opinions of Hearing Intellectual Civil Disputes Arising from Domain Name Registration and Use"<sup>21</sup> released by Beijing High People's Court recently, it still can not be deemed as a decisive rule with national jurisdiction.

---

<sup>20</sup> See the (V) and (VIII) factors of the nine factors which a U.S. court may consider (but is not limited to) in determining whether a person has a bad faith intent under Sec. 3002 of the ACPA.

<sup>21</sup> See Beijing Youth Daily, Aug. 25, 2000 at column 3. The Guiding Opinion points out that preemptive registration in bad faith is a kind of unfair competitive conduct. The court can order the malevolent preemptive registrant stop using, apply for revoking or change the domain name, or the court even can adjudicate the registrant to pay for the economic compensation. However, it should be noted that this Guiding Opinion is of local binding effect (i.e. in Beijing area) only.

In conclusion, this article agrees with many Chinese scholars' suggestion to make use of the Anti-Competition Law to provide legal protection for the party infringed by cybersquatting. This is what the Ikea Court has done already. Hopefully, the courts will follow the same approach toward the pending case after the Ikea judgment. Nevertheless, in order to resolve the "cybersquatting" problem thoroughly, it is necessary to establish an ad hoc procedure to deal with the domain name dispute by legislation, and the US Anti-dilution clause and Anti-Cybersquatting Consumer Protection Act seem to be a good reference for amending Chinese Trademark Law or Anti-Unfair Competition Law, or legal mechanism can be adjusted properly, and then, it will effectively provide remedy for the infringed party and curb the cybersquatting phenomenon to the final end.<sup>22</sup>

---

<sup>22</sup> For example, Song Sun Lin, *supra* note 17 at 50. (The trademark preemptive registration conduct can be deemed completely an unfair competitive act under the legal theory.) See also Yin Xue Xin, General Discussion on the Legal Problem of Domain Name (published in *Int'l Trade Questions (Monthly)*, No.5 in May 1999) at 58. (As to the preemptive registration in bad faith and which is used to engage in unfair competitive conduct, we may expand the interpretation of Article 5 of AFCL by interpreting broadly the "market transaction" as dividing into "tangible market transaction" and "cyber electronic market transaction". Therefore, if one preemptively registers other's trade name as his domain name and engages in unfair competitive conduct, it violates the Anti-Unfair Competition Law). But how about the well-known or unwell-known trademarks? Why are they not included in this resolving approach? The author didn't explain! In addition, see Xue Hong, *supra* note 19 at 50 and the accompanying text.

# Chapter 15

## iPad Trademark Dispute: An IPR Management Lesson Not Just for Apple

Weiwei Hu and Yimeei Guo

**Abstract** Apple's paying \$60 million to settle iPad trademark long-standing dispute between itself and Proview Shenzhen. It is worthy for us to have a glance on the dispute at first and to analyze the IPR management lesson for Apple, and figure out some alarms and warnings for China's domestic enterprises to deal with trademark right problems as well.

**Keywords** Trademark · Dispute · IPR management

### 15.1 Introduction

As an internationally renowned trademark brand in the USA, Apple keeps introducing revolutionary electronic products. For example, when new iPad products, e.g., mini iPad and iPhone 5 have been launched since March 2012, it is able to rally multitudes at its call around the world. China is Apple's second-largest market after the USA. China contributed 7.9 billion US dollars, or about 20 % of Apple's revenues, during its second fiscal quarter in 2012 (Apple buys trademark 2012). But, it is prevented for China's consumption because of a long-standing trademark dispute between Apple and Proview Shenzhen starting from 2010.

Even though Apple finally agreed to pay Proview Shenzhen \$60 million to settle the trademark dispute between them in June 2012, it has not yet assumed ownership of the iPad mark. And now Grandall, the law firm that represented Proview in its spat with Apple, has asked a court to seize the mark until the company pays off its legal fees (China iPad Trademark Dispute Refuses to Stay Dead 2012).

---

W. Hu (✉) · Y. Guo  
School of Law, University of Xiamen, Xiamen 361005, China  
e-mail: Helusi420hw@163.com

Y. Guo  
e-mail: ymguo@xmu.edu.cn

Nevertheless, for Apple, the settlement can help it seize huge market opportunities in China. Otherwise, Apple might not have been able to sell its popular tablet computers in the Chinese mainland. It should also be noted that currently the amount of the captioned trademark settlement is reported to be the top one among all IPR infringement cases in China (Qu 2012), it thoroughly breaks the previous “nominal price” theory for trademark right.

Thus, it is worthy for us to have a glance on iPad trademark dispute between Apple and Proview Shenzhen at first and to analyze the IPR management lesson for Apple, and figure out some alarms and warnings for China’s domestic enterprises to deal with trademark right problems as well.

## 15.2 iPad Trademark Dispute—a Fact Summary

Proview Shenzhen had previously claimed that the Taipei subsidiary of its Hong Kong-based parent company, Proview International Holdings Limited, registered the iPad trademark in a number of countries and regions as early as 2000.

According to testimony in the legal fight, Apple retained British lawyers several years ago to set up a company, IP Application Development Limited, to buy up rights to the iPad name around the world. Apple paid only £35,000 to Proview Taipei for that company’s iPad trademarks in various countries.

Though Apple bought the rights to use the iPad trademark from Proview Taipei in 2009, Proview Shenzhen said it reserved the right to use the trademark it registered on the Chinese mainland in 2001. The two sides have since been entangled in a drawn-out legal battle.

Apple and its proxy IP Co. for the trademark purchase brought a lawsuit against Proview Shenzhen on April 19, 2010, concerning iPad trademark’s attribution. Guangdong Province Higher People’s Court heard the case in February 2012, as Apple and IP Co. appealed the previous court ruling by the Shenzhen intermediate People’s Court in favor of Proview Shenzhen in November 2011 (Apple buys trademark 2012).

Apple also filed a complaint against Proview Shenzhen in Hong Kong for failing to honor its agreement in May 2010. The Hong Kong court decides in Apple’s favor in June 2011 (Elmer-DeWitt 2012). In May 2012, the Hong Kong court also decided that two copies of expert report presented by Proview Shenzhen in 2011 will not be recognized by the court because they were not in accord with the court’s instruction (The Materials for Proview v 2012).

As to Proview Shenzhen, it has started to bring the lawsuit against Apple’s distributors in Guangdong district since December 2011, it demanded Apple’s distributors stop infringement, i.e., stop using iPad trademark (Memorabilia of TM dispute between Proview and Apple 2012). On February 17, 2012, Guangdong Province Huizhou City Intermediate People’s Court held that one of the Apple’s distributors in Shenzhen to be prohibited to sell Apple’s iPad. This the first Apple’s distributor held losing the case so far (Guangdong Province Huizhou City 2012).

In January 2012, Proview Shenzhen also filed the lawsuit against Apple Trading (Shanghai)Co., Ltd for trademark infringement. But on February 23, 2012, its application for interim injunction was rejected by Shanghai Pudong New Area People's Court on the grounds that "iPad trademark case is still at second trial in Guangdong's higher court" (He 2012).

In February 2012, Proview Shenzhen filed a lawsuit in California, alleged that Apple engaged in deceptive practices when it acquired the iPad name in 2009. But on May 8, 2012, the case was thrown out by Judge Mark Pierce in the Superior Court of the State of California in Santa Clara County citing an apparent agreement showing that Apple and Proview Shenzhen had to adjudicate their differences in Hong Kong courts. After Proview Shenzhen took their legal case to the USA, Apple argued for the case to be dismissed on the grounds that the parties had agreed to settle any legal disagreements in the Chinese city-state. Pierce agreed saying Proview Shenzhen failed to provide evidence that the selection of Hong Kong was "unreasonable or unfair" (Wolfe and Bryan 2012).

In June 2012, Proview Shenzhen was brought to court in a bankruptcy case. Its creditors demanded that the court have the company liquidated, as it took a tumble in the 2008 global financial crisis and allegedly owed more than 400 million US dollars to eight Chinese banks, according to media reports.

Finally, on July 2, 2012, Guangdong Province Higher People's Court said in a statement that Apple had settled the lawsuit there by paying \$60 million into a court-approved bank account for the legal rights to use the iPad trademark in China. The mediation letter was sent to both parties and came into effect on June 25, 2012. A request has been made by legal authorities to the State Administration for Industry and Commerce (SAIC) to transfer the iPad name from Proview Shenzhen to Apple (Zheng et al. 2012).

## 15.3 An IPR Management Lesson

### 15.3.1 *Apple's Woolly Trademark Management*

Being regarded as the essential intellectual products in life and economy, trademarks not only are closely related to lives of ordinary citizens, but also the intangible assets and weapon in business for the producers. Trademarks transfer through three ways which are contract, inheritance, and some administrative orders. These transfers enable the registered trademarks get circulated to adapt to the requirements of the companies, enterprises, and the market. Comparing with the traditional commodity trading, intellectual property transactions are typically indirectly conducted by the trademark holders. Thus, transfer process of a registered trademark is highly specialized, complex in legal relationship, and the cases are always complicated. Thus, before promoting intellectual products in the market, enterprises should fully regulate their trademarks transfer and improve the trademarks protection strategy.



The basic reason for Apple to encounter this huge trouble in China is that Apple itself did not soundly protect trademark in advance. Whether believing the method of keeping confidential too much or not, the early work of those attorneys who took charge of Apple's trademark transfer were very disqualified. They even did not make general investigation from the beginning to under the exact attribution of relevant trademark. At the same time, the agreement signed by Apple and Proview Taipei was also too rough without regulating specific transfer detail. Just as several years ago, Apple unexpectedly registered iPhone trademark in China without registering in mobile category. Therefore, Apple has to confront trademark litigation at up for several years because of lack of protection for its own brand and lack of trademark awareness.

Simultaneously, being the company which owns trademark in China's district, it surprisingly did not sign the above-mentioned contract. But in fact, trademark transfer is a formal act which requires the trademark right holder's attendance. Hence, Proview Taipei is incompetent to represent Proview Shenzhen to sell the trademark and cannot transact the procedures of trademark transfer as an agent. All of those stuffs are home works which should be done beforehand, not to mention involving the company's core product. Just as the first trial judge in *Apple v. Proview Shenzhen* case pointed out: "The court thinks that Plaintiff wanting to acquire commercially other people's trademark shall bear higher duty of care, sign trademark transfer contract with the trademark right holder in accordance with China's laws and regulations and go through the necessary procedure for trademark transfer" (Civil Judgment of Shenzhen Intermediate People's Court 2010).

Actually, iPad trademark dispute is not the first one in China. As stated above, Apple had bled once for "iPhone" trademark. Early in 2002, Apple filed the application to China Trademark Office for "iPhone" trademark registration, but people cannot understand that its trademark category only included computer software and hardware and did not include telephone and mobile phone. The result was Hanwang Technology filed the application for "iPhone" trademark registration on commodities such as telephone set, portable telephone, and video telephone, etc., and obtained approval thereafter.

Owing to this very puzzled and low-grade error, Apple's "iPhone" cell phone could not enter into China after it was released in 2007. It was until July 18, 2009, Apple reached an agreement with Hanwang Technology and paid \$3.65 million (calculated in RMB 24,904,600), it took back such precious trademark (*Proview v 2012*).

Business is business. As one kind of IPR, trademark by nature is one kind of property and another kind of market competitive strategy except tariffs, patent after the non-trade barriers. When a company is doing planning, it should make certain anticipation for its trademark. If it is a trademark regarded as important by the company, it can be completely registered in advance or finalize the deal through a proxy. If done so, even there is squatting, it will not cause the company any trouble. But as a Western company having a long history, it should know and take seriously market rules. If Apple cannot always make good and careful protective plan and pay attention even to its owned core product, then it will repeatedly face the captioned embarrassed situation in China.

### ***15.3.2 What Can China's Enterprises Learn from iPad Trademark Dispute?***

Just as Stan Abrams, a law professor at Central University of Finance and Economics indicates, the case showed “how complex cross-border or multi-jurisdictional intellectual property issues can be.” Companies must do their homework. “If Apple, which is one of the world’s largest multinationals, can make these kinds of mistakes, that should really serve as an example for smaller, less experienced companies, including those from China, that they need to take great care in cross-border deals.”

Wang Jun, a law professor at Fudan University, agreed that the arrival of more foreign capital could herald an escalation in legal disputes, especially over intellectual property. “Apple would not have got into trouble if it had done due diligence.”

Feng Xiaoqing, an intellectual property scholar with the China University of Political Science and Law, said companies should attach equal attention to the management of intellectual property rights as they did to creating them. “They have to look forward in making brand strategies. Otherwise, they may face difficulties in seeking protection or end up paying large sums” (Zheng et al. 2012).

Generally speaking, China’s enterprises must put great emphasis on trademark’s value, establish ad hoc trademark management department with full-time staff to form perfect trademark management system, and aggressively protect their rights once finding infringement.

## **15.4 Conclusion**

It is universally accepted by legal professionals that before completing trademark right transfer to be most impatient to launch products and wantonly use iPad trademark is the fatal mistake committed by Apple. It is also evaluated by insiders that the successful mediation of iPad trademark dispute realizes the value maximization of iPad trademark, greatly protects creditors’ rights and interests, create a new route to solve trademark attribution concerning foreign affairs so as to have milestone significance in China’s IPR trial history.

As everyone knows, trademark is a brand kernel and important constitutive requirement of intangible assets; it can bring excess profit to enterprises within a longer period. Thus, trademark is called “perpetual note printing machine” by people. At present, even though China’s IPR protection environment is not quite ideal and most of enterprises’ protection consciousness is not so strong, Proview Shenzhen faced such a powerful multinational giant (Apple possibly will launch iPhone 5 2012) and engaged in lawsuits with it with full confidence. This shows that more and more domestic enterprises are not afraid of strong nemeses, argue on the basis of reason and are brave to apply the law to safeguard their legitimate

rights and interests. In this sense, Apple was “bitten” by Proview Shenzhen provides a valuable specimen for China’s enterprises to improve awareness of IPR and apply the law to protect self interests and benefits.

Besides, Proview Shenzhen’s biting Apple let us see that technology can be bought by capital to level difference, but core competitiveness is still creativity and innovation. Without its owned core IPR, even grasps the same technology, the enterprise can only make “copycat product” and even though it squats a valid trademark, there is no guarantee for its optimistic prospect. Proview Shenzhen’s bankruptcy ending seems proving this issue.

## References

- Apple buys trademark, may soon offer new iPad to China. 2012. <http://english.peopledaily.com.cn/102774/7863407.html>. 03 July 2012.
- Apple possibly will launch iPhone 5 on September 12, 2012. Its stock price startling rose to \$6235 m on August 20, 2012 with the market optimistic expectation, exceeded the record of Microsoft witten in 1999 and became the company owning the highest market capitalization in global history. See Apple’s market capitalization exceeded the record of Microsoft—the highest in history. <http://udn.com/NEWS/WORLD/WOR2/7311522.shtml>. 22 Aug 2012. (Published by “Proceedings of 2013 3rd International Conference on Applied Social Science <ICASS 2013>”, Vol. 1, pp. 22–26, Jan 2013).
- China iPad Trademark Dispute Refuses to Stay Dead. 2012. <http://allthingsd.com/20120727/china-ipad-trademark-dispute-refuses-to-stay-dead/>. Visited on 20 Aug 2012.
- Civil Judgment of Shenzhen Intermediate People’s Court. 2010. Shen Zhong Fa Min San Chu Zi No. 206, 233.
- Elmer-DeWitt, Philip. 2012. How may Apple terminate long legend as iPad’s leader. <http://www.emarketing.net.cn/operation/detail.jsp?did=1956>. 22 July 2012.
- Guangdong Province Huizhou City Intermediate People’s Court held an Apple’s distributor to be prohibited to sell iPad (Chinese version). 2012. <http://tech.sina.com.cn/it/2012-02-17/20456738359.shtml>. 17 Feb 2012.
- He, Jing. 2012. Shanghai Pudong new area People’s Court rejected the application for interim injunction in ‘Proview v. Apple case’ and suspended the litigation (Chinese version). <http://old.chinacourt.org/html/article/201202/24/475694.shtml>. 24 Feb 2012.
- Memorabilia of TM dispute between Proview and Apple (Chinese version). 2012. [http://news.1nd.com.cn/htm/2012-03/07/content\\_2197221.htm](http://news.1nd.com.cn/htm/2012-03/07/content_2197221.htm). 7 Mar 2012.
- Proview v. 2012. Apple trademark dispute: disclosing state-owned enterprises’ weak sense of trademark right (Chinese version). [http://blog.sina.com.cn/s/blog\\_9389932401011j7t.html](http://blog.sina.com.cn/s/blog_9389932401011j7t.html). 3 Mar 2012.
- Qu, Lili. 2012. The expense of Apple’s arrogance: from \$10 m to \$60 m (Chinese version). <http://tech.qq.com/a/20120707/000075.htm>. Visited on 20 Aug 2012.
- The Materials for Proview v. 2012. Apple trademark infringement were rejected by Hong Kong Court (Chinese version). [http://news.iyaxin.com/content/2012-05/23/Content\\_3491874.htm](http://news.iyaxin.com/content/2012-05/23/Content_3491874.htm). 23 May 2012.
- Wolfe, Bryan M. 2012. Apple Scores iPad Trademark Victory in California. <http://appadvice.com/appnn/2012/05/apple-scores-ipad-trademark-victory-in-california>. 9 May 2012.
- Zheng, Caixiong, Wenting, Zhou, Wang H. 2012. Apple settles iPad trademark case with \$60 m. <http://english.peopledaily.com.cn/102774/7863382.html>. 3 July 2012.

# Chapter 16

## A Comment on Chinese Legal Environment of Online Copyright Protection

Yimeei Guo

**Abstract** China's online population has grown rapidly in recent years from just 620,000 in 1997. Independent forecaster Analysys International said earlier in 2005 it expected the total number of citizens in China to reach 134 million by late 2005. According to "2005 Special 301 Report" released by USTR concluding that infringement levels remain unacceptably high throughout China, in spite of Beijing's efforts to reduce them. Among other things, Internet piracy is quickly becoming the number one threat to the copyright industry. Therefore, this article tries to conduct a comprehensive survey on Chinese legal environment of online copyright protection, including introducing government policies, the recently enacted and amended relevant law and regulations, and discussing judicial views by doing some case studies as well. Finally, this article calls for China's corporation with her trading partners especially the USA to work out to diminish the conflicts arising from IPR infringement disputes in China including the online aspect. Hopefully, a goal of "double or multiple wins" can be achieved thereafter.

**Keywords** Internet piracy · Chinese legal environment of online copyright protection · Corporation

### 16.1 Introduction

According to a report in *the People's Daily*, the copyright industry production value contributed more than 6 % to China's GDP. The copyright industry is based on the manufacture, storage, usage, and consumption of knowledge and information, involving such fields as literature, art, journalism, publishing, broadcasting, cinema, computer software, and Internet.

---

Y. Guo (✉)

Management Science Department, Xiamen University, Xiamen 361005, China  
e-mail: yimei\_guo@necmail.xmu.edu.cn

China has had a batch of exemplary companies in the copyright industry, such as the Shanda Interactive Entertainment Limited (Nasdaq: SNDA), an interactive entertainment media company opened to run in Shanghai in 1999 that offers a portfolio of diversified entertainment content that users access via the Internet. With more than 10 products developed by itself or operated as an agent, SNDA earned 154 million US dollars from Internet games in 2004, with all its services each having a 100 % increase.

The Chinese copyright industry, however, still faces challenges; Shen Rengan, director-general of the Copyright Society of China, pointed out “Copyright awareness of the public is still weak, and some local governments conceal and even connive in copyright infringement actions, and smuggled pirated productions into China are encumbering China’s copyright industry.”<sup>1</sup>

For example, an article in *LA Times* discusses Time Warner’s strategy of making legitimate DVDs available for as low as \$2.65, which has difficulty competing with lower-quality knockoffs that compress 5 movies onto a single disk for \$0.60 in China. However, price is not the only factor working against the big media companies. Timing is crucial too, and cultural sensitivities and bureaucracy can block or delay the official release of DVDs in China, giving pirates an opening.

The Ministry of Culture, which has a staff of 50 who review foreign movies and music, would not comment on specific titles. But Chen Tong, director of the Ministry’s Audio-Visual Movie Section, said it was “complete nonsense” that government censorship played a decisive role in hurting sellers of legitimate DVDs. The Internet gives bootleggers an advantage, Chen said, and studios sometimes are the ones responsible for delays.<sup>2</sup>

Nevertheless, China’s online population has grown rapidly in recent years from just 620,000 in 1997. Independent forecaster Analysys International said in early 2005 it expected the total number of citizens in China to reach 134 million by late 2005.<sup>3</sup>

China has long been on the USTR’s “Priority Foreign Country List” resulting from a Special 301 investigation against China ever since 1991. China avoided USTR’s threatened sanctions four times by signing an MOU on IPR separately in 1992, 1994, 1995, and 1996. In its “2002 National Trade Estimate Report,” the US Trade Representative (USTR) explained “China has made substantial progress in some aspects of intellectual property rights protections since it signed agreements in 1992, 1994, 1995, and 1996 ... However, significant problems remain, particularly in the area of enforcement.”<sup>4</sup>

<sup>1</sup> “Copyright industry contributes 6 % to GDP”, May 29, 2005, [http://news.xinhuanet.com/english/2005-05/29/content\\_3016621.htm](http://news.xinhuanet.com/english/2005-05/29/content_3016621.htm).

<sup>2</sup> Ernest Miller, “Gov’t Censorship Spurs Copyright Infringement in China”, May 15, 2005, [http://www.corante.com/importance/archives/2005/05/15/govt\\_censorship\\_spurs\\_copyright\\_infringement\\_in\\_china.php](http://www.corante.com/importance/archives/2005/05/15/govt_censorship_spurs_copyright_infringement_in_china.php).

<sup>3</sup> “China expects 120 m netizens by year end”, March 3, 2005, [http://english.people.com.cn/200503/03/eng20050303\\_175348.html](http://english.people.com.cn/200503/03/eng20050303_175348.html).

<sup>4</sup> USTR (2002, p. 14).

On April 29, 2005, the Office of USTR released its “2005 Special 301 Report.”<sup>5</sup> The report also announced the results of a special Out-of-Cycle Review (OCR) of China’s intellectual property regime in early 2005, concluding that infringement levels remain unacceptably high throughout China (see also Chart below), in spite of Beijing’s efforts to reduce them.<sup>6</sup> The USTR has now elevated China to the Priority Watch List.

Among other things, Internet piracy is quickly becoming the number one threat to the copyright industry according to OCR submissions.<sup>7</sup>

**Chart: USTR 2005 “Special 301” Decisions on Intellectual Property**

IPA 2003–2004 ESTIMATED TRADE LOSSES DUE TO COPYRIGHT PIRACY (in millions of US dollars) and PIRACY LEVELS IN COUNTRY

	Motion pictures		Records and music		Business software <sup>a</sup>		Entertainment software <sup>b</sup>		Books	Total losses
	Losses	Piracy levels	Losses	Piracy levels	Losses	Piracy levels	Losses	Piracy levels	Losses	
Priority watch list										
People’s Republic of China	280.0	95 %	202.9	85 %	1465.0	90 %	510.0	90 %	50.0	2507.9

<sup>a</sup>BSA’s 2004 piracy statistics are preliminary. BSA’s final 2003 figures represent the US software publisher’s share of software piracy losses in each country as compiled in October 2004. In prior years, the “global” figures did not include certain computer applications such as operating systems, or consumer applications such as PC gaming, person, finance, and reference software. These software applications are now included in the estimated 2003 losses resulting in a significantly higher loss estimate than was reported in prior years

<sup>b</sup>BSA’s reported dollar figures reflect the value of pirate product present in the marketplace as distinguished from definitive industry “losses”

Source Excerpted by Yi-meei Guo from: [http://www.iipa.com/pdf/2005\\_Apr29\\_USTR\\_301DECISIONS\\_Asia.pdf](http://www.iipa.com/pdf/2005_Apr29_USTR_301DECISIONS_Asia.pdf)

Therefore, this article tries to conduct a comprehensive survey on Chinese legal environment of online copyright protection, including introducing government policies, the recently enacted and amended relevant law and regulations, and discussing judicial views by doing some case studies as well. Finally, this article calls for China’s corporation with her trading partners especially the USA to work out to diminish the conflicts arising from IPR infringement disputes in China including the online aspect. Hopefully, a goal of “double or multiple wins” can be achieved thereafter.

<sup>5</sup> The full text can be found in [http://www.ustr.gov/assets/Document\\_Library/Reports\\_Publications/2005/2005\\_Special\\_301/asset\\_upload\\_file195\\_7636.pdf](http://www.ustr.gov/assets/Document_Library/Reports_Publications/2005/2005_Special_301/asset_upload_file195_7636.pdf).

<sup>6</sup> “US reveals intellectual property blacklist”, May 3, 2005, [http://www.out-law.com/php/page.php?page\\_id=usrevealsintellect1115115505&area=news](http://www.out-law.com/php/page.php?page_id=usrevealsintellect1115115505&area=news).

<sup>7</sup> USTR Releases 2005.

## 16.2 Implementation of the WTO TRIPS Agreement

One of the most significant achievements of the Uruguay Round was the negotiation of “the Agreement on Trade-Related Aspects of Intellectual Property Rights” (hereinafter TRIPS Agreement), which requires all World Trade Organization (WTO) Members to provide certain minimum standards of protection for patents, copyrights, trademarks, trade secrets, geographical indications, and other forms of intellectual property. The Agreement also requires countries to provide effective IPR enforcement. The TRIPS Agreement is the first broadly subscribed multilateral intellectual property agreement that is subject to mandatory dispute settlement provisions.

Developed countries were required to fully implement the TRIPS Agreement as of January 1, 1996, while developing countries were given a transition period for many obligations until January 1, 2000. Ensuring that developing countries are in full compliance with the TRIPS Agreement obligations now that this transition period has come to an end is one of the Bush Administration’s highest IPR priorities. The least developed countries have until January 1, 2006, to implement the TRIPS Agreement.

However, in order to address the concerns raised by the least developed countries, the United States suggested, and all other WTO members agreed, to extend the transition period for 10 years, until 2016, for the least developed countries to implement their TRIPS obligations for patent and data protection for pharmaceutical products.

Developing countries continue to make progress toward full implementation of their TRIPS obligations. Nevertheless, certain countries are still in the process of finalizing implementing legislation and establishing adequate IPR enforcement mechanisms. Every year, the US Government provides extensive technical assistance and training on the implementation of the TRIPS Agreement to a large number of US trading partners. Such assistance is provided by a number of US Government agencies, including the US Patent and Trademark Office, the US Copyright Office, the Department of State, the US Agency for International Development, US Customs and Border Protection, the Department of Justice, and the Department of Commerce.

This assistance is provided on a country-by-country basis, as well as in group seminars, including those cosponsored with the World Intellectual Property Organization (WIPO) and the WTO. In addition, US industry is actively involved in providing specific enforcement-oriented training in key markets around the world. Technical assistance involves the review of, and drafting assistance on, laws concerning intellectual property and enforcement. Training programs usually cover the substantive provisions of the TRIPS Agreement, including IPR enforcement.<sup>8</sup>

---

<sup>8</sup> USTR 2005.

## 16.3 Internet Piracy and the WIPO Internet Treaties

The Internet has undergone explosive growth and, coupled with the increased availability of broadband connections, serves as an extremely efficient global distribution network for pirated products. The explosive growth of copyright piracy on the Internet is a serious problem.

An important first step in the fight against Internet piracy was achieved at WIPO when it concluded two copyright treaties in 1996: “the WIPO Copyright Treaty” (WCT) and “the WIPO Performances and Phonograms Treaty” (WPPT) (collectively, the “WIPO Internet Treaties”).

The WIPO Internet Treaties help to raise the minimum standards of intellectual property protection around the world, particularly with respect to Internet-based delivery of copyrighted works. They clarify exclusive rights in the online environment and specifically prohibit the devices and services intended to circumvent technological protection measures for copyrighted works.

Both treaties entered into force in 2002. As of April 29, 2005, there are 51 members of the WCT and 49 members of the WPPT; this number will rise significantly when the EU joins, which, by internal arrangement, is expected to occur when the last five EU Member States complete their implementation processes.

Many countries have implemented in their national laws key provisions of these treaties even though they have not yet formally ratified them. At this point, therefore, the WIPO Internet Treaties are now part of the international IPR legal regime and represent the consensus view of the world community that the vital framework of protection under existing agreements, including the TRIPS Agreement, should be supplemented to eliminate any remaining gaps in copyright protection on the Internet that could impede the development of electronic commerce.

In order to realize the enormous potential of the Internet, a growing number of countries are implementing the WIPO Internet Treaties and creating a legal environment conducive to investment and growth in Internet-related businesses and technologies.<sup>9</sup>

## 16.4 A Glance at China’s Legal Environment of Internet Copyright Protection

### 16.4.1 *Government Anti-piracy Policy and Efforts—A Software Industry Perspective*

On July 27, 2004, Chinese Vice-Premier Wu Yi said at “the Second China International Software and Information Service Fair” in Dalian that the country

---

<sup>9</sup> Ibid.



regards software as an industry with strategic importance and is formulating effective policies in areas including anti-piracy and anti-monopoly, to encourage its development. Wu Yi said that only with effective IPR protection could software companies be interested in staying in the business and contributing to the prosperity of the industry.

Apart from tighter government efforts in using copyrighted software, another challenge for pirated software pedlars is the increasing unauthorized proliferation of software on the Internet. As the Internet has grown more and more popular among the Chinese, it has also become a faster route for peddling the software.

A report by the Electronics Intellectual Property Rights Consulting and Service Center (EIPRC) under the Ministry of Information Industry (MII) and the China Software Industry Association (CSIA) in 2004 indicated that organizational users get 10 % of their software from the Internet, while the rate was 34 % among individual users. Despite the increasing adoption of copyrighted software among enterprises and organizations, unauthorized copies within organizations became another issue meeting serious concerns from software companies.

The EIPRC-CSIA report showed illegal copying, and unauthorized use of copyrighted software ranked the No. 1 means of piracy in the eyes of software companies, even before pirated discs, pre-installation with hardware, and Internet downloading.

Zhao Tianwu, director of EIPRC, said the results showed there was still a lot of work to be done to improve software users' awareness of IPR protection, which should include more than simply not buying pirated software disks.

More than 60 % of the organizations surveyed said education could raise people's awareness of IPR protection. Forty percentage of them believed education with examples of legal and financial risks was the most effective way. From the software companies' side, 72 % of them said the law should be enforced more strictly, or the legal system improved, while only 9.8 % of them said education through the media was more effective.

It is believed that all these things might need a lot of effort from the government, companies, and ordinary users, and it will take a long time to elevate people's awareness to a significant degree.<sup>10</sup>

### ***16.4.2 Law and Regulations***

China's legal system for copyright protection was gradually established in the 1990s, with the implementation of the "Copyright Law" as a hallmark in this process. It has also promulgated a number of regulations with legal effect, such as "Regulations on the Protection of Computer Software," "Regulations for the Implementation of the Copyright Law," "Procedures for the Implementation

---

<sup>10</sup> Wen 2004.

of Administrative Sanctions Concerning Copyright,” and “Regulations on the Collective Management of Copyright.” The promulgation and implementation of these legal documents have laid a solid legal foundation for copyright protection.

As to Chinese “Copyright Law,” it was issued on June 1, 1991. In accordance with its accession to the WTO in 1999, and to comply with its obligations on copyright protection under the TRIPS Agreement, China has amended its “1991 Copyright Law” on October 27, 2001. Besides, changes in the international and domestic environments, development of the information technology (IT) also demanded amendments to Chinese “Copyright Law.”

The amended law features regulations relating to online copyright protection, such as adding a new kind of property to the copyright owners in accordance with the WIPO Internet Treaties as follows: “the right of communication via information networks, that is, the right to communicate to the public a work, by wire or wireless means in such a way that members of the public may access these works from a place and at a time individually chosen by them” provided by Article 9(xii).

But Chinese “Copyright Law” does not specify that the right of reproduction applies in the digital network environment, nor does its definition of the right of reproduction provided by Article 9(v) follow the expression “in any manner or form” as used in Article 9 of the Berne Convention. Consequently, despite recognizing the right of communication via information networks, it seems that the “Copyright Law” is not adequate enough to effectively protect the copyright in the digital network environment.

Therefore, it is suggested by some expert that the legislation enables the right of reproduction to cover the acts of temporary reproduction with proper limitation on it. In respect of the proper limitations, the legislation may follow the relevant agreed statements of the WIPO Internet Treaties, or consult with “the EU Copyright Directive” to expressively provide that temporary act of reproduction, if it is a transient or incidental act, and an integral and essential part of a technological process with a purpose of enabling a transmission in a network by an intermediary, or a lawful use of a work, performance or phonogram to be made, and without any independent economic significance, should be exempted from the limitation on the right of reproduction.<sup>11</sup>

Nevertheless, in accordance with the pertinent provisions of the “Criminal Law of the People’s Republic of China,” the Supreme People’s Court and the Supreme People’s Procuratorate, out of practical need for punishing IPR infringement crime, promulgated “*the Interpretation on Several Issues of Concrete Application of Laws in Handling Criminal Cases of Infringing Intellectual Property*” (hereinafter referred to as “*the Interpretation*”) on December 8, 2004, to further strengthen criminal judicature protection of intellectual property,

---

<sup>11</sup> Liu (2004, p. 76).

effectively crack down on intellectual property infringement crime, maintain market economic order, and constantly improve legal protection level of intellectual property in China. The interpretations went into effect on December 22, 2004.<sup>12</sup>

Under *“the Interpretation,”* Internet copyright violators may face criminal prosecution in China if their ultimate motive is profit. It expands the scope of intellectual property rights offences that are now considered criminal, i.e., Article 11, Sect. 3 stipulates “People who spread others’ writings, music, film and video products as well as computer software via the Internet without authorization shall be deemed ‘reproduction and distribution’ under Article 217 of ‘Criminal Law.’”

Besides, *“the Administrative Measures for Internet Copyright Protection”* jointly issued by the National Copyright Administration and the MII is scheduled to be implemented on May 30, 2005. This is another legislative step China takes to improve the legal protection system for Internet copyright following *“the Supreme Court’s Interpretation of Several Issues Concerning the Laws Applicable to the Hearing of Copyright Disputes Involving Computer Networks.”*

By the end of 2004, China had had ten Internet skeleton networks, more than 800 Internet information access service providers, nearly 10,000 Internet information service providers, hundreds of thousands Web sites, and nearly 100 million netizens. The fast-growing Internet has made considerable contribution to the development of China’s information industry. At the same time, Internet copyright has become a problem impeding the further development of China’s Internet.

Generally speaking, the release of *“the Administrative Measures for Internet Copyright Protection”* will contribute to both China’s online copyright protection and the development of information industry.<sup>13</sup>

### ***16.4.3 Selective Online Copyright Infringement Case Studies***

#### **16.4.3.1 Two Model Cases Before China’s 2001 Copyright Law Amendment**

Cases concerning infringement of copyright of works placed on the Web had occurred frequently in China in the past few years, while the *“1991 Copyright Law”* had no clear provisions dealing with online copyright disputes. When faced

<sup>12</sup> Intellectual Property Protection in China 2005, <http://jp2.mofcom.gov.cn/aarticle/chinanews/200503/20050300030740.html>.

<sup>13</sup> “China to implement first administrative regulations on Internet copyright protections”, May 18, 2005, [http://english.people.com.cn/200505/18/eng20050518\\_185529.html](http://english.people.com.cn/200505/18/eng20050518_185529.html). See also “China protects Internet copyright through legislation”, May 17, 2005, [http://english.people.com.cn/200505/17/eng20050517\\_185451.html](http://english.people.com.cn/200505/17/eng20050517_185451.html).

with these cases, the Chinese courts boldly interpreted then existing Chinese copyright law, giving them new meanings for the Internet age.

- *Wangmeng et al. v. Century Internet Communications Technology Co. Ltd. (1999)*<sup>14</sup> (nature of online dissemination of copyrighted works and ISP/ICP's liabilities)

In this nationwide-known case, a Beijing court held that, except as otherwise provided by the law, any entity or individual with publicly exploits others works without authorization, constitutes copyright infringement. The case involved a dispute between six famous Chinese writers and one of China's earliest Internet service provider (ISP) and Internet content provider (ICP) (hereinafter ISP/ICP). The defendant established on its Web site a novel section, which carried a lot of novel stories by Chinese writers, including those authored by the above six writers. The works were uploaded by a special group in charge of the maintenance of this section on the Web site, which got the works either by downloading them from other Web sites or from novel fans who e-mailed the works to the group for free.

The defendant argued that existing Chinese law had no provision on whether the dissemination of other's works via the Internet required prior consent from the copyright owners concerned or how to pay the copyright owners remunerations. It maintained that it was not the first one to put the works on the Internet, and therefore, it was not aware of the exploitation of the plaintiffs' works on the Internet.

The First Instance Court, the Beijing Haidian District Court, interpreted that current copyright laws cover online publications and distributions. It held:

Paragraph 5 of Article 10 of the Copyright Law of China does not exhaust or enumerate all means of exploiting works. With the development of science and technology, new media of works will emerge and the range of exploiting works will be expanded. .... It should be affirmed that the dissemination of works via the Internet was one of the ways of using works, and the copyright owners of works had the right to decide whether their works could be disseminated through the Internet. .... Although the dissemination of works through the Internet is somewhat different from the ways of exploiting works through publication, circulation, public performance and play as defined by "the Copyright Law of China", it is meant in essence to realize the dissemination of works to the general public, to enable viewers or listeners to know the content of the works concerned. .... The difference among the ways of disseminating works should not affect the right of the copyright owners to control the dissemination of their works.

As to the defendant's liabilities, the court ruled that the defendant, as an ISP/ICP, was an infringer, because it saved the works on its Web servers and made it available to everyone who visited the Web site. The First Instance Court's decision was fully upheld by the appeal court. The most prominent feature of the case is that Chinese courts began to decide cases by relying on its own interpretations of legislative intent. The appeal court held that, since the legislative intent is to protect the exclusive right of copyright owners, it is natural to reason that the law governs online use of works, which is only one of the ways of using works. This is a very

---

<sup>14</sup> No. 57 (1999) of the Intellectual Property Branch of Haidian Dist. Court.

encouraging message for copyright owners who are concerned with their rights being infringed in China.

- *Chen Weihua v. Chengdu Computer Business Information Weekly (CBIW)* <sup>15</sup> (determining authorship of online works)

Chinese courts also dealt with cases concerning identification of authors of works published on the Internet. Generally, Chinese judges' view is that it is the defendants' burden of proof to prove the plaintiff is not the legitimate author. In this so-called 3D Sesame Street case, an article entitled "Joking Talk about MAYA" was uploaded to a Web page called "3D Sesame Street," with the author name "Wufang." Later, the article was published on a newspaper with the name "Wufang," but no contribution fee was paid. The plaintiff claimed "Wufang" was his penname and sued for copyright infringement, but the defendant insisted that the plaintiff proves he was "Wufang" at first. The Beijing Haidian Dist. Court, upon the finding that (1) the article was first published on "3D Sesame Street" Web page and that (2) the Web page was the plaintiff's homepage because the plaintiff was in control of the homepage access, ruled that the plaintiff was assumed the true author of the article, unless the defendant could provide reasonable evidence to prove the contrary.

As indicated in the captioned cases, Chinese courts touched some respects of online copyright infringements and preferred to protect the rights of true copyright owners. However, in a traditionally civil law country like China, the judges' enthusiasm cannot last long without legislative backup.<sup>16</sup> As pointed out by a Chinese judge, the online copyright problem "must be tackled through the joint efforts of legislature, judicial authority and the jurisprudence circle."<sup>17</sup>

2. *Hanwang Tech. Co. v. Taiwan Jingpin Tech. Co. & Zhongshan Mingren Computer Development Co.*(2005) (China's first online software sales infringement case)

According to China's Legal Daily, after 4 years' of court hearings, the Beijing Municipal Superior People's Court issued a judgment in China's first online software sales infringement case in May 2005. The two defendants, Taiwan Jingpin Technology Company and Zhongshan Mingren Computer Development Company, were ordered to pay Hanwang Technology Company RMB ¥300,000 and RMB ¥2.8 million, respectively, as compensation.

In May 2000, Taiwan Jingpin Technology Company began to manufacture and sell online the "WinCE Handwriting Chinese Characters Identification Core V1.0" software, which was developed by Hanwang Technology. In the same year, Zhongshan Mingren installed the pirated software, provided by Taiwan Jingpin Technology Company, in Zhongshan Mingren PC products.

<sup>15</sup> No. 18 (1999) of the Intellectual Property Branch of Haidian Dist. Court. The full text is available at <http://www.chinaiprlaw.com/english/judgements/jmdi.htm>.

<sup>16</sup> See supra notes 10–13 and the accompanying text.

<sup>17</sup> Wang 2001.

The court believed that the two defendant's software, though having different branding and names from Hanwang's products, both originated from Hanwang's software code. Local media report that Hanwang Technology is not content with the low compensation in this judgment, and the company is now preparing for another appeal.<sup>18</sup>

## 16.5 Conclusion and Suggestions

Since China launched major economic reforms in the late 1970s, its economy has experienced tremendous growth. This fact is well known and widely respected in the international community. Much of China's economic reform, as well as much of the economic development resulting from this reform, were in the agricultural and manufacturing sectors of the Chinese economy. The information sector of the Chinese economy, although it has grown in recent years, remains a sector with a far greater potential for growth than has occurred to date.

Intellectual property law can help fulfill China's further aspirations for growth of its economy. As Dr. Lulin Gao has observed, "[t]hrough there is no doubt that many factors contributed to the rapid development of the Chinese economy, the favorable legal situation for intellectual property assumes an ever-increasing importance in stimulating economic development."<sup>19</sup> This is especially true for the information sector of China's economy because markets for information products and services can only thrive when intellectual property rights are secure.

Internet will continue to challenge copyright protection. How to effectively deal with the expected challenges is a common task for China. New technology forced us to choose cooperation rather than conflict. As discussed above, Chinese copyright protection system is a recent legal development in response to China's need to join the international economic community. Despite inadequate enforcement and relatively short copyright protection history, China's government is dedicated to building an efficient copyright protection system.

However, under the annual pressure from the US Special 301 report on the prevalence of IPR infringement in China and the strengths and weaknesses of China's IPR protection and enforcement regimes and more experience acquired in complying with international standard, China will make strides toward more effective copyright protection system. The Internet will not only introduce challenge to us but also create a new opportunity for China and all her trading partners to attain new cooperation in a new era.<sup>20</sup>

---

<sup>18</sup> "China's First Online Software Sales Infringement Case Settled", March 17, 2005, <http://www.chinatechnews.com/index.php?action=show&type=news&id=2461>.

<sup>19</sup> See, e.g., Gao 1998 at135. See also Mansfield 1990 (discussing the relationship between intellectual property rights and economic growth more generally).

<sup>20</sup> For years, China has conducted active exchanges and cooperation with other countries or regions regarding IPR. See *supra* note 12.

## References

- China expects 120 m netizens by year end. 3 Mar 2005. [http://english.people.com.cn/200503/03/eng20050303\\_175348.html](http://english.people.com.cn/200503/03/eng20050303_175348.html).
- “Copyright industry contributes 6 % to GDP”, 29 May 2005. [http://news.xinhuanet.com/english/-05/29/content\\_3016621.htm](http://news.xinhuanet.com/english/-05/29/content_3016621.htm). (Published by “Proceedings of Seventh International Conference on Electronic Commerce—ICEC05: Toward Ubiquitous Business”, August 15-16, 2005, pp.874-879 < ISTEP indexed >).
- Intellectual property protection in China. 29 Mar 2005. <http://jp2.mofcom.gov.cn/article/chinane ws/200503/20050300030740.html>.
- Gao, Lulin. 1998. China’s intellectual property system in progress. In *China in the world trading system: Defining the principles of engagement*, ed. Frederick M. Abbott. The Hague: Kluwer Law International.
- Hays, Thomas, and Zhang Yun. 2002. New amendments to the copyright law of the People’s Republic of China. *European Intellectual Property Review* 24(6): 301–312.
- Liu, Bolin. 2004. On improvement of the Chinese copyright system in the digital network environment. *China Patent and Trademarks* 76(1).
- Mansfield, Edwin. 1990. Intellectual property, technology, and economic growth. In *Intellectual property rights in science, technology, and economic performance: international comparisons*, eds. Francis W Rushing, Carole Ganz Brown. Boulder: Westview Press.
- Samuelson, Pamela. 1998. Intellectual property and economic development: Opportunities for China in the information age. ’98 International symposium on the protection of intellectual property for the 21st Century, 28–30 Oct 1998, in Beijing, PRC.
- USTR. 2002. 2002 National trade estimate report on foreign trade barriers, People’s Republic of China.
- USTR. 2005. 2005 Special 301 report. [http://www.ustr.gov/assets/Document\\_Library/Reports\\_Publications/2005/2005\\_Special\\_301/asset\\_upload\\_file195\\_7636.pdf](http://www.ustr.gov/assets/Document_Library/Reports_Publications/2005/2005_Special_301/asset_upload_file195_7636.pdf).
- Wang, J. 2001. The internet and E-commerce in China: Regulations, Judicial views, and Government Policies. *The Computer and Internet Lawyer* 18(1): 12–30.
- Wen, Dao. 2004. China guarding against software piracy. [http://www.chinadaily.com.cn/english/doc/2004-09/20/content\\_376112.htm](http://www.chinadaily.com.cn/english/doc/2004-09/20/content_376112.htm). 20 Sept 2004.

# Chapter 17

## Copyright Disputes and Resolutions to P2P File-Swapping Application

Yimeei Guo and Ying Luo

**Abstract** Because P2P networks enable unauthorized file-sharing, they are currently a significant source of copyright-infringement concerns. By doing case studies, this article wants to explore and analyze the potential legal liability assumed by different parties involved owing to unauthorized file-swapping in various jurisdictions, mainly in the USA and EU. Then, it puts forward some resolutions to the P2P copyright-infringement disputes. Finally, this article presents its conclusion with the hope to achieve the goal of triple wins of the copyright holders, P2P service providers, and users as well.

**Keywords** P2P · File-swapping · Copyright infringement · Resolutions

### 17.1 Introduction

Peer-to-peer (P2P) networks allow individual computers to share files on the Internet. The original P2P networks were administered by a central server, which managed access to the files available on the network. Users who sent a search request to the central server for a particular file, such as a music or movie track, would receive a list of available files and their location on the P2P network. The user would then download the file directly from one of the individual computers connected to the network.

Current P2P networks, in contrast, operate in a decentralized fashion—that is, without a central server. The software that connects each computer on the network conducts the search-and-retrieval process. When a user searches for a file, the

---

Y. Guo (✉) · Y. Luo

Management Science Department, Xiamen University, Xiamen 361005, China

e-mail: yime\_i\_guo@necmail.xmu.edu.cn



request is transmitted sequentially to individual computers connected to the P2P network. The responses from each computer are then sent to the requester, who receives a list of files and locations available for downloading.

Because P2P networks enable unauthorized file-sharing, they are currently a significant source of copyright-infringement concerns. Eventually, however, P2P technology is expected to make the Internet less vulnerable to disruption and to allow greater efficiency in transferring data and information online—for example, by facilitating collaboration among a company's geographically dispersed workers or by reducing the cost of voice calling.

In contrast, for example, according to Screen Digest, the overall European music market has been in decline—losing 22 % of its total value since 2001. Also, IFPI said overall recorded music sales (physical and digital) fell by 3 % in 2005. The persistence and magnitude of those revenue declines are exceptional in recent history and are regularly attributed to unauthorized file-sharing across P2P systems.

The popularity of music file-swapping shows the ease with which copyrighted material can be obtained and redistributed on the Internet today. The rate of data transfer that the Internet allows currently makes the distribution of movie-length video files much more time-consuming than that of audio files; hence, illicit sharing is less common for video content than for audio files.

Nevertheless, movie and software companies (especially computer-game makers) are increasingly worried that technological advances in digital compression, transmission, and file-sharing will soon lead to piracy of their copyrighted content. According to The Motion Picture Association of America, the number of Web sites offering pirated movies increased from 143,000 in 2002 to approximately 200,000 by the end of 2003. In March 2004, video files accounted for 31.9 % of bytes transmitted over P2P networks, up from 16.4 % in March 2003.

By doing case study, this article wants to explore and analyze the potential legal liability assumed by different parties owing to unauthorized file-swapping in various jurisdictions, mainly in the USA and European Union. Then, it puts forward some resolutions to the P2P copyright disputes such as licensing schemes and digital rights management (DRM). Finally, this article makes its conclusion with the hope to achieve the goal of triple wins of the copyright holders, P2P service providers and users (i.e., consumers) as well.

## **17.2 Legal Action Against Companies Providing P2P Software or P2P File-Sharing Sites**

### ***17.2.1 An Overview***

Initially, lawsuits were brought by record companies against P2P file-sharing sites, i.e., in a legal action against Napster Inc., in 2001, the first centralized MP3 file-sharing network. A US federal court required Napster to exclude unauthorized music files from its directory, where it had centrally coordinated distribution of

music files among users. The court considered Napster to be liable for contributory copyright infringement, because Napster had actual knowledge of infringing file-sharing made possible by its software, and for vicarious copyright infringement because Napster profited financially from the infringement and had the right and ability to supervise and block infringing conduct. Facing the requirement to filter infringing files out of its network, Napster closed its operations in 2001, before reemerging as Napster 2.0, a legal music distribution service.

Similarly, in the case of *Re Aimster*, the US Court of Appeals for the 7th Circuit found the Aimster P2P network liable for contributory infringement, because Aimster had knowledge of the infringing activity. While recognizing that it was possible that the Aimster network could be used for non-infringing uses, the 7th Circuit seemed to find particularly important the fact that the Aimster software tutorial gives as its only examples of file-sharing the sharing of copyrighted music, including copyrighted music that the recording industry had notified Aimster was being infringed by its users.

Copyright holders have also successfully taken legal action against file-trading networks such as Audiogalaxy and Scour, to address unauthorized file-sharing activities. Moreover, a Japanese case was brought by the Japanese Society for Rights of Authors, Composers and Publishers (JASRAC) and 19 record companies against MMO Japan, a P2P network that ran a local version of the "File Rogue" file-sharing software which, like Napster, stored information about its music files on a central server. Other cases have been settled out of court (e.g., the case of iMesh) in 2004. So far, there have been several litigations involving P2P network in China including two guilty judgments against Kuro separately in Taiwan and Mainland China in 2005 and 2006 and a not guilty one for ezPeer in Taiwan in 2005, whereas the Chinese presiding authority has continuously strengthened criminal judicature protection of intellectual property.

In addition, on November 30, 2004, a Brussels Court of First Instance has ruled that Internet provider Tiscali should disconnect customers if they violate copyrights and block the access for all customers to Web sites offering file-sharing programs. The case was instituted by the Belgian Society of Authors, Composers and Publishers (SABAM) on June 24, 2004 with an appeal to consideration 59 of the European Copyright Directive (2001/29/EC).

However, legal actions for copyright infringement have proven more difficult to sustain against decentralized P2P platforms, where shared content is said not to be physically routed via centralized network computers of firms that provide P2P facilities. While Napster provided centralized P2P networks, it was quickly followed by second-generation file-sharing networks such as Gnutella, KaZaA, Morpheus, and Grokster; all designed with a decentralized structure thereby allowing users to connect directly with each other to trade files. While Napster offered a list of files on a centralized server, Gnutella operates via a network of computers that each maintains a separate list of files available on only that computer. Finally, KaZaA utilizes a "Fast Track" technology (also used by Morpheus and Grokster) to operate a super node system, in which a number of computers operate as indexing servers.

In 2002, in a case brought by the author's collecting society BUMA/STEMRA, a Dutch Appeals Court held that KaZaA was not liable for copyright infringement committed by users who used its software to trade unauthorized music files. The Dutch Supreme Court held that makers of file-sharing software KaZaA were not liable for copyright infringement, because the software merely provided the means for accessing copyright protected works. In addition, KaZaA's software was also used for legal purposes, such as sharing works that were authorized or were in the public domain.

### ***17.2.2 Lawsuits Against File-sharing Networks Grokster and Morpheus***

Grokster and StreamCast Networks are companies that freely distribute software that allows users to share computer files with each other. A lawsuit of *MGM Studios v. Grokstel* in 2003 presented the question of whether distributors of P2P file-sharing computer networking software may be held contributorily or vicariously liable for the copyright infringements of its users, thus implying a secondary liability alleging that the P2P systems contribute to and profit from the infringing conduct of their users. The copyright owners argued that Grokster and StreamCast are "turning a blind eye to detectable acts of infringement for the sake of profit which gives rise to liability." The case has raised concerns throughout the technology sector that the Court, in determining the liability of Grokster and Streamcast, would impose overly broad new theories of secondary liability that will result in increased litigation for companies who will be accused of "inducing" infringement by virtue of introducing a new product or service.

The US Court of Appeals for the 9th Circuit rejected the plaintiffs' claims and concluded that the two software companies are not liable for contributory and vicarious copyright infringement. The plaintiffs appealed later on and the US Supreme Court agreed to hear the case. On June 27, 2005, in a 9-to-0 body slam, the US Supreme Court ruled that Grokster et al can be held liable for the use of their software and networks, and remanded the case. Justice David H. Souter wrote for the court: "*We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement.*"

Significantly, the court did not overturn its *Sony Betamax* decision of 1984, which established the principle of technology neutrality. Instead, the Justices focused on the business models and behavior of the P2P developers. "*The record is replete with evidence that from the moment Grokster and StreamCast began to distribute their free software ... each one clearly voiced the objective that recipients use it to download copyrighted works and each took active steps to encourage infringement,*" Souter wrote. The decision in 2005 also noted the "*probable scope of copyright infringement [on P2P networks] is staggering.*" MGM Studios Inc. et al. (2005).

### ***17.2.3 Legal Action Involving ISPs***

As a result of the passage of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), ISPs were granted limitations on their liability in implementing legislation, such as the US Digital Millennium Copyright Act of 1998 (DMCA), the European E-commerce Directive and similar law in Singapore, Japan, Australia, China, and other countries. ISPs' functions such as conduit, transmission, and routing functions, caching, hosting, linking, and information location tools were protected from liability.

The content community has brought several test cases to test the limits of those protections. Several legal actions have been taken by the music industry against ISPs. They involved either the music industry requesting the ISPs to reveal the names of suspected music copyright infringers, or attempt to hold the ISPs liable for tolerating or facilitating P2P traffic, including claims for damages. On the one hand, the content industry contended that ISPs have no intrinsic interest in limiting infringing use and that ISPs induce copyright infringement and boost their broadband subscriber numbers while tolerating or even advertising the possibility of unauthorized file-sharing over P2P networks. On the other hand, ISPs have refuted the latter arguments and pointed to the technological neutrality of their broadband technology (essentially pipes). ISPs have also argued that the identification of file-sharers poses technical difficulties (also because differentiating legal from illegal file-sharing proves to be a challenge) and that enforcement activities impose significant costs on ISPs and potential privacy concerns for Internet users.

These cases, while not always consistent, have demonstrated the limits of ISP liability. In cases where the ISP acts as a "mere conduit" for transmission of digital data over the networks, ISPs have been found not liable for copyright infringement. In some cases, the courts have imposed restraints on the music industry's requests for ISPs to reveal their customers' identities, to facilitate legal actions against individuals for copyright infringement, so as to protect individual privacy and free speech. In other cases, courts have ordered ISPs to provide data, as the providing of customer data for law enforcement purposes is covered by ISPs general contract terms, and as this is covered by the recognition of enforcement interests in any privacy legislation.

In 2004, the Canadian Supreme Court addressed the question of how Canadian artists should be compensated for their copyright in music downloaded in Canada from a foreign country via the Internet. The Court confirmed that ISPs, when acting only as a conduit, and caching for information provided by others, cannot be held liable for copyright infringement. In 1995, the Society of Composers, Authors, and Music Publishers of Canada (SOCAN), asked the Copyright Board to approve a tariff establishing a royalty structure for ISPs. The Court noted that the useful capacity of the Internet to disseminate information should not come at the expense of copyright holders' interests; however, the Court also noted that it was impractical, both technically and economically, for ISPs to monitor the amount of material that passes across their systems.

To the extent that ISPs act as mere conduits, they cannot be held liable for infringements, but in cases where ISPs perform other functions (e.g., acting as content providers, or creating embedded links to copyrighted music from other sources), they may become liable in that respect. As mere intermediaries, the Court ruled that ISPs were not liable to pay royalties to composers and publishers for music that is downloaded or streamed by their customers from file-sharing networks (a tariff of 3.5 % of gross revenues had been proposed). The Court also stated that ISPs are not liable to pay royalties for music content that is stored on their networks. The Court did find that for purposes of Canadian copyright law, Internet communication originating outside Canada could constitute licensable communications to the public covered by Canadian copyright law if there was a “real and substantial” connection with Canada, including if the user was in Canada. In another recent case in Canada, the Court of Appeal has confirmed that consumer copying onto MP3 players is not covered by Canada’s private copying exemption.

The DMCA establishes a scheme that is designed to limit ISP’s liability for copyright infringement, provided they meet certain requirements. It also provides an expedited subpoena procedure that enables applicants to obtain identifying information about users of the Internet, who may operate anonymously and are otherwise difficult to identify through their online activities. In the USA, the music industry made use of these procedures by serving subpoenas on ISPs to obtain details of users alleged to have infringed copyright.

The subpoena process has been examined in a series of legal actions involving the Recording Industry Association of America (RIAA) and Verizon Communications, Inc. (a US network provider). At issue was whether a subpoena attached to no other legal proceedings could be used to obtain information about the identity of customers using the ISP service for infringing copyrights through file-sharing networks. At issue were not only the need for RIAA to obtain users’ identities, but the question of privacy, safety, and due process. Verizon argued that the copyright infringement in question was not covered by the scope of the specific subpoena provision in the DMCA. Verizon also argued that the RIAA demands created serious privacy concerns over how easily a subscriber’s identity could be revealed.

After a District Court rejected Verizon’s interpretation and Verizon appealed, the US Court of Appeals ruled that subpoenas could not be issued against an ISP provider that does not store the copyrighted material on its computer servers. The Court instead required the recording industry to seek the identities of users suspected of illegal file-sharing by filing civil law suits. In October 2004, the US Supreme Court rejected an appeal by the RIAA. RIAA brought the identical test case in *RIAA v. Charter Communications* (03-3802). RIAA sued Charter, a cable company seeking the names and addresses of its subscribers again based on a subpoena. The 8th Circuit Court of Appeals, following the *Verizon* case, rejected the RIAA’s use of this subpoena process and questioned *in dicta* whether the process was constitutional. In *CoStar v. LoopNet*—MPAA and RIAA argued that ISPs can still be found to be direct infringers of copyright when they passively host and

copy materials for their users. The 4th Circuit Court of Appeals affirmed that ISPs are not direct infringers, noting that when a network provider hosts content, it is more like a copy machine than a publisher.

In the case of *Sony Music Entertainment, Inc. v Does 1-40* in 2004, a US District Court held that use of anonymous P2P networks to “download, distribute or make sound recordings available” qualifies as constitutionally protected free speech, but that the protection is subject to copyright owners’ legitimate need to discover who is infringing their works. A subpoena was served on the ISP, Cablevision Systems Corp, to reveal the defendants’ identities, and four of the defendants claimed that the subpoena violated their First Amendment Rights.

However, other cases—like one case by the British Phonographic Industry (BPI) before the High Court of London in 2004—have led to the ISP being asked to hand over customer information in cases of massive copyright infringements (users uploading music on a massive scale).<sup>1</sup>

## 17.3 Some Resolutions to P2P Copyright-Infringement Disputes

### 17.3.1 Legal Solutions

#### 17.3.1.1 A Quick and Inexpensive System for Resolving P2P Copyright Disputes

Indeed, P2P file-sharing poses significant new challenges to the enforcement of copyright law. Copyright owners’ initial response to these challenges—to try to shut down the technologies that facilitate file-sharing—is bad for society. Lemley and Reese (2004) suggested a dispute resolution system might work and proposed a draft amendment to the US Copyright Act to implement the system.

There is, however, an online model in the Uniform Dispute Resolution Policy (UDRP) for Internet domain name trademark disputes, which has resolved over 10,000 domain name trademark disputes in 3 years, at a cost of \$1,200–\$1,500 each and an average resolution time of little more than a month. The UDRP is an alternative dispute resolution (ADR) system that allows trademark owners to bring complaints that a domain name registrant has “in bad-faith” registered and used a domain name identical or confusingly similar to the owner’s trademark. These complaints are considered by expert panelists through accredited private providers of dispute resolution services. The system is designed to resolve only straightforward cases of bad-faith cybersquatting and to reserve for the court system difficult factual and legal disputes between parties with competing and arguably legitimate

---

<sup>1</sup> Copyright and Digital Media in a Post-Napster World Version 2 (Updated January 2005). From <http://cyber.law.harvard.edu/media/files/wp2005.pdf>.

claims to the same domain name. For those straightforward cases of cyber squatting, there are unlikely to be significant factual or legal disputes that need resolving. A panelist given the basic facts can make a decision fairly quickly.

Like the UDRP, a copyright dispute resolution system, if properly conceived, could target straightforward conduct that is unlikely to have legitimate justifications, such as high-volume uploading of copyrighted works to P2P networks. Assertion of a plausible factual or legal dispute—evidence suggesting that the works in question were not copyrighted, or were not copied, or that the use is fair—should result in denial of the copyright owner’s claim without prejudice to her ability to bring a lawsuit where such legal and factual issues can be fully explored Lemley and Reese (2004).

### 17.3.1.2 Licensing Schemes for P2P Networks

Some academic scholars have proposed a range of content licensing schemes and alternative compensation systems that would recompense rights holders for works made available on file-sharing networks. A number of these *alternative compensation mechanisms* have recently been proposed which assume that exclusive rights apply to both uploading and downloading of files, but seek to overcome the difficulties of individual licensing and to establish sustainable business models for music distribution based on either collective licensing, compulsory licensing systems, or a combination thereof.

However, they have to be set against the number of online music stores, which has increased recently (as has the quantity of works available from these outlets). Marketplace solutions rather than collective or compulsory licenses, blanket fees (i.e., non-market pricing) or other interventions in the IPR-related transactions may thus be working. New compulsory licenses for P2P could also be found to interfere with obligations under the major international agreements dealing with copyrights such as the Berne Convention and the WCT (Wunsch-Vincent and Vicker 2005).

### 17.3.2 Digital Rights Management

Effective DRM or electronic copyright management system (ECMS) technologies have been seen as business enablers for the digital distribution of music and for the variety of new business models that consumers may want. Despite their shortcomings, they may be an essential technical tool to protect intellectual property rights and are expected to become pervasive throughout the entire digital distribution chain. Through their ability to protect content, they may encourage the content right holders to make content available for digitization and subsequent digital sale.

Through its ability to create diverse access schemes to content, DRM may enable content offerings that are more tailored to consumer demand (e.g., the right

to purchase time-limited access to songs) and that may—if prices reflect the level of access—increase consumer choice and satisfaction. The European Commission has also stated that the: “*establishment of global and interoperable infrastructure on DRM systems based on consensus among the stakeholders appears to be a necessary corollary to the existing legal framework and a prerequisite for the effective distribution and access to protected content.*”

Several problems still exist in relation to DRM. First, one of the central problems with DRM seems that in the past they have failed to prevent unauthorized uses. DRM programs and technologies must be sufficiently robust to ensure that digital content cannot be subjected to unauthorized copying or unintended uses. Ways of harnessing technology to protect intellectual property are just developing and starting to be effective. To remedy this situation, many governments have through the signing of the WIPO Treaties pledged to create “adequate legal protection and effective legal remedies against the circumvention” of technological protection measures like DRM. These legal protections are likely to be needed so that DRM may operate as intended.

Second, the increasing use of DRM technologies that has raised the concern that the latter could potentially limit usage rights. This topic became a policy consideration notably for consumer associations The European’s Consumers’ Organization, Beuc and was reflected in relevant conferences and consumer surveys in 2005. According to some academics, limits set to private copies could be troublesome when they shift the balance between the interests of copyright holders and the public. But it is fair to say that—as opposed to some CD-Rom copy-protection technologies—so far DRM has rarely been known to prevent legitimate uses of content and services. Still, developers of DRM, players in the market employing DRM, and users of DRM-protected material should be equally concerned to ensure appropriate usage rights, transparency, privacy, as well as ease and reliability of access (Wunsch-Vincent and Vicker 2005).

In sum, some of the challenges posed by P2P can be addressed by judicial and administrative interpretation of existing laws and solved by technological measures, as noted above, including by technical standards worked out voluntarily by the commercial sector. Nevertheless, it may require adjustment to national legislation. National policymakers are always guided by an international framework of copyright treaties, which have expanded in recent decades to keep pace with technology.

## 17.4 Conclusions and Suggestions

Viewing from the above-mentioned legal actions against P2P networks, it seems that there has been no final word about regulating P2P file-sharing services so far. There is much pressure from various parties to make some further changes to copyright laws in respect of P2P services. It may be observed that businesses that are infringing copyright and other laws may find more favorable jurisdictions to place their servers.



The impact of the lawsuits on P2P usage is being debated with some seeing a decline in downloading while others see an increase. Certainly the music industry has affirmed that legal actions against a limited number of file-sharers can significantly reduce music piracy. However, the future is still confused and unknown, but looking back at the history of the media industry, technological innovations have always brought a change in the organization of distribution that in the end favors innovators rather than conservators. The process of change will take time, because it is a struggle between old and new media, but it is very unlikely that Internet users will have to renounce to the new opportunities of file-sharing distribution technologies to obtain content (Numerico and Bowen 2005).

As to technical solutions, although Justin Tygar, professor of University of Berkeley of Computer Science and Information Management, said that technology is the answer to keep users from infringing copyright during the ongoing trial against Sharman Networks for alleged copyright infringement in Australia, he also pointed out that “*the problem of copyright infringement is so pervasive in our society that legal mechanisms alone can never address this.*”

Therefore, apart from those legal and technical solutions discussed afore, it is suggested by this article the copyright holders such as record labels, movie makers negotiate with P2P service providers and make an effort to find a way that would create benefits for both parties and users (i.e., consumers) as well, so as to prevent the rigid legal system from hindering the progress of technological invention and then create the fair and equitable Internet content consuming market.

## References

- Lemley, Mark A., and R. Anthony Reese. 2004. Reducing digital copyright infringement without restricting innovation. *Stanford Law Review* 56: 1345.
- MGM Studios Inc., et al., Petitioners, v. Grokster Inc., et al.* (June 27, 2005). 545 U.S 913, 920.
- Sacha Wunsch-Vincent, Graham Vickery. 2005. *OECD Report on Digital Music: Opportunities and Challenges*, 08 Jun 2005, DSTI/ICCP/IE (2004)12/FINAL.
- Teresa Numerico, Jonathan P. Bowen (July 2005). *Copyright and Promotion: Oxymoron or Opportunity?* EVA 2005 London Conference, 25–29. (Published by “Proceedings of the Sixth Wuhan International Conference on E-Business—Innovation Management Track”, May 26–27, 2007, pp. 2357–2363).

# Chapter 18

## Legal Risks and Solutions to Video-Sharing Web Sites—Focusing on Copyright Infringement

Yimeei Guo, Zhou Yu and Junjie Ji

**Abstract** In recent years, video-sharing Web sites have a rapid development as a new product, but they are shadowed by the problems of law violations and endless litigations. The major problems which video-sharing Web sites encountered are infringement of copyright and privacy and contravention of foreign countries' national dignity and religion. Although the “Safe Harbor” doctrine is the amulet to protect the video-sharing Web sites from copyright-infringement liability, yet there are also some unavoidable legal risks against video-sharing Web sites for some of their broadcasting videos insulted foreign countries' dignity and religion. This article analyzes the legal risks mentioned above and referring to the “Safe Harbor” doctrine in particular to exonerate the copyright-infringement liability of video-sharing Web sites. Finally, this article gives some advices in view of the healthy and sound development of video-sharing Web sites.

**Keywords** Video-sharing web sites · Legal risks · “Safe harbor” doctrine

---

(Published by “Proceedings of the IASTED International Conference on Modeling, Simulation, and Identification (MSI 2009)”, October 1, 2009<EI indexed>)

---

Y. Guo (✉) · Z. Yu · J. Ji

Law Department, Center for Economic Law, Xiamen University, Xiamen 361005, China  
e-mail: yimei\_guo@necmail.xmu.edu.cn

Z. Yu  
e-mail: yuzhou\_0407@sina.com

J. Ji  
e-mail: jijunjie11@126.com

## 18.1 Introduction

### 18.1.1 General Situation of Video-sharing Web sites

As the Internet continues to develop in recent years, various new online entertainment service modes have been created, bringing people much more pleasure than ever. Among them, there are many foreign and domestic popular video-sharing Web sites, which are based on the traditional host–client model; however, they do not provide videos themselves, but provide the netizens with cyberspace. By nature, the videosharing Web sites are the ones with the Web 2.0 (i.e., the second-generation technology) concept. After registering in such Web sites, the netizens can upload any video that they want to share with the others from the Web sites. As long as the size and length of the video uploaded is in line with the Web sites' requirement, any netizens who browse the Web sites can watch these videos for free without registration.

So far, the most famous video-sharing Web site in the world has been YouTube, an American Web site founded in February 2005. Inspired by YouTube's rapid development and successful venture capital's attraction to Google, many YouTube's simulative Chinese video-sharing Web sites emerged starting from 2006, including some well-known ones, e.g., youku.com, tudou.com, and ku6.com, etc. In the very beginning, netizens usually upload the videos screened by them, but today, nearly all kinds of the videos, including movies, TV plays, sport games, and news could be found in the video-sharing Web sites, and the Web sites are just like Web TVs that can broadcast any programs as the netizens wish any time. As a notable performance, tudou.com claims more than 100 million daily unique video views and more than 60 million visitors a month.<sup>1</sup> The video-sharing Web sites are free for all the netizens, so that neither the netizens uploading their videos nor the netizens watching the videos should pay for it. The main source—even the only source of income of the video-sharing Web sites—is advertising, and as the Web sites attract more and more attention from the netizens, the advertising income of the Web sites also increases.

### 18.1.2 Introduction of Major Video-Sharing Web Sites Home and Abroad

#### 18.1.2.1 YouTube

YouTube, founded by Chad Hurley, Steve Chen, and Jawed Karim in February 2005, is an American video-sharing site. At the very beginning, it was used to share video clips among friends, but then it developed and became a space for

---

<sup>1</sup> As leading Chinese video sites Tudou and Youku battle on, more, <http://venturebeat.com/2008/06/24/as-leading-chinese-video-sites-tudou-and-youku-battle-on-more-reasons-emerge-for-56coms-downtime/>.

the netizens to publish their video works. Until 2006, YouTube had had 40 million videos and were visited by 6 million people every day. Fifteen months after it was founded, it had become the Web site visited by most people in the twenty-first century, exceeding its opponents MSN Video and Google Video. In October 2006, YouTube was purchased by Google at the cost of \$1.65 billion dollars. YouTube had tried to develop in the world since 2007, and it had set up Web sites in many countries including Great Britain, France, Italy, Spain, Japan, and so on. According to the statistics from ComScore Corporation, in January 2009, there were more than 100 million Americans who visited YouTube, and the amount of videos watched came to 6.3 billion. Undoubtedly, YouTube is the most influential videos sharing Web sites in the world nowadays.

### **18.1.2.2 Youku.com**

Youku.com, founded by former chairman and CEO of SOHU.com Gu Yongqiang, is the most famous video-sharing site in China. This site, taking “the world is watching” as its logo, started its public beta in June 2006 and began to operate formally in December 2006. Until December 2007, the first anniversary of the site, the times of its videos played every day had surpass 100 million, ranking first in the industry. In April 2009, Gu Yongqiang told the journalist of China Security News that in the first quarter of 2009, the average monthly income of youku.com was more than 10 million. Youku.com is still the largest and most influential video-sharing site in China.

### **18.1.2.3 Tudou.com**

Tudou.com is one of the earliest video-sharing Web sites in China, and it started its public beta as early as April 2005. This site provides with the users unlimited size of personal storage space and independent personal homepage in order to make it easy for the users to upload the videos, besides, it also offer iTudou, a downloading tool to the users, so that they can download the videos in the site easily.

## **18.2 Major Legal Risks of Video-Sharing Web Sites**

For most of the videos in the video-sharing Web sites are uploaded by the netizens, and it is very difficult for the Web sites to do a prior review, some of the videos may violate other people’s rights, then the Web sites are often indicted by the right owners. Currently, the major legal risks for the video-sharing Web sites are copyright and privacy infringement, besides, sometimes the Web sites may be blocked by foreign national authorities for some of their broadcasting videos insulted their dignity or religion.

### 18.2.1 Copyright Infringement

It is the most common problem for video-sharing Web sites, such as YouTube, youku.com, and tudou.com, have been frequently accused by copyright owners. In those cases, the most eye-catching one is *Viacom v. YouTube*.<sup>2</sup> Viacom is a media giant in the USA, and Columbia Broadcasting System (CBS), MTV.com, and Paramount Pictures all belong to it. In March 2007, Viacom indicted YouTube and its parent company Google, claiming that more than 160,000 unauthorized video clips were uploaded to YouTube and they had been watched for 1.5 billion times, but YouTube's strategy was to take no proactive measures to reduce the copyright violations, and their commercial mode was completely based on attracting the netizens through unauthorized videos.

After *Viacom v. YouTube*, more and more copyright owners in the world indict YouTube for copyright infringement. In May 2007, England Premier League, a football association and Bourne, a music publisher submitted their complaint to the court in Manhattan, New York, claiming that YouTube had violated their copyright and benefited from the unauthorized works. In August 2007, eight groups, including National Music Publisher Association (NMPA), the largest music publishing and trade organization in the USA, Rugby football association and football association of Finland took part in this lawsuit, accusing that YouTube had encouraged infringement intentionally. Being faced with so many cases, YouTube even declared that it would establish a reserve of \$200 million dollars to deal with the infringement suits that may arose at any time.<sup>3</sup>

As the copyright owners and publishers in China are gradually aware of their rights, the video-sharing Web sites, which got a smooth development in the last few years, are now confronted with more and more suits. In July 2007, NuBB.com, which was authorized to broadcast the movie "Crazy Stone" in the Internet, prosecuted tudou.com asking ¥ 150,000 yuan compensation for loss, because the netizens uploaded this movie to tudou.com without authorization. This case is well known as "the first case about the copyright dispute of video-sharing Web sites in China." On March 24, 2008, Shanghai NO. 1 Intermediate People's Court judged that tudou.com should remove the infringing movies immediately and compensate ¥ 50,000 yuan.

In August 2007, Hong Kong Television Broadcasts Limited (TVB) decided to prosecute some video-sharing Web sites including tudou.com, for there were unauthorized TVB TV plays broadcasted in these Web sites. In July 2008, Phoenix New Media collected a bulk of evidence which showed that there were massive unauthorized videos which belonged to Phoenix New Media and Phoenix Satellite TV in the video-sharing Web sites including youku.com and ku6.com, and then it prosecuted two of the Web sites in Haidian People's Court.

---

<sup>2</sup> Viacom sues YouTube over copyrights, [http://www.chinadaily.com.cn/world/2007-03/14/content\\_827403.htm](http://www.chinadaily.com.cn/world/2007-03/14/content_827403.htm).

<sup>3</sup> Google reserves \$200 million dollars for YouTube as compensation, <http://it.21cn.com/itnews/qydt/2006/11/16/3035447.shtml>.

Since 2009, the video-sharing Web sites have confronted even more suits. In January 2009, the anti-piracy alliance, which was composed of the copyright owners including joy.cn, Beijing Chunqiu Television, Universe Films Distribution Company, Xiamen Broadcast and TV Group and so on, alleged that it would prosecute tudou.com, for it had broadcasted more than 10 unauthorized TV plays. According to court information from hshfy.sh.cn, tudou.com was faced with 14 suits in February 2009.

Finally, in April 2009, letv.com, the exclusive network copyright owner of TV play “latency,” required that youku.com and tudou.com should remove the unauthorized versions of the play and compensate RMB 60,000 Yuan for loss.<sup>4</sup>

### ***18.2.2 Privacy Infringement***

Video-sharing Web sites may also face the legal risk of privacy Infringement. In 2006, a mobile video up to 3 min appeared in Italian YouTube, which showed that four youngsters were playing a trick on a boy suffering from Down’s syndrome. An Italian rights keeping organization thought that it suspected violation of people’s privacy and protested to YouTube. The video was removed, but four senior management officers of YouTube were accused of crime.

In January 2008, a subway monitoring videotape clips appeared in YouTube, which was screened by subway corporation personnel. This video extended as long as 2 min and 48 s, showing that a couple of lovers were embracing and kissing good-bye at the gate of subway station. The scene was kept cutting over between the long-range view and middle-range view, even the feature articles showing the faces of the two lovers, and the laughter vulgar words from the photographers could also be heard. Three days after this video was uploaded; it had been watched for more than 15,000 times.<sup>5</sup>

### ***18.2.3 Political Risks***

In these years, YouTube has been “interim reviewed” and even blockaded by many countries in the world for there are some videos which offend or insult the countries or their religions in the site. In 2007, a video which displayed that two legs were against the Thailand king, which was considered to be an action of affront to the king in Thailand, so that YouTube had been blockaded for more than 5 months.

---

<sup>4</sup> letv.com sued tudou.com and youku.com for broadcasting the TV play “latency” without authorization, <http://it.sohu.com/20090403/n263192390.shtml> (in Chinese).

<sup>5</sup> YouTube aids Thai video ban. <http://www.encyclopedia.com/doc/1G1-163063245.html>, April 10, 2007.

Finally, YouTube has offered to help Thai authorities block antimonarchist films on the video-sharing service rather than continue with a blanket ban on the whole site.<sup>6</sup>

In January 2008, YouTube was blockaded by Turkey for a video satirizing Mustafa Kemal Atatürk, the founder of this country, and it was impossible for the Turks to visit YouTube directly since then. In April 2008, some videos which were anti-Islamic appeared in YouTube, and the Indonesia government asked the Internet Service Provider (hereinafter ISP) to blockade the site. Though the government agreed to cancel the blockade after the protest from the people, the pages containing the anti-Islamic videos would still be blockaded.<sup>7</sup>

Besides, there are some videos which are contrary to the ethics, which cause adverse effects in the society and reduce the social assessment of video-sharing Web sites. On November 6, 2007, a woman in London was gang-raped by three youngsters, and during the period, some people screened a video up to 3 min and uploaded it to YouTube. Three months later, after the video had been watched for more than 600 times, YouTube removed it after receiving a complaint. On November 7, 2007, a campus gun slinging case took place in a middle school in Finland. A boy student aged 18 killed 8 persons including the schoolmaster and students with a pistol, and then he killed himself. Two weeks before this case, the murderer uploaded a video called “Jokela High School Massacre” in YouTube, clearly implying what he would like to do. After the campus gun slinging case happened, the video was removed, but it had been watched and copied by many netizens.<sup>8</sup>

## 18.3 Solutions to Legal Risks of Video-Sharing Web Sites Focusing on Copyright Infringement

### 18.3.1 Brief Explanation of the “Safe Harbor” Doctrine

Either in theory or in practice, video-sharing Web sites are defined as a kind of ISP. As the Internet service becomes more and more universal, many countries make clear the responsibility of ISP in their copyright laws. Before 1998, ISP was usually required to assume strict liability, which meant that ISP should be responsible for all the content in the space provided to the netizens. This situation was changed after *the Digital Millennium Copyright Act of 1998 (DMCA)* was issued by the USA. *DMCA* modified the article 512 of *US Copyright Law* and limited the infringement liability of ISP, and it provided that ISP should not be responsible for

---

<sup>6</sup> Subway monitoring videotape clips was uploaded, leading to people’s discussion, [http://news.xinhuanet.com/society/2008-01/16/content\\_7431871.htm](http://news.xinhuanet.com/society/2008-01/16/content_7431871.htm) (in Chinese).

<sup>7</sup> Indonesia blocks YouTube to protect Islam film, <http://www.cnn.com/2008/WORLD/asiapcf/04/08/indonesia.youtube/index.html>.

<sup>8</sup> Jokela High School Massacre warning on YouTube, [http://www.shinyshiny.tv/2007/11/jokela\\_high\\_sch.html](http://www.shinyshiny.tv/2007/11/jokela_high_sch.html).

the netizens' act of copyright infringement in some given situation. DMCA divided ISP into four kinds<sup>9</sup>:

- I. Transitory Digital Network Communications,
- II. System Catching,
- III. Information Residing on Systems or Networks at Direction of Users and
- IV. Information Location Tools.

Video-sharing Web sites were classified as an ISP of information residing on systems or networks at direction of users. This article was also called "Safe Harbor" doctrine. According to this doctrine, when a video-sharing Web site just provided the netizens with Web space service but uploaded no video itself, if the videos uploaded by the netizens violated other people's copyright, the site should take no responsibility if it examined and removed the videos in time after it received a notification.

After *DMCA*, most countries adopt "Safe Harbor" doctrine and limit the infringement liability of ISP including video-sharing Web sites. In China, "*Ordinance on the Protection of the Right to Network Dissemination of Information*," issued in May 2006, also adopted such doctrine. Article 14 and article 23 of *the Ordinance* embody the "safe harbor" doctrine. Article 14 provides that "with respect to a network service provider that provides information memory space, or searching or linking services, in case the relevant owner believes that any of the works, performance or audio-visual products as involved in the services has injured his right to network dissemination of information or that his electronic information on right administration has been deleted or altered, he may file a written notice with the relevant network service provider, requesting it to delete his works, performance, and audio-visual products or to cut off the link to the works, performance, and audio-visual products concerned."

Article 23 provides that "where a network service provider provides any searching or linking service to its service objects or cuts off the link to any infringing work, performance, or audio-visual product after receiving a notice from the right owner according to the provisions of the present Ordinance, it is not required to assume the liabilities of compensation. However, when anyone is fully aware or should have known that any of the works, performance, or audio-visual products it has linked to constitutes any infringement, it shall be subject to the liabilities of joint infringement."

The "Safe Harbor" doctrine greatly reduced the infringement responsibility of video-sharing Web sites. Today, either in the USA or in China, after receiving a notification from the copyright owner, the video-sharing site will usually abide by such doctrine and remove the video that is suspected to infringe the copyright. In this situation, even if the copyright owner lodges a complaint, the video-sharing site can win the lawsuit by virtue of the "Safe Harbor" doctrine. In the case of *Ciwen Film v. 56.com*, the court held that though the TV play "family," whose copyright owner was the plaintiff, was uploaded to 56.com by the netizens, the

---

<sup>9</sup> Limitations on liability relating to material online, <http://www4.law.cornell.edu/uscode/17/512.html>.



defendant was an ISP who only provided web space. Besides, the defendant removed all the videos after receiving a notification, so that the defendant should take no responsibility. It is a kind of application of the “safe harbor” doctrine in judicial practice.<sup>10</sup>

### ***18.3.2 The Limitation of “Safe Harbor” Doctrine***

It does not mean that the video-sharing Web sites will take no responsibility in any situation according to the “Safe Harbor” doctrine. First, the video-sharing Web sites should remove the videos that are suspected to infringe the copyright as soon as they receiving the notification, or they will shoulder the infringement liability. In the case of *NuBB.com v. tudou.com*, after finding that there were videos that violate its copyright, NuBB.com sent a letter to tudou.com, asking it to remove the videos, but tudou.com did not response to it in time, so NuBB.com indicted tudou.com in the court. The court held that tudou.com should shoulder the infringement liability and compensate RMB 50,000 yuan for loss.

Second, the video-sharing Web sites will shoulder the infringement liability if they know that the video uploaded are suspected to infringe others’ copyright. In the cases of *members of anti-piracy alliance v. tudou.com* which are being heard, though tudou.com defends itself by virtue of the “safe harbor” doctrine, some experts argue that before making sure that whether tudou.com should be responsible, the court should judge whether or the not tudou.com knew that the videos uploaded violated the copyright of others.

Third, the videos suspected to infringe others’ copyright should come from the netizens. In some video-sharing Web sites, there are not only videos from netizens, but also some videos from the Web sites themselves. In this situation, the Web sites should shoulder the infringement liability.

### ***18.3.3 The Drawbacks of Relying on “Safe Harbor” Doctrine***

There are also some drawbacks for the video-sharing Web sites to response to the infringement suit by virtue of the “Safe Harbor” doctrine. First, the video-sharing Web sites will remove the videos which are suspected to infringe others’ copyright only if they receive notifications from the copyright owners, which lead to that there are always these kinds of videos in the Web sites. The advertisers, who are the major source of profits of the Web sites, will scruple to do business with the

---

<sup>10</sup> 56.com wins in the case of *Ciwen Film v. 56.com*, <http://tech.163.com/09/0326/13/55B85ELR000915BF.html> (in Chinese).

Web sites. The video-sharing Web sites cannot guarantee the quality of the videos uploaded; and some of them violate the copyright and privacy of other people'; some are contrary to the ethics, so that the advertisers will be reluctant to participate. As a result, some video-sharing Web sites have a high clicking rate, but they are not able to make profit from it.

Taking YouTube for example, due to the impact of many infringement suits, in 2008 its advertising revenue of the whole year was only \$200 million dollars, which was much lower than its expectation. Nowadays, many video-sharing Web sites home and abroad have a high clicking rate, but very few of them are profiting. Many Web sites, including YouTube, are still bearing a financial loss, which is a result of the copyright problem of the videos uploaded.

Second, after all, the "safe harbor" doctrine is only a passive way to deal with the copyright problem, and it cannot stop the copyright owners from indicting the video-sharing Web sites. The increasing of the suits will waste a lot of money and time, which is adverse to the development of the Web sites. In February 2009, tudou.com was faced with 14 suits just in a month, which is definitely a waste of massive time.

## 18.4 Conclusion

As some experts have said, it is not a long-term solution for the video-sharing Web sites to be exempt from infringement liability by virtue of the "Safe Harbor" Doctrine. Before *DMCA* was issued in 1998, ISP would take strict responsibility, but then the safe harbor doctrine reduces the liability of ISP and promotes its improvement. With the further development of science and technology, the growth of ISP and the development of management level, the legislation in the future may incline to protect the copyright owners more again, so that the video-sharing Web sites should not keep hiding in the safe harbor, and they should try to resolve the problem of copyright dispute actively.

The suggestions of this article are as follows:

First, video-sharing Web sites should strengthen the review of the videos uploaded actively and remove the infringement videos as soon as possible. Today, most of the video-sharing Web sites, especially the Web sites in China, do not review the videos when they are uploaded, and what they only do is removing the videos when receiving notifications. Though it is legitimate, it hides the danger of being indicted in the future, so that the Web sites should do some active review. YouTube has done something in this field. Now YouTube has used the electronic fingerprint technology to distinguish videos and audios, translating the videos and audios into electronic graphics modes and indentifying whether the files are the same through contrast. Besides, YouTube has proposed a system called Content ID. The copyright owners upload their videos to YouTube to establish a Content ID, and then contrast them with the videos uploaded by the netizens to determine whether the videos are the same.

Second, the video-sharing Web sites can pay for the right to broadcast the videos of the copyright owners. Purchasing the copyright directly is the simplest way to avoid disputes. Take youku.com for example, now youku.com mainly takes four ways to get copyright:

- I. Paying for the copyright;
- II. Guaranteeing the minimum income and sharing the income pro rata with the copyright owners;
- III. Sharing the income pro rata with the copyright owners;
- IV. Resource exchange.

Among these four ways, the proportion of paying for the copyright is up to 70 %.

Third, video-sharing Web sites should cooperate with the copyright owners and seek a win-win model of development. On the one hand, through cooperation with the copyright owners, the video-sharing Web sites can reduce costs and reduce the chance of being indicted. On the other hand, through the cooperation, the copyright owners can improve the popularizing rate of their works, and finally improve their economic benefits. This cooperation mode could be double wins. YouTube has also done something in this field. In 2006, YouTube reached cooperation agreements with some copyright owners such as Universal Music Group and CBS Corp. Through the cooperation, YouTube was allowed to broadcast the programs from the copyright owners for free.<sup>11</sup>

---

<sup>11</sup> YouTube trifecta: CBS, Universal Music, SONY BMG Music deals, <http://blogs.zdnet.com/micro-markets/?p=520>.

# Chapter 19

## “Safe Harbor” Doctrine: A Panacea for Chinese Search Engine’s Copyright Infringement Liability or Not

Yimeei Guo, Zhengzheng Fang and Weiwan Zhang

**Abstract** Thanks to the increasingly progressing of search engines, millions of netizens enjoy free music download without pay. However, for the lack of efficient and effective regulations on this issue, copyright infringements caused by search engine have taken central stage in courtrooms. After “Ordinance on the Protection of the Right to Network Dissemination of Information” promulgated in 2006, “safe harbor” doctrine under US 1998 Digital Millennium Copyright Act (DMCA) was introduced into China and the legal attitude toward copyright protection is going through a great change, which can be clearly seen from the treatment of two significant cases involving Baidu and Yahoo! China. After discussing the copyright infringement of search engines and these two cases, this article explores and analyzes “safe harbor” doctrine of China and its improvement methods. Finally, this article concludes with some suggestions to the development of search engine industry, hopefully to realize a long-time healthy progress and a win-win future.

**Keywords** Search engine · Copyright infringement · “Safe harbor” doctrine

---

Published by “Proceedings of the 1st International Conference on E-Business and E-Government (ICEE2010)”, May 9, 2010 < EI indexed >

---

Y. Guo (✉) · Z. Fang · W. Zhang  
Law Department, Xiamen University, Xiamen 361005, China  
e-mail: ymguo@xmu.edu.cn

Z. Fang  
e-mail: yangse1986@163.com

W. Zhang  
e-mail: luckyall970@hotmail.com

## 19.1 Introduction

Search engine is a kind of network technology and also a program by which one can get a link list of relevant URL addresses in accordance with the content or the key words one inputs to the Internet Explorer. Clicking on the hyperlinks to visit third party Web pages, netizens can obtain the information what they want. During this procedure, search engine uses its indexer such as spider or robot program and sets up a Web database in which it gathers and classifies the information so that clients can easily and quickly get the targeted information.

In 2008, it is reported that over 80 % of information online were taken from search engine service and most of them are for free. Taking the example of MP3 search service by many search engines such as Baidu and Yahoo! China, they provide search results, but ranking and auditioning as well as download service are also included in their service. While great convenience it brings to netizens, it still raises great controversy on copyright infringement.

While pure search engines only provide link service instead of posting the music, it is the third party that should assume major liability, and search engines only constitute indirect infringement especially contributory infringement. This principle has been adopted by most countries and can be seen from cases such as Napster. No case of Norway, *Techno Design BV v BREIN* of Holland, and *Universal Music Group(UMG) Australia v Cooper* in Australia.<sup>1</sup> Therefore, this article will focus on the contributory liability of Chinese search engines when they provide links to illegal MP3 files or Web sites.

## 19.2 Baidu and Yahoo! China's Copyright Infringement Case Study

Here, this article wants to do case study on two Chinese leading cases with similar fact but different outcome shown in Table 19.1 as follows:

In both cases, the premise was the same: Record companies were claiming that search engine providers infringed their music copyright by providing links to download copyrighted music. Nevertheless, the outcomes of these two rulings were completely different.

While analyzing the judgments, the following reasons should be taken into account:

First, "*Ordinance on the Protection of the Right to Network Dissemination of Information*" (hereinafter "*the Ordinance*") came into effect in July 2006 and did not apply in the Baidu case.

---

<sup>1</sup> Cases from IFPI (International Federation of the Phonographic Industry), see <http://www.ifpi.com/>.

**Table 19.1** Baidu and Yahoo! China cases brief

Parties	Fact summary	Court judgment	Key comment
IFPI v. Baidu (2006)	Baidu was sued by 7 int'l record companies through IFPI for uploading and downloading their copyrighted songs on its search engine service	Beijing's 1st Intermediate Court ruled for Baidu on November 17, 2006. Beijing High People's Court rejected IFPI's appeal on December 30, 2007 saying that Baidu's service does not constitute an infringement	Whether or not Baidu's act violated a copyright owner's exclusive right of distribution under Article 10 (6), PRC Copyright Law and Article 8, WCT
IFPI v. Yahoo! China (2007)	Yahoo! China was sued by 11 int'l record companies through IFPI for uploading and downloading their copyrighted songs on its search engine service	Beijing 2nd Intermediate People's Court ruled for IFPI. Yahoo! China should remove their songs search links from its Web site and compensate plaintiffs damages on April 2007. Both parties appealed. Beijing High People's Court rejected the appeals and sustained the original judgments on December 23, 2007	Yahoo! China failed to get exemption from “safe harbor doctrine” appeared the court's changing attitude and indicated that search engine has a long way to develop safely

*Resource* Compiled by Yimei Guo and Zhengzheng Fang (December 18, 2009)

Second, the plaintiff of Yahoo! China case argued for both contributory liability and direct liability, while the plaintiff of Baidu case argued mainly for direct liability, and the argument on direct liability all got rejected.

Third, Baidu was also not contacted regarding the infringing music search links, and as such could not be proved to have known or should have known about the infringing links. While in ‘Yahoo! China’ case, the plaintiff sent “take down” notice and the defendant removed only the URLs provided by the copyright owners, which the court believed to be an “obvious indulgence” of infringement (see footnote 1).

But in general, the reasons for the different rulings are not so obvious or fully convincing. According to the judgments, Baidu was not considered to have the ability to distinguish and control the infringing music search links, while Yahoo! China was considered to be a professional music search Web site, which apparently increased the requirements for Yahoo! China. That is, although China has adopted safe harbor doctrine and made a great progress in legislation. The judges still have considerable discretion such as deciding search engines’ awareness of infringement or not; thus, there are still much to be done so that safe harbor doctrine achieves the desired results in China. For example, the restrictions on the authority of judges and the improvement on the judges’ professional level should be put to the agenda.

## 19.3 “SAFE HARBOR” DOCTRINE OF CHINA

### 19.3.1 *Brief Explanation of the “Safe Harbor” Doctrine*

Before “the Ordinance,” online copyright disputes were ruled by the 2001 China’s Copyright Law and the “*Interpretation by the Supreme People’s Court of Several Issues Relating to Application of Law to Trial of Cases of Dispute over Copyright on Computer Network*” amended and taken effect in 2006, which were obviously not enough to handle the increasingly sophisticated and abundant network copyright disputes. “The Ordinance” not only filled the gap of regulation on this issue, but also brought in “safe harbor” doctrine. According to “the Ordinance,” search engines that qualify for “safe harbor” protection will not be liable for certain illegal activities (such as copyright violations) performed by their customers (Table 19.2).

### 19.3.2 *Comparison Between Safe Harbor Laws in China and the United States*

As can be seen from Article 512 of 1998 DMCA, it sets up complete terms for the application of safe harbor doctrine.<sup>2</sup> In order to qualify for safe harbor protection, a service provider who hosts content must:

---

<sup>2</sup> Frequently Asked Questions (and Answers) about DMCA Safe Harbor , <http://www.chillingeffects.org/dmca512/faq.cgi>.

**Table 19.2** “Safe harbor” Doctrine in USA and China

	Regulations	Content	Major cases
USA	§512 of 1998 DMCA	It separates ISPs into four kinds (search engine belongs to information location tools) and each has the corresponding immunity rules	Arista Records Inc. et al. v MP3 Board (2002); Perfect 10 v Google, Inc., et al. (2006)
China	§§14 and 23 of “ <i>the Ordinance</i> ”	ISPs’ liabilities can be exempted if they cut off links to infringing works or Web sites on receiving right owners’ notice. But those who fully aware or should have known about the infringement are not included	IFPI v Yahoo! China (2007)

*Resource* Compiled by Yimeei Guo and Zhengzheng Fang (December 18, 2009)

- have no knowledge of or financial benefit from the infringing activity on its network;
- have a copyright policy and provide proper notification of that policy to its subscribers; and
- list an agent to deal with copyright complaints.

What is more, ISPs have to demonstrate that they do not know about the infringement and these three conditions should be taken into account:

- does not have actual knowledge that the material or activity is infringing;
- in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
- upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material.

While in China, safe harbor doctrine is made up of two articles of “*the Ordinance*,” Article 14 provides that the copyright owner has the right to file a written notice in case of infringement by ISPs’ searching or linking services. Besides, Article 23 prescribes that ISPs, upon written notice from a complaining party claiming to have rights, disable access to the alleged infringing works, performances, or audio/visual works, will be exempted from contributory liability. But those actually knows or should have known about the infringement are not included.

### 19.3.3 “Safe Harbor” Doctrine and Yahoo! China Case

“Safe harbor” doctrine is established to limit ISPs’ liability on indirect infringement, which shows the encouragement to protect the development of Internet industry. But Yahoo! China failed the case because of this doctrine. Does it mean



the doctrine is a Panacea to handle the problem of Chinese search engine's copyright infringement liability? This article does not agree.

According to "safe harbor" doctrine, search engines are assumed to have no cognitive ability on whether the large number of linked sites are infringing. In other words, search engines have no idea of the infringement by the linked sites under normal circumstances. But if evidence shows that the search engine knows or should have known about the infringement, safe harbor doctrine cannot apply.

Yahoo! China might be deemed to be unknown about the infringement at first, but by the time it received the right owners' notice, it must be aware of the infringement. If it had fulfilled its taking down obligation well, it might be exempted. But it removed only the links pointed out by the plaintiff instead of all the infringing links. Therefore, the court held that Yahoo! China knew or should have known about the infringement, which violated the spirit of "safe harbor" doctrine and thus failed to get protection from Article 23 of "*the Ordinance*."

### ***19.3.4 Improvements on "Safe Harbor" Doctrine of China***

Compared to the comprehensive rules of *DMCA*, this article strongly recommends that "*the Ordinance*" be enriched. First of all, the rules on "notice and taking down" should be supplemented. Specific elements such as the time, format, and method to send the notice should be refined, and the legal consequences of unlawful notice should be provided in order to reduce losses caused by malicious notice. Besides, the rules of counter-notice and put back should be included. As in Article 512 of *DMCA*, if the material of the linked third party has no infringements but got improperly removed because of the notice, the third party involved can file a counter-notice with the search engine provider, who must transmit it to the "right owners" for remediation. If the copyright owner does not bring a lawsuit in district court within 14 days, the service provider is then required to restore the material.

Second, matching requirements should keep up with "the Ordinance." It is of great significance to establish tort liability system of ISPs so as to distinguish different ISPs' direct and indirect infringement liability, and the four different kinds set in *DMCA* can be a good example. Besides, the banning system of intellectual property rights infringement should be set up, not only off-line but also online. Finally, criminal liability should be set as the penal provisions of Australian and Norwegian Copyright Law applied separately in the Cooper and Napster. No case (see footnote 1).

Third, as we previously mentioned, when search engines know or should have known about the infringement, "safe harbor" doctrine does not apply. However, "*the Ordinance*" does not explicitly provide the judging standard on knowing or should have known. Thus, it becomes crucial to fill the gaps of "*the Ordinance*" so that the court may follow easily and take a more consistent standard to make the judgment.

## 19.4 Suggestions for the Infringement Issue of Search Engines

### 19.4.1 Search Engine Providers’ Active Defense

As “safe harbor” doctrine is only a passive means of defense, search engines cannot expect too much on it. The victory of Yahoo! China case brought hope to the recording industry, while Baidu and Yahoo! China were brought to the court again in early 2009. But if search engine providers change their attitude to active defense, the situation would further improve.

For example, Article 90(4) of Taiwan’s newly revised Copyright Law stipulates that ISPs can inform the network users on their infringement online by way of contract, e-mail, automatic monitoring system, or otherwise. Once the violation has accumulated three times, ISPs should terminate of all or part of their service to the violators.<sup>3</sup> In this way, ISPs successfully eliminate the tort liability. And French set up a similar three-strike system this May, provided that copyright violators would first receive an e-mail warning, then a letter, and ultimately lose their Internet access if they were caught a third time.<sup>4</sup> Such active defense will help drive netizens away from pirated music, toward legal download sites.

### 19.4.2 Cooperate and Profit Mode Change

Search engine service is an important profit-making point to Baidu and Yahoo! China, but long-term legal disputes have a great negative impact on its progress for sure. Therefore, it is vital for the search engine industry to reduce operational risks in order to obtain stable development. In the recently ongoing litigation of Baidu, it announced the cooperation with EMI and EMI quashed the indictment. Through this collaboration, Baidu will provide netizens with free and lawful MP3 audition of EMI works and the two sides will share their profit from the advertisement on the Web page (The Beijing News 2009). This cooperation is just a start of the changing, a beginning beneficial to the search engine industry and the recording industry as well as the majority of netizens.

---

<sup>3</sup> Taiwan Revised Regulation and Stipulates the termination on network services when netizens infringe three times (in Chinese ) <http://www.chinaelaw.com/News/2009-04-23/14523.html>.

<sup>4</sup> Mike Sachoff: France Approves Internet Piracy Bill <http://www.webpronews.com/topnews/2009/05/12/france-approves-internet-piracy-bill>.

### ***19.4.3 Strengthening Self-Discipline***

Internet industry and the recording industry should strengthen communication and cooperation, by set up a professional association specifically against linking service's infringement. Such association can develop self-regulatory norms to guide the two sectors' activities, lead the collaboration and negotiation as well as help resolve the disputes. Through these efforts, the confrontation of the two industries can go to an early end and achieve a win-win result.

### ***19.4.4 Propaganda and Education on Netizens***

Propaganda and education can help raise the awareness of netizens so that they will reject illegal or piracy music download and accordingly minimize the market of infringing Web sites. All these will reduce the infringement and alleviate the loss of copyright owners. What is more, only when netizens realize the importance of copyright online can they accept a certain level of pay. This will facilitate the participation of the recording industry for online music profits, reduce risks of search engine service, and also help to legitimize the development of online music, thus allowing netizens to enjoy more legal, high-quality music online.

## **Reference**

Baidu unites with EMI on digitizing corporation and EMI will quash the indictment. From The Beijing News (June 25, 2009) (in Chinese).

## Chapter 20

# “Google Library”: Some Copyright Infringement Concerns in China

Yimeei Guo, Yixuan Liu and Zhou Yu

**Abstract** Digital reading brings more conveniences to our life, but at the same time, it brings more worries to the copyright owners about copyright infringement. Digital reading or sharing the files has to be legal and fair use according to the copyright laws in many jurisdictions including China. Google is a private-owned corporation. This article discusses Google’s plan—Google Book Service (including Google Book Search and Google Library)—and analyzes what the Google Book and Google Library are and their legal controversy in the copyright area and the difference between “Google Book Search” and “Google Library” as well. This article assumes “Google Book Search” and “Google Library” are parts in the entire “Google Book”. In addition to using “the Google Book Settlement” and China’s Copyright Law to solve the controversy, we hope that we can find a better way to balance the right and benefit between users and copyright owners.

**Keywords** Digital reading · Google library · Copyright infringement · Google book settlement

---

Published by “Proceedings of the 1st International Conference on E-Business and E-Government (ICEE2010)”, May 9, 2010 (EI indexed).

---

Y. Guo (✉) · Y. Liu · Z. Yu  
Law Department, Xiamen University, Amoy 361005, China  
e-mail: ymguo@xmu.edu.cn

Y. Liu  
e-mail: 908692963@qq.com

Z. Yu  
e-mail: yuzhou\_0407@sina.com

## 20.1 Introduction

Google began to carry out its “Google Book” plan in 2004, and now its new project “Google Library” causes a big controversy all over the world. Some people believe the “Google Library” will help spreading the culture and acquiring knowledge more quickly, which is a good news for the readers, publishers, and libraries, while the other thinks such new project will infringe the authors and publishers’ copyright seriously and it is a challenge to every country’s copyright laws and regulations. Internet is worldwide, and Google is well known as an “Internet giant,” so that when Google infringes others’ copyright, the region affected may not be the same as the country where copyright owners live. However, this article discusses “Google Book” at first and then analyzes legal controversy. Finally, this article ponders over and presents some solutions based on China’s Copyright Law mainly.

## 20.2 The Advantages and Disadvantages of Digital Reading

### 20.2.1 *The Advantages of Digital Reading*

When everyone can make use of the digital reading, the knowledge will spread more quickly and conveniently. If we have the scanner, we can dispense with large space for books and save the scanned files in our hard disk or CD-ROM. When we have a flash disk with bluetooth, we can send scanned files to our friends or store them in other hard disks, and we are just like a small walking library with personal interest orientation. Another advantage for the readers is that you can see the others’ appraisals or preview some paragraphs in the Web page, and then you can pay for the scanned files and download them. You will understand the book more by reading some paragraphs through the Web site. Of course, the digital reading or sharing the files has to be legal and fair use according to the copyright laws in many jurisdictions including China.

We can bring the e-book reader with us everywhere, which will make our backpack portable, and we can mark the paragraphs we have read easily and find it more quickly. Elders can adjust the script to read easily in e-book reader. When the e-book reader is connected to the Internet, you can refresh your e-book and download what you are interest in. The precondition of digital reading is a digital library with rich book collection, which is the goal of “Google Library.”

For the authors, publishers, and libraries, the digital reading is beneficial. For the publishers, they can sell the scanned files which they publish in the Web site and gain more worldwide readers. Their books can enter the international market at the lowest cost. The publishers could sell traditional books and take the online sale as a channel to add other value in their traditional books.

For the libraries, the digital technology allows them to minify the room for their books storage easily. The readers, who do not live in local, can use Internet to visit their digital library and download the scanned files.

As to the authors, they can interact with their readers by the Web site, surf the download statistics, and rewrite or supplement their works easily, and their readers can renew the scanned files. The digital reading makes the authors, libraries, and publishers earn money more easily.

### ***20.2.2 The Disadvantages of Digital Reading***

When we get the digitized books easily, bookstores may suffer loss for the decrease in their book sale off-line. In the Internet era, the piracy and copyright infringement become more and more severe, and this is the difficulty that the Internet brings. The piracy and copyright infringement has no national boundaries, which would cause jurisdiction problems toward every country. To the culture workers, would you like to be isolated or hope the worldwide readers understand your culture by watching your book? The book is not the same as music, and the book could be translated into different languages and accepted easily. These translators are also the bridge among different cultures.

Because of the convenience brought by digital reading and Internet, the netizens will not pay attention to knowledge. When you download the digitized books easily, you may not review them after reading, because you know you can download them again and again as you wish. You will look down on the authors' work and what they want to express, and the number of people who study from the books may decrease.

In 2005, the US Authors Guild (AG) sued Google for massive copyright infringement and profiting from the full-text copying and indexing of copyrighted content that its crawlers discover online.<sup>1</sup> Moreover, Google also sells ads on the same pages to earn the money, will the income totally belongs to Google or the authors? Something Google has no intention of doing, but it does not explain these questions well.

## **20.3 The Difference Between Google Book Search and Google Library**

These two projects are quite similar. “Google Book Search” helps you search but not download or read books for free. So when you find a book that is still under copyright, you will see only a small portion of the book at a time—either the snippet view or the sample pages view—plus links to places where you can buy or borrow it. If you find a book that is out of copyright, however, we are able to display the full book view.

We can see the search results, which show that the “Google Book Search” has three kinds of policies in copyright:

<sup>1</sup> Google confronted global right maintenance: a suitable opportunity but not a disaster, <http://www.chinaclaw.com/readArticle.asp?id=15696> (Chinese version), visited on 2009-11-9.


1. Full view, it is able to display the full book.
2. Limited view, a book that is still under copyright, so you will see only a small portion of the book at a time and has advertisement.
3. No preview available, the publisher can decide how many pages the readers read and advertisement.

Books Showing: All books

Books Showing: All books



**Pride and prejudice: a novel**  
 by Jane Austen - English fiction - 1853 - 340 pages  
Full view [About this book](#) - [Add to my library](#) - [More editions](#)



**Pride and Prejudice**  
 by Jane Austen - Fiction - 2004 - 316 pages  
 It is a truth universally acknowledged, that a single man in possession of a large fortune, is in want of a wife.  
Limited preview [About this book](#) - [Add to my library](#) - [More editions](#)



**Pride and Prejudice: a novel in three volumes**  
 by Jane Austen - 1813 - 323 pages  
 The author of "Sense and sensibility" = Jane Austen. - Colophon varies. - With box  
Full view [About this book](#) - [Add to my library](#) - [More editions](#)



**Pride and Prejudice: Insight Edition**  
 by Jane Austen - Fiction - 2007 - 360 pages  
 In this new edition of *Pride and Prejudice*, readers will find not only the full novel but **engaging side notes** that offer more background on social customs, ...  
No preview available [About this book](#) - [Add to my library](#) - [More editions](#)

A library is a collection of resources, and services, and the structure in which it is housed; it is organized for use and maintained by a public body, an institution, or a private individual. In the more traditional sense, a library is a collection of books. It can mean the collection, the building or room that houses such a collection, or both. The “library” has itself acquired a secondary meaning: “a collection of useful material for common use. According to the definition “library”, this article assumes “Google library” will provide the netizens with his digitalized books for free finally. This is the difference between “Google Book Search” and “Google Library.” Google is a private-owned corporation, so if we have to pay for “Google Library,” Google will be the last and biggest digitalized bookseller, but not a library.

“Google Library” is a project, which means that the participating libraries agree that Google can scan their collection without the author’s permission. When you click on a search result for a book from the “Google Library,” you will see basic bibliographic information about the book and, in many cases, a few snippets—a few sentences showing your search term in context. If the book is out of copyright, you will be able to view and download the entire book. In all cases, you will see links, which guide you to online bookstores where you can buy the book and libraries where you can borrow it.

The library project’s aim is simple: make it easier for people to find relevant books—especially books they would not find by any other way, for example, those books that are out of print—while carefully respecting authors’ and publishers’ copyrights. The ultimate goal is to cooperate with publishers and libraries to create a comprehensive, searchable, virtual card catalog of all books in all languages and helps users discover new books and publishers discover new readers.

Now, Google has made the “Google Library” agreement with five well-known universities.

With more than 15,000,000 books collection in the library, Harvard University supplied 40,000 public domain books at the project. It may increase the quantity in the future.

Stanford University supplied thousand of public domain books, but the Stanford University may scan all his books collection (total 7,600,000) in the future.

The University of Michigan at Ann Arbor will participate in this project with all of his books collection (total 7,800,000), but some of his collections are copyrighted.

The University of Oxford in England which has 6,500,000 books collection will supply all his books collection that is published before 1990.

The New York Public Library which has 20,000,000 books collection plans to supply 10,000 public domain books and the library.

“Google Publisher” uses opt-in policy, which means that the users participate in Google’s plan at their own will, but “Google Library” uses opt-out policy, which means “Google Library” will include public domain books and copyrighted ones without the authors’ permission in advance.

As we mentioned before, the US Authors Guild (AG) sued Google for the copyrighted books in “Google Library.” The works of those authors that AG cannot contact with are collected in “Google Library”. Google has made a disproportionate control over the digitalized books. But after two years long litigation, both parties acknowledged that such litigation will not only be time consuming, but also failed to the end for them. Hence, they started to negotiate a settlement (See footnote 1).

The other corporation who also want to set a digital library may be obstructed by the huge compensation that Google pays to the copyright owners, and as a result, Google will be the largest and last digital library in the world. This is the reason why Amazon, Apple, and Microsoft fight against “Google Library.” On the other hand, the actual library worries that the scanned files and pricing right will be under the control of Google.

The academia worries that Google will be the last digital library, and then in the future, for example, after 100 years, will the scanned files manager be Google or other else? There will be high risk if all the digital books are controlled by a private-owned corporation.

The legalist worries about privacy, “Google Book Search” can record what pages the readers have visited and their favorite through the option “Add to my library,” so you may not be able to protect your privacy in the last digital library. But the readers will be happy to see that their search will be brought into the marrow in the history of human knowledge when they do their online search.



## 20.4 Google Book Settlement

Google has emphasized that the original privacy policy will extend to its settlement with the publishers; therefore, the copyright registration agency will have no access to their netizens' personal information and Google will also not sell their netizens' reading record. Everyone in the world can use the Google Books (including Google Library) without setting cookie. Google will record the personal information only if the users use the service of Google Books after logging in their Google account.

"The Google Book Settlement" will involve the topic of market competition. Amazon declares that this settlement will not only go against the Competition Law, but also violate the Anti-trust Act, with which Google will monopolize all the digitalized books. The copyrighted authors will have to join this settlement and they have no other choice. The copyright registration will make the book price higher and product lower, which is bad news for the consumers and these authors and publishers who do not participate in this settlement.

Google will set a neutral copyright registration agency to pay infringement compensation to the copyright owners. The users of "Google Book" service can search, preview, and buy the books that are copyrighted but out of print online.<sup>2</sup>

## 20.5 Google Books and Library Legal Analysis

Google now is consulting with many country's authors and publishers on the matter related to authorization. Notably, although Google's Book Settlement is drafted between Google and American copyright owners, yet it is equally applied to Chinese copyright owners. Because according to the "Berne Convention for the Protection of Literary and Artistic Works" with both USA and China as signatories, Chinese citizens' works are protected by US Copyright Act as well.

If you are an author or publisher, when you visit the "Google Book Settlement," you can create an account, read all the notice, and sign the settlement. After you sign the settlement, you will be restricted by the Civil Law and the principle of contract freedom. Unless the settlement is obvious unfair, you shall not violate it.

You can refuse to sign the settlement, so that you will not be included in the settlement, and you will also not receive the benefits conferred by the settlement and you will retain the right to sue Google and the participating libraries.

If you opt out of the settlement, you will not be eligible for a cash payment or to participate in any of the revenue models under the neither settlement, nor

---

<sup>2</sup> Google Book Settlement, [http://www.googlebooksettlement.com/r/home?hl=en&cfe\\_set\\_lang=1,visited](http://www.googlebooksettlement.com/r/home?hl=en&cfe_set_lang=1,visited) on 2009-12-16.

will the settlement’s restrictions or obligations on Google or the participating libraries apply to your books or inserts. If you checked the box on the opting out form requesting that Google not digitize books that you identified, the settlement administrator will pass along your request to Google. Although Google has no obligation under the settlement to comply with such request, Google has advised the settlement administrator that its current policy is to voluntarily honor such requests and refrain from digitizing your books or, if they have already been digitized, refrain from displaying them. By opting out, you will not participate in the settlement and retain all rights against Google and the participating libraries.

When you choose to opt out of the settlement and want to sue, you have to find another defendant—the participating libraries and determine the jurisdiction act—the defendant may not live in your country, because Internet has no national boundaries.

Google negotiates with the library and gets the library’s permission to scan the participating libraries’ book collection. We can reason from the paragraphs above that “Google Library” will be free and full view to every online readers who visit “Google Library”.<sup>3</sup>

According to Article 1, the amended “Interpretation by the Supreme People’s Court of Several Issues Relating to Application of Law to Trial of Cases of Dispute over Copyright on Computer Network” coming into effect on July 1, 2006, a case of dispute over copyright on computer network shall be under the jurisdiction of the people’s court of “the place where an infringing act is committed or where the defendant has his or its domicile.” We assume Google scanned the Chinese authors or publishers’ works and uploaded the digitalize files to his digital library in China, and the participating libraries are also in China.

According to China’s Copyright Law, using the copyrighted work without payment and permission causes infringement. Concretely speaking, Google infringes the author’s duplication right (See Article 9 V)). Besides, Article 24 provides that using the other’s work shall get the author’s permission or contract with the author. For the publisher, Article 35 stipulates that the publisher has the right to permit or inhibit anyone to use the book that it publishes.

When the author gives the publisher his works, the publisher has to make the cover, the illustration, etc., and the author and the publisher have their own copyright, but what Google does is to scan the book and upload the digitalized files, which infringes the author and the publisher’s copyright.

It is noted that one famous author Mien Mien brought a lawsuit against Google on November 6, 2009, asking the court to confirm Google’s infringement, and hold that Google remove the work from the Web site, apologize publicly, and compensate ¥60,000 totally for the economic and mental loss.<sup>4</sup>

---

<sup>3</sup> Google Books Legal Analysis <http://books.google.com/googlebooks/legal.html>, visited on 2009-12-6.

<sup>4</sup> Hua jingyan, Han Han supports Google against the tendency (Chinese version), <http://www.chinaelaw.com/News/2009-11-24/15804.html>.

## 20.6 Fair Use

According to Article 22 of China's Copyright Law, under certain circumstances, the user can use the copyrighted work without the author's permission or contract with the author, but the user should point out the author's name and the work's detail and should not infringe the other copyright according to this law.

Google is a private-owned corporation but not an individual and scan the book completely. The participating library and Google Book Search could declare Article 22(VI): In order to teach at school or do scientific research, the user can translate or copy part copyrighted works for the researcher and teacher, but should not publish or distribute the works. But Google Library digitalizes the whole books, and everyone could download them for free.

The participating library could declare Article 22(VIII): The library, archives, memorial hall museum, and art gallery can copy their collection for exhibiting or preserving, but Google could not. If Google, the trustee, spread the copy files without permission, it will be infringement.

## 20.7 Conclusion

Digital reading brings more and more convenience to our lives, and we are just like a small walking library with personal interest oriented. "Google Library" will save more storage room and economic cost by using digital technology and the worldwide readers can enter "Google Library" to search and read the full text of books for free online. For the libraries, the publishers, and the authors, this project has more good than harm, although the infringement and piracy would be more and more in the digital reading now.

Digital reading in the Internet has no national boundaries, which would cause jurisdiction problems to every country. This is the detriment that the copyright owners worry about, and they hope their government can protect their rights and interests.

Google's plan is good to everyone, and everyone could get knowledge easily through Internet, but it is also harmful. You can read the copyrighted books in limited preview through "Google Book Search" now, and then, you will watch the copyrighted ones in full view in "Google Library" in the future. This is the most important difference between "Google Book Search" and "Google Library."

Notably, Google's plan would infringe the copyright owners seriously; therefore, Google wants to make the settlement with them, but "Google Book Settlement" may not mention the renewed settlement, ad income, or reasonable compensation. You can reverse the settlement and get away for your copyright, but you will be alone without knowledge swap.

Generally speaking, copyright law can protect the copyright owners, but it cannot provide the best solution to them and Google. Chinese government shall

play as an impartial third party and consort with Google and the copyright owners in “Google Book Settlement.” China’s presiding governmental agency, i.e., National Copyright Administration (NCA) and China Written Works Copyright Society (CWWCS), which is the only domestic administration of written works copyrights, can provide better suggestions regarding the crucial reality in China. Google can adjust and amend the settlement in light of these suggestions.

Since Google is a worldwide Internet enterprise, when the authors or publishers want to sign the settlement, NCA and CWWCS shall examine the settlement or inspect it to protect the authors or publishers’ right and benefit. Therefore, to achieve multiple wins in the long run, this article suggests that CWWCS continuously conducts the fair and equitable negotiations with Google and hopes NCA makes its best efforts to push the US government to handle the issue properly.<sup>5</sup>

---

<sup>5</sup> Xie Yu, Google violating copyrights, authors say, [http://www.chinadaily.com.cn/china/2009-10/21/content\\_8822335.htm](http://www.chinadaily.com.cn/china/2009-10/21/content_8822335.htm) .

# Chapter 21

## Chinese Internet Industry's IP Financing: Opportunity and Possibility

Yimeei Guo, Zhengzheng Fang and Xinfeng Zhang

**Abstract** The prominence of Intellectual Property (IP) assets in economic growth and corporate valuation has never been greater. For the technology- and innovation-driven Internet industry, IP financing plays an even more important role on raising funds for both start-ups and expansion. Yet, we are failing to tap into the full potential of IP assets, especially as a financing tool. IP is major assets or even only assets of Internet companies, thus they are missing valuable sources of capital that could be used for business expansion and innovation. Starting from the concept of IP financing, this article then gives a brief introduction to two Internet companies, which can be a sample of Chinese Internet Industry's IP financing. They both have abundant IP assets and successfully got IPO on GEM board in December 2009. After that, this article specifically analyzes the selected patterns for Internet companies' IP financing in China. That is IP pledge, IPO, and VC as well as IP securitization. Studying both the promise and the reality, it finally provides suggestions and solutions to the improvement on the above-mentioned financing patterns, hoping to promote the IP financing of Chinese Internet companies and thus encourage the progress of Internet Industry.

**Keywords** IP financing · Internet industry · Pledge · IPO on GEM · IP securitization

---

Published by "Proceedings of the Ninth Wuhan International Conference on E-Business", May 1, 2010, pp. 97–102 <ISSHP indexed>

---

Y. Guo (✉) · Z. Fang  
Law School, Xiamen University, 361005 Fujian, China  
e-mail: ymguo@xmu.edu.cn

X. Zhang  
IPR Institute, Xiamen University, 361005 Fujian, China

## 21.1 Introduction

Intellectual Property financing (hereinafter IP financing) is the branch of financing that deals with intangible assets such as patents, trademark, and copyright. Like other areas of financing, IP financing is concerned with the interdependence of value, risk, and time. Thus, Internet industry's IP financing refers to the Internet corporations' raising funds through the lever of IP such as patent, trademark, and copyright.

Innovation is a key driver of Internet industry's competitiveness and growth. There have been great improvements on technical innovation of Chinese Internet industry; hence, numerous valuable IP comes out recent years. However, young and innovative Internet corporations in China face bottlenecks when trying to grow up. They are disadvantaged when it comes to attracting external financing if they cannot find equity, since they do not usually have the track record or collateral often required by banks. It has been said that money is the lifeblood of business. Therefore, how to find realistic and feasible means of financing through IP assets becomes even more crucial.

Analyzing relevant laws and regulations as well as rules for financing, the following means should be taken into account: IP pledge, initial public offer (hereinafter IPO) through IP on Growth Enterprises Market (hereinafter GEM) and venture capital (hereinafter VC) backed by IP as well as IP securitization. In the following part, a case study of two Internet corporations' IP financing will be introduced and then the specific analysis of the selected patterns.

## 21.2 Case Study of Xiamen 35.com and Shenzhen Zqgame.com

### 21.2.1 Background of the Two Corporations

Xiamen 35.com Technology Co., Ltd (hereinafter Xiamen 35.com) is a famous internet service provider (ISP) providing domain name registration, enterprises post office, Web hosting, Web site construction, office automation platform (OA), and customer relationship management (CRM), etc., software product and service as well. It was founded in 1996 and holds the following three Web sites: [www.35.com](http://www.35.com), [www.china-channel.com](http://www.china-channel.com), and [www.namenic.cn](http://www.namenic.cn) and has more than 1 million customers. It is called "Alibaba of Fujian province" and finally became Fujian's first enterprise to get IPO on GEM on December 22, 2009 (Shen Tuqingnan 2009).

Shenzhen zqgame.com Network Technology Co., Ltd (hereinafter Shenzhen Zqgame.com) is a professional online game corporation. It was founded in 2003 and holds the following Web site: [www.zqgame.com](http://www.zqgame.com) and completed the joint-stock reform in 2008 and successfully obtained IPO on GEM on December 25, 2009. During the six years, it has contributed a lot on R&D and meanwhile focused on exploring national online game such as "Tian Dao (Natural Law)," "Qing Empire," and "Warring States Period Hero" and thus financed 35 billion Yuan with its 25 % shares through IPO on GEM (Shenzhen 2009).

### ***21.2.2 IP Financing of the Two Corporations***

As can be seen from the prospectuses of the two corporations, IPRs (hereinafter Intellectual Property Rights) are all important components of their assets. That is, Xiamen 35.com has patents composed by 16 core techniques, and the revenues from these techniques have reached 70 % of the company's revenues by June 2009. What is more, it holds 9 trademarks and 25 domain names, while 44 more trademarks are on the application procedure. As for Shenzhen Zqgame.com, 17 software products of online games and engines are its key assets. Meanwhile, trademark on online game "Warring States Period Hero" and 3 domain names are also important aspects of its IP assets.

Because the patent of Xiamen 35.com is leading in domestic China, and Shenzhen Zqgame.com's online game also has a huge market share, this massive amount of IP assets display great opportunity for IP pledge. Furthermore, IP securitization can be a potential discretion, as the scale economy and commercial potential of IP assets has already emerged.

Analyzing the shareholders of the two corporations, we can easily recognize the role of venture capitalists (hereinafter VCs) on raising funds. Among the top ten shareholders of Xiamen 35.com, Shenzhen ZhongKeHongYi Venture Capital Co., Ltd. and Shenzhen Rainbow Venture Capital Group Co., Ltd. are professional venture capital investors, and Xiamen ZhongJinTai Guaranty Co., Ltd. is a financial investor. And for Shenzhen Zqgame.com, there are four venture investors among the eight shareholders, such as Beijing ZhongQingLianChuang Technology Co., Ltd., Shenzhen Innovation and Investment Group Co., Ltd., Shenzhen ZhongZhiHe Technology Co., Ltd., and Shenzhen ZhongKe Merchants Investment Management Co., Ltd.

Finally, the IPO on GEM itself is successful model for financing. For example, Shenzhen Zqgame.com got funds four times as much as its own assets through IPO.

## **21.3 Selected Patterns for Internet Industry's IP Financing**

In view of the tremendous commercial value, it is important for Internet companies to look after IP not only as a legal asset but also as a financial instrument. But as opportunities are always accompanied by huge risks, they should also aim at finding out responding measures to tackle the problems. That is, they need to manage IP assets more actively to identify additional ways of extracting value from such assets. Next, this article will discuss opportunities and possibilities of several major IP financing approaches.

### ***21.3.1 IP Pledge: The Most Important Approach of Chinese Internet Companies' IP Financing***

Among all the possible approaches of Chinese Internet companies' IP financing, loaning through pledge of IP assets is so far the most practical and most widely

used way. In order to acquire bank loans or other debt investment, IP's function of pledge security to leverage loans must be fully realized.

In order to promote IP pledge financing, governments as well as banks have adopted a series of measures to encourage cooperation between banks and IP enterprises. For example, in December 2008, six areas of the country were appointed to be the first IP pledge financing pilot by the State Intellectual Property Office (SIPO), and the Office stated that IP pledge will be expanded to the whole country after the success of the pilot. As another example, *Implementation suggestions on promoting IP pledge financing of the city* issued by Shanghai Municipal Government on August 10, 2009, encourages the collaborations among IP management agencies, financial regulators, banks, enterprises, and rating agencies of intermediary transaction, and by this means, channels and scope of IP financing can be magnified. In addition, Wuhan, Beijing, Chengdu, Guangdong, Chongqing, and other places have all launched the relevant opinions to guide and regulate IP pledge financing.

According to the different ways of risk sharing, IP pledge financing models adopted by the banks at the present time can be separated into three kinds: First, banks themselves bear the risks, while the pledgees register IPR. The credit financing of 65 million Yuan between Jinan JiCheng Electronics Co., Ltd. and Shandong Qilu Bank can be a suitable example to this direct IP pledge (Tian Zhaowu 2009). Second, banks and credit institutions take risks together. That is, IP enterprises get loans from banks, while credit institutions provide credit guarantees based on the IP pledge offered by IP enterprises. Third, banks, assessment agencies, and third-party guarantee institutions shoulder risks separately. For example, when Shanghai Pudong Development Bank offered a 5 million Yuan IP pledge loan to Shanghai YiBao Network Technology Co., Ltd., the banks, assessment agencies, and guarantee institutions, respectively, took the responsibilities at 10, 5, and 85 % of the risk of each loan. What is more, IP assets were pledged to guarantee institutions, thus risks for bank's loaning were decreased via multi-party participation and risk sharing (Zhouli 2009).

Studying the captioned models, the obstacles of IP pledge financing can be concluded into three aspects: the lack of definite and uniform standard for IP collateralized assets valuation, the difficulty to guarantee the stability of the value of IP collateralized assets and the trouble to control risks on IP transaction or financing. Hence, banks cannot accurately determine a market price of an IP collateralized asset and its liquidity. Second, when the technical background of certain technology change, the value of patents and copyrights also change, and it is difficult for banks to perceive such changes sensitively and quickly. Third, the lack of a secure, open, transparent, fair, and efficient IP transaction market leads to the vacuum on market basis for IP value assessment. As a result, assessment institutions may control the assessment on their own interest instead of the basis of the market. Last, because of the diversification of income from IPR, the pledgee cannot control the whole income from IPR in a timely manner so as to guarantee the achievements of the creditor's rights.



### 21.3.2 VC and IPO on GEM: Important Opportunity at Present

Arguably, no market entity has played a more vital role in financially supporting business innovation than VCs who have served to bridge the capital gap between financial markets often hungry only for large proven winners or established enterprises and entrepreneurs who are restrained by their own limited capital resources and unproven track record. The VCs generally infuses both financial support and managerial expertise into businesses that have more potential than physical assets. That is, IP is the most appealing product to VC.

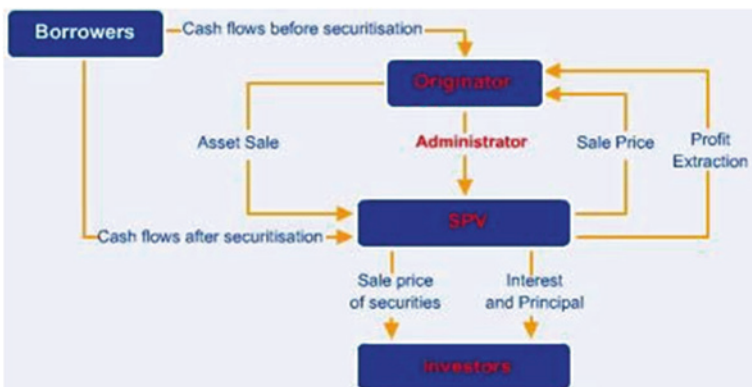
Although China's VC has a history of more than 20 years, yet the absence of GEM constraints its development. This situation will no longer exist because China officially listed on GEM in Shenzhen on October 30, 2009, after released *Interim Measures on Management GEM IPO* in March 2009. It is <3 months since the launch of the GEM, but a number of high-tech enterprises have successfully listed. Just as the two mentioned above, they not only gain funds but also get opportunities for more VCs.

VC and GEM are twins, the establishment of multi-level capital market provides VC with a flexible and direct exit way. Meanwhile, the development of VC in turn constantly promotes the birth of more innovative and promising enterprises, which will foster more excellent listing resources to GEM and the capital markets.

### 21.3.3 The Securitization of IP Assets—A New Trend

Securitization normally refers to the pooling of different financial assets and the issuance of new securities backed by those assets. In principle, these assets can be any claims that have reasonably predictable cash flows, or even future receivables that are exclusive. Thus, securitization is possible for future royalty payments from licensing a patent, trademark or trade secret, or from musical compositions or recording rights of a musician. The following is a flow chart for reference.

Resource: <http://en.wikipedia.org/wiki/Securitisiation>



IP-backed securitization consists of the transfer of IP by an owner to a special purpose investment vehicle (SPV) for securitization and the receipt of capital from investors in the form of a lump sum payment. In 2005, IP innovations estimated that there are about \$1 billion in IP-backed deals each year. This figure is not so exciting, for the universe of buyers and sellers is limited. But if the recent proliferation of Intellectual Property Exchanges on the Internet is an indication, then it is only a matter of time before all concerned will develop greater interest and capacity to use IP assets for financing business start-ups and expansions.

To be attractive to prospective investors, the securitization of IP needs to be based on a diversified portfolio of patents and/or other IP assets. This helps to spread risks and increases transaction size, thereby making investment worthwhile. From the Internet companies' perspective, the problem is that they usually only have a few patents or IP assets. Another complication is that costs are (potentially) higher if it is necessary to defend a large number of patents.

## **21.4 Suggestions and Conclusions**

Though there have been welcome changes and development on IP financing for Internet industry in China, the situation is still far from optimistic. IP owners or the IP-based Internet companies often lack the necessary knowledge about IP protection and management. Investors again find it rather difficult to adequately evaluate IP assets that have not been properly reported. Additionally, a secure, open, transparent, fair, and efficient capital market for intangible assets such as IP assets has not been built yet. Finally, the VC industry and the GEM are not fully developed, while IP securitization meets many obstacles. Based on the analysis of the selected patterns above, this article puts forward many possible approaches to solve current problems.

### ***21.4.1 Comprehensive and Effective Systems on Registration and Publicity of IP***

The registration and publicity of IP and its licensing contract are basic premise for IP financing, because clear ownership on IPR can help reduce the risk of financing and thus promote the transactions and flow of IP assets. But China's current IP registration and publicity system fell far short of the requirements of IP financing.

According to *Chinese Copyright Law*, copyright is granted automatically and no registration or publicity is required. This may result in dilemmas like selling or licensing the same copyright to more than one buyer or licensee. Therefore, the safety of IP exchange cannot be guaranteed, VCs and other investors may stop when considering such risks.

As for patent and trademark, registration and publicity are needed for obtaining corresponding rights, which brings more safety than copyright. But no registration or publicity is required on IP licensing, which may cause trouble to IP financing. IP licensing refers to the transfer of specific rights of IP. The IP owner and the

licensee sign a license contract first and then the licensee gains certain rights of IP at the appointed time and area according to the contract, while the IP owner retains the ownership and receives payment on licensing. Thus, publicity is of great need to protect the safety of licensing transactions. However, relevant regulations by the SIPO only advocate registration and record on patent and copyright for software. As such registration and record have no impact on the effectiveness of the licensing contract, they are not enough to ward off risks. In a word, the lack of a uniform registration institution and the deficiency on the rules for publicity are big obstacles to IP financing in China.

In order to guarantee the effectiveness, transparency, and security of IP assets, it is crucial to establish a sound IPR registration system. Considering the additional burden caused by compulsory registration for all IPRs, this article suggests establishing nonprofit agencies for IPR registration in Beijing, Shanghai, and other cities with urgent financing need. In this way, there can be uniform registration institutions for IP ownership, licensing, and pledge. Meanwhile, a nationally consistent system of sharing and publicity for IP registration information must be set up and the information should be open to the society. Last, compensation for registration error should also be included to guard against the legal risks arising from mistaken registration.

### ***21.4.2 IP Valuation and Market***

Correct evaluation of IP assets can attract external finance. The most prevalently ways of IP assessment can be separated into 4 types:

- Income based—using a multiple of historic profits (but what multiple should be used?) or through an evaluation of the incremental profits earned (e.g., from a branded vs. a generic product);
- Cost based—based on the cost of reproducing the asset, which may be particularly of interest to those who wish to make a similar development;
- Discounted cash flow—future cash flows discounted to the present at a weighted average cost of capital. This requires projections of future income and costs (including IP protection costs), and clear assumptions or data on income (as such, this approach is only appropriate where data is available);
- Transaction based—comparison with similar transactions in the market. The difficulty is that these are few and far between and pricing is often not very visible. With little or no public information, the transaction-based market remains an essentially private one.

This article believes that every evaluation method has its own advantages and disadvantages, and the way in which IP is evaluated is influenced to some extent by the purpose of the evaluation—financial reporting, commercial transactions such as the sale of IP or its use as collateral. Thus, a general standard for IP evaluation combining the advantages of the captioned types should be established for commercial transactions of IP. Furthermore, international accounting

rules should be taken into account so that domestic Internet companies can attract foreign financing too.

For the establishment of IP transaction and financing market, the following factors should be paid attention to. First of all, basic transaction rules and principles should be emphasized. Second, industry self-discipline and government regulation should be effectively integrated so as to resist risks as well as help the progress of IP financing. Meanwhile, relevant intermediary and service organizations should be established in order to promote market integrity. Finally, there should be sound communications and collaborations among IP owners, banks, investors, evaluation institutions, and IP office.

### ***21.4.3 Suggestions to Government and Internet Companies***

First of all, governments need to set an adequate regulatory framework for an IP-based growth strategy. Just as the case of Thailand, Thai banks such as the Thai SME bank are starting to consider IP as collateral after a year of intensive examination several. This will significantly decrease the cost of capital for entrepreneurs. For another example, Indonesia has launched several programs of privately managed public VC funds that seek to promote IP. What is more, governments can do a lot to support IP financing, such as adequate legislation and proper supervision, reasonable policy stimulation and professional guidelines should be included. In other words, guidelines for IP valuation and IP reporting are further actions governments can take to raise overall levels of funding.

As for Internet companies, they should first raise awareness on IP protection, management, and valuation. In this way, they will concentrate more on R&D of IP to constantly get more and more valuable IPRs and use IP as a basis for seeking finance. That is, supercharging R&D through IP planning and then IP mapping the business development strategy and finally gaining financial leverage through IP mining. In this process, IP protection is the foundation and IP management is the key part and IP financing is the ultimate way out. Therefore, enterprises should set up appropriate departments and specialized personnel.

What is more, different financing pattern has different requirements on IP. For example, IP securitization calls for a diversified portfolio of patents and/or other IP assets. Meanwhile, different investors/lenders may value IP assets in different ways and may attach different degrees of importance to IP rights. For instance, owners, long-term investors, and speculators have different investment aims. As the owner/manager of an Internet company, one must therefore take steps to understand the commercial value of different IP assets of the company, ensure their proper evaluation by professionals if needed, and understand the requirements, if any, for their proper accounting in the accounts books and balance sheet. Above all, make sure to include the IP assets of one's company in the business plan when presenting it to potential investors/lenders. Finally, this article suggests that one focus on cooperation with banks and other financial institutions; seize every opportunity and access to finance as possible as he/she can.

## References

- Shen Tuqingnan 35 Corp. was approved IPO in GEM (in Chinese). [http://www.cs.com.cn/cyb/02/200912/t20091223\\_2299672.htm](http://www.cs.com.cn/cyb/02/200912/t20091223_2299672.htm).
- Shenzhen zqgame.com passed smoothly, became 1st stock of online game in GEM (in Chinese). <http://finance.sina.com.cn/stock/cngem/gemipo/20091225/22197157346.shtml>.
- Tian Zhaowu, Wang Guan. 2009. Case study of "JiCheng Electronics Co., Ltd", financial development research (in Chinese), Issue No. 10.
- Zhouli. 2009. Comparison and analysis among typical Chinese IP pledge financing models (in Chinese). Electronics intellectual property, Issue No. 11.

# Chapter 22

## Combating Against Counterfeit: Third Party E-commerce Trade Platform's Liability Analysis

Weiwei Hu and Yimeei Guo

**Abstract** Is the third party e-commerce trade platform operator such as eBay or Taobao liable for IPR infringement when there is counterfeit product sold on the Web site? This article wants to examine relevant legislation and do some case studies abroad and in China. In addition to the conclusive remark on relevant legislation and judicial decision abroad and in China, this article tends to support the healthy development of third party e-commerce trading platforms in China.

**Keywords** E-commerce · Counterfeit · Infringement liability

### 22.1 Introduction

In recent years, while the convenience of online shopping benefits most people, the accompanying intellectual property right (IPR) especially trademark and copyright infringing cases bring headaches to IPR owners. It is increasingly common to find third party e-commerce trade platform which sell forged or counterfeit products of well-known brands or copyrighted works. Usernames or address can be false, and the Internet users are usually disguised by their IP addresses and thus difficult to locate for commencing legal action. In that case, is the third party e-commerce trade platform operator such as eBay or Taobao liable for the infringement?

---

Published by "Proceedings of Int'l Conference on Management and Service Science (MASS 2012), August 1, 2012

---

W. Hu (✉) · Y. Guo  
School of Law, University of Xiamen, Xiamen 361005, China  
e-mail: Helusi420hw@163.com

Y. Guo  
e-mail: ymguo@xmu.edu.cn

This article wants to examine relevant legislation abroad and in China, then do some case studies in European Union, France, German, USA, and China focusing on the courts' inconsistent judicial interpretation over eBay and Taobao for the same conduct, namely allowing counterfeit goods to be sold on their third party e-commerce trade platforms. Finally, in addition to the conclusive remark on relevant legislation and judicial decision abroad and in China, this article tends to support the healthy development of third party e-commerce trading platforms in China.

## **22.2 Relevant Legislation Abroad and in China**

### ***22.2.1 EU Directive on Electronic Commerce***

Paragraph 1, Article 14 of *EU Directive on Electronic Commerce* (2000/31/EC) provides that:

- (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

Article 15 further provides that: "Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."

### ***22.2.2 The French Trust in Digital Economy Act***

France has implemented the E-commerce Directive through the *Trust in Digital Economy Act* (Law No. 2004-575 of June 21, 2004) which has established a separate liability regime, on the one hand, for Internet providers and on the other hand, for hosts. The *Act* categorizes Web site administrator as two kinds: one is the Web site editor, another is the cyberspace provider. The Web site editor is the individual or organization that appears and disseminates the selected, sorted out, and controlled information to the public. The cyberspace provider is the individual or organization that provides storage space but does not participate in issuing information. The Web site editor shall bear complete liability for illegitimate information issued on the Web site, whereas the cyberspace provider normally is not obliged to investigate and review the Web site's information and shall bear liability only when it does not filter the knowing illegitimate information in time. According to the "L'Oréal v. eBay" decision discussed

below, third party e-commerce trading platform providers stated here should belong to the cyberspace provider.

### 22.2.3 *German Multimedia Gesetz*

German passed “*Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikations dienste*” (also called “*Multimedia Gesetz*”) on August 1, 1997. “*Multimedia Gesetz*” classifies Internet service provider (ISP) in accordance with different types and adopts different attribution principle. Third party e-commerce trade platform providers stated here should belong to the hosting service provider under “*Multimedia Gesetz*,” which clearly provides the infringement liability for the hosting service provider, i.e., only when the hosting service provider knows illegitimate content existing on the Web site and should prevent such illegitimate content’s continual use but does not do so under technology permitted circumstance, shall it bear the infringement liability.

### 22.2.4 *The US DMCA*

Title II of the *Digital Millennium Copyright Act (DMCA) of 1998* adds a new section 512 to the US Copyright Act to create four new limitations on liability for copyright infringement by Internet service providers (ISPs), i.e., to establish a “Safe Harbor” system for ISPs. “Safe Harbor” system is applied in the following circumstances:

- The transmission of information must be initiated by user’s instruction. ISPs can only transmit the unreplaced and unmodified material via automatic technology to a subscriber at the user’s direction within reasonable deadline;
- ISPs are not aware of infringing content or behavior existing in system or network;
- Once knowing infringing content or behavior, ISPs immediately remove such content or prohibit access to it;
- When having right and ability to control the infringing activity, ISPs do not receive a financial benefit directly attributable to it;
- ISPs comply with the “Notice-Take down” procedure of *DMCA*.

According to *DMCA*, as to ISPs only provide the function of media, if they do not actively transmit information and are not capable to manage or edit the content of transmitted information, then they shall not assume infringement liability. As to ISPs providing host storage service, once they have already known or receive notice to know the information on its Web site is an infringing one, they must quickly prohibit surfing or downloading such information, otherwise such ISPs shall bear joint and several liability.



### 22.2.5 *China's Ordinance to Protect the Right of Dissemination via Information Network and Tort Liability Law*

In 2006, the State Council, China's Cabinet, issued the *Ordinance to Protect the Right of Dissemination via Information Network*. The *Ordinance* defined the rights of copyright owners in disseminating information using networks, provided a notice and taking down procedure for handling online copyright disputes and afforded limited immunities to Internet service providers (ISPs).

In China, a principle similar to the US Safe Harbor Principle, i.e., Section 512 of **DMCA** as mentioned above (the "Chinese Safe Harbor Principle") is established by Article 23 of the *Ordinance*. Article 23 provides that: "Where a network service provider provides any searching or linking service to its service objects or cuts off the link to any infringing work, performance, or audio-visual product after receiving a notice from the right owner according to the provisions of the present Ordinance, it is not required to assume the liabilities of compensation. However, when anyone is *fully aware* or *should have known* (emphasis added) that any of the works, performance or audio-visual product it has linked to constitutes any infringement, it shall be subject to the liabilities of joint infringement."

Under such principle, an ISP shall be immune from compensation liability if the ISP removes the links to the infringing work, performance, and audio or video products upon receiving the notice from the right owner. China's laws do not contain the US doctrine of "Red Flags." However, the last paragraph of Article 23 of the *Ordinance* provides an exception to the "Notice-to-Remove" procedure, namely, "the ISP shall be liable for contributory infringement if such party has known or should have known the links to the works, performances, or audio-video products are illegal."

But we should pay attention that the captioned Safe Harbor Principle and doctrine of "Red Flags" are mainly enacted by the *Ordinance* which belongs to the *Copyright Law* system. Thus, they cannot be applied to deal with other IPR law such as *Trademark Law*, *Patent Law*, and *Anti-unfair Competition Law* cases. Currently, the law mainly can be applied in e-commerce to definitely protect online IPR other than copyright is Article 36 of *Tort Liability Law* (coming into force on July 1, 2010), which was criticized by some expert as falling far behind the practice in cyberspace (Liu 2011).

Nevertheless, Article 36 of *Tort Liability Law* provides the assumption of liability for the network service provider by "knowing" that a network user is infringing upon a civil right or interest of another person through its network services, and fails to take necessary measures, is also actually originated from the US Safe Harbor Principle of DMCA. Some expert argued that this law relaxed the control of many confused Web sites and contributed to the global development climax of e-commerce (Alamusi 2011).

## 22.3 Selected Relevant Case Studies Abroad and in China

### 22.3.1 *L'Oréal v. eBay*

In response to a reference from the High Court in London on May 22, 2009 [*L'Oréal v eBay* [2009] EWHC 1094 (Ch)], the European Court of Justice (ECJ) has finally on July 12, 2011 provided clarification on the liability of companies operating Internet marketplaces for trademark infringements committed by users and on the specific questions referred to it by Arnold J.

In summary, the Court rules that the duty on eBay and similar entities is much more onerous than was generally thought and that not only any active role but also a negligent failure can be the basis of liability. Further, the ECJ states that national courts must be able to order companies to take measures intended not only to bring to an end infringements of IPRs but also to prevent further infringements of that kind (*L'Oréal v. eBay* 2011).

### 22.3.2 *LVMH v. eBay*

In 2006, Louis Vuitton Moët Hennessy (LVMH) filed a lawsuit against eBay in the Paris Commercial Court (PCC). Although France has statutory protections for online auction sites that merely act as a host for the sale of counterfeit goods, the PCC found against eBay in this matter on June 30, 2008, reasoning that eBay had not taken sufficient measures to prevent transactions involving counterfeit goods on its site.

The PCC held that eBay was acting not just a host, but also as a broker, because eBay received commissions from transactions between sellers and buyers. The PCC also stated that eBay facilitated the selling and marketing of counterfeit products on a large scale through electronic means, and such conduct made eBay responsible for the infringement that occurred on its Web site.

The PCC particularly faulted eBay for its failure to prevent illegal sales, stating, “eBay defaulted its obligation of insuring that its business does not generate any illicit actions like infringement.” In addition to equitable remedies against eBay, LVMH was awarded about 8 million Euros in compensatory damages for eBay’s tortious use of the rights of the owner, 10 million Euros for damage to the image of LVMH, and 1 million Euros in moral damages, totaling almost 20 million euros (*Kangxin Partners* 2009).

### 22.3.3 *Rolex v. eBay*

A court in the German city of Dusseldorf on February 27, 2009, ruled in favor of eBay on the grounds that the company had removed from its site auctions of

counterfeit watches. Court spokesperson Ulrich Egger told Bloomberg, “eBay now uses a filter program to detect offerings that blatantly violate trademark rights. ... Ebay doesn’t have to review each item before it gets posted on its site, because it would jeopardize the whole business model.” (Rolex 2009)

#### **22.3.4 *Tiffany v. eBay***

The main issue in the case was not whether counterfeit Tiffany jewelry can appear on eBay, but rather, who has the burden of policing Tiffany’s trademark in an e-commerce context. The Southern District Court of New York held for eBay, concluding that Tiffany failed to bear its burden of protecting its trademark. The court held that Tiffany must show that eBay had direct control and monitoring over the sale of counterfeit items. The court in *Tiffany* decided that eBay did not infringe Tiffany’s trademark because it did not have sufficient knowledge of specific acts of infringement on its site and it acted appropriately to discontinue an infringing listing when it discovered a counterfeit on its site (Tiffany Inc. v. eBay, Inc. 2008).

The Court of Appeal ruled earlier in 2010 that eBay had fulfilled its duty by removing specific items when instructed to by Tiffany, and that its obligations went no further than that (Tiffany Inc. v. eBay, Inc. 2010). The US Supreme Court has refused to hear an appeal, meaning that the Court of Appeal ruling stands.

#### **22.3.5 *Zhiqiang v. Wong Chao and Taobao***

The Plaintiff is the producer of a video training series called Zhiqiang Club’s Stock Training Course and has registered its copyright over the training series with the Copyright Protection Centre of China. After conducting investigation on Taobao Web site, the Plaintiff discovered that hundreds of unauthorized distributors have been selling pirated copies of its training course through Taobao. While the genuine copies are sold at above RMB10,000, the pirated copies were being sold for RMB5 via Taobao, causing substantial loss to the Plaintiff. An individual named “Wong”—claimed that he has been sourcing the pirated copies from an online store of Taobao. In order to enforce its copyright, the Plaintiff instituted a copyright infringement suit against both Wong and Taobao.

The Court held that Wong had infringed the copyright of the Plaintiff since he knew that the videos sold were pirated copies and he deliberately sold those pirated copies with intent of yielding illegal commercial profits. As to the liability of Taobao, the Court held that there was evidence showing that Taobao had not immediately removed the infringing links upon receipt of the complaints from the Plaintiff or attempted to verify the alleged infringement. As such, Taobao was also liable for the damages suffered by the Plaintiff. Wong was ordered to pay

damages of RMB20,000, and Taobao was held jointly and severally liable for RMB10,000 of such damages (Civil Judgment of Beijing City Haidian District People's Court 2010). This case is currently under appeal at the First Intermediate People's Court.

## 22.4 Conclusion and Suggestion

Generally speaking, common law system countries confirm third party e-commerce trade platform provider's liability mainly according to "indirect infringement" liability system, while continental law system countries confirm third party e-commerce trade platform provider's liability mainly according to "joint infringement" liability system. If we examine the handling of existing cases, the processing idea of China's courts have been similar to the mode of foreign courts but are inconsistent in some recognition of individual problems.

In short, online auction is a newly appearing kind of e-commerce model recently. This model comprehensively involves third party e-commerce trade platform providers, products seller, consumers, and IPR owners' benefit. In China, e-commerce is on the developing stage and more or less exist various kinds of irregular management behavior. When the court deals with the IPR infringement cases in online auction, it should fully consider the benefits of parties in every aspect and when protecting IPR owners' benefit, it should consider China's national circumstance simultaneously to take care of maintaining balance among the benefits of parties in every aspect. Therefore, we must earnestly research and refer to foreign experiences as a foundation, make reference to China's national circumstance and follow China's legislative spirit to deliberately handle well online auction cases. When conditions mature, we must in detail provide the judging standard and exemption condition for third party e-commerce trade platform providers' legal liability in IPR infringement cases in legislation.

Even though in December 2011, the USA kept Alibaba Group's Taobao unit on the US Trade Representative's (USTR) November notorious markets list for offering a wide range of copyright infringing products. We should notify that Taobao is still making continual efforts to fend off piracy. For example, statistics from Taobao show that the company had addressed a total of 62 million items of information regarding trade in rights-infringing goods during the first 11 months of 2011, and 570,000 of its members have been punished. However, such kind of platform should establish and enforce reasonable IPR protection policy and enforcement mechanism to guarantee that after IPR owners' complaints, it can remove the page of related infringing behavior in time or adopt other appropriate solution.

Finally, this article would like to give understanding and support to third party e-commerce trade platform and hope people in every aspect to work hard together to protect online IPR so as to create a more harmonious new business commercial civilized environment.

## References

- Alamusi, 2011. How to Look at the Liability and Obligation of Taobao etc. 3rd Party E-commerce Trade Platform when Combating against Counterfeit, <http://www.chinaclaw.com/blog/more.asp?name=alamusi&id=953>. Accessed 25 Apr 2011.
- Civil Judgment of Beijing City Haidian District People's Court. 2010. Hai Min Chu Zi No. 16148.
- Kangxin Partners PC. 2009. China, World Trademark Review (Feb/Mar 2009) 60.
- L'Oréal v eBay. 2011. ECJ judgment. <http://www.scl.org/site.aspx?i=ne21303>. Accessed 12 July 2011.
- Liu Chunquan. 2011. Analysis on E-commerce platform's IPR protection liability, Chinaipmagazine. Also available at <http://www.chinaipmagazine.com/journal-show.asp?id=1113&pn=2>.
- Rolex, S.A. 2009. I ZR 73/05 (German Fed. S. Ct., Apr. 30, 2008); Rolex v. eBay, OLG Dusseldorf, I-20 U. 204/02 (Feb. 24, 2009).
- Tiffany Inc. v. eBay, Inc. 2008. 2576 F.Supp.2d 463 (S.D.N.Y. 2008).
- Tiffany Inc. v. eBay, Inc. 2010. 600 F.3d 93 (2d Cir. N.Y. 2010).

# Chapter 23

## Digital Music Copyright Protection Dilemma: A Discussion on Draft Amendments of China's Copyright Law

Yimeei Guo and Weiwei Hu

**Abstract** On March 31, 2012, China's National Copyright Administration of the People's Republic of China (NCAC) published the Draft Amendment to the Copyright Law at its Web site to seek public feedback. Some articles in the current Draft Amendments, such as Articles 46 and 48, have attracted the most attention from the public, especially the music industry, because they involve unauthorized use of copyrighted material. Some musician indicated that "the draft clearly favored Internet." This paper wants to discuss those controversial articles under the Draft Amendments and some other solution except legislation for musicians to face digital era with an aim to make a healthy development of digital music sector in China.

**Keywords** Digital music · Copyright · Draft amendments · Solution

### 23.1 Introduction

Consumer choice has been revolutionized, as new models for consuming and accessing music are rolled out in new and existing markets. The number of paying subscribers to services such as Spotify and Deezer has leapt in 2011, from an estimated 8 to more than 13 million. At the same time, cloud-based services, such as iTunes Match, have become a reality in the marketplace, helping drive the popularity of music downloading.

---

Published by "Proceedings of the Twelfth Wuhan International Conference on e-Business <WHICEB 2013>", May 25, 2013, pp. 76–80

---

Y. Guo (✉) · W. Hu  
School of Law, University of Xiamen, Xiamen 361005, China  
e-mail: ymguo@xmu.edu.cn

W. Hu  
e-mail: Helusi420hw@163.com

The truth is that record companies are building a successful digital music business in spite of the environment in which they operate, not because of it. Figures in Digital Music Report (2012) show that more than 1 in 4 Internet users globally regularly access unlicensed sites that contain copyrighted music. This is a startling statistic that captures the challenges we face in developing a sustainable legitimate digital music sector.

We are undoubtedly making important progress in changing this environment, dealing with both peer-to-peer (P2P) and other forms of digital piracy. In the USA, music and film companies have agreed with Internet service providers (hereinafter ISPs) a new copyright alert system. In France, the Hadopi law has been successfully implemented, and research shows it is accepted and having an impact on consumer behavior.

South Korea, a pioneer of anti-piracy legislation which has required an effective role from ISPs in stopping infringement, is seeing continued market health. New Zealand implemented a new graduated response law in 2011, and surveys show it is already affecting consumer behavior positively. In Europe, a series of successful court actions required ISPs to block access to the Pirate Bay, prompting substantial reductions in users of that service (Digital Music Report 2012).

As to China, China's music industry accrued \$82.8 million in total sales in 2011, according to the International Federation of the Phonographic Industry (IFPI). But 76 % of that total revenue came from digital sales. In 2010, more than 70 % of the revenue from China's music companies came from digital music sales, although the IFPI said that 99 % of the music in China was pirated (A record tailspin in Music Industry 2012). In recent years, affected by piracy and the Internet, China's domestic music industry has been declining greatly (Great change in China's Music Industry 2012). Instead of the music creators, the ISPs turned out to be the beneficiaries of the increasing trend of music digitization (CPPCC Deputy 2012).

On March 31, 2012, China's National Copyright Administration of the People's Republic of China (NCAC) published the Draft Amendment to the Copyright Law (hereinafter the "*Draft Amendments*") at its Web site to seek public feedback. Some articles in the current **Draft Amendments**, such as Articles 46 and 48, have attracted the most attention from the public, especially the music industry, because they involve unauthorized use of copyrighted material. Under the **Draft Amendments**, some governmental organizations would be responsible for authorizing use of copyrighted works. Such **Draft Amendments** also have aroused great controversy among famous local songwriters. Among them, Gao Xiaosong, a famous singer-songwriter indicated that "the Draft clearly favored Internet." Meanwhile, many people felt disappointed that Paragraph 1, Article 69, provides that ISPs which provide pure technical services have no examination obligation.<sup>1</sup>

---

<sup>1</sup> Copyright Law providing that one may use music works without authorization was questioned (Chinese version), <http://www.chinamedia360.com/newspage/20120826/3E51BBC3F7194CC0.html>. 5 Apr 2012.

Therefore, this paper wants to discuss those controversial articles under the **Draft Amendments** and some other solution except legislation for musicians to face digital era with an aim to make a healthy development of digital music sector in China.

### 23.2 The Pros and Cons of Digital Music Copyright Protection-Related Draft Amendments of Copyright Law

As mentioned above, on March 31, 2012, the NCAC released the *Draft Amendments* to the Copyright Law and the Brief Explanations on the Draft Amendments (“*Brief Explanations*”) for soliciting public opinions. Unlike the two previous revisions, the **Draft Amendments** proposed by China on its own initiative are homegrown.

The current **Draft Amendments** make significant changes to the Copyright Law both in style and content. The **Draft Amendments** have 8 chapters and 88 articles, while the **Copyright Law** has 6 chapters and 61 articles. The proposed amendments include the following:

1. adding provisions regarding the lease rights of authors and performers and the broadcast rights of performers and phonogram producers;
2. perfecting the systems of technical protection measures and rights management information;
3. putting forward a new category of copyright works for “works of applied art” as well as the “three-step test”;
4. specifying information network transmission rights and broadcast rights;
5. clarifying the ownership of the audiovisual works and the works created in the course of employment;
6. establishing the framework for the measures of administrative mediation of copyright disputes; and
7. improving the infringement compensation standards (i.e., the maximum statutory damages were raised from RMB500,000 to RMB1,000,000 and the infringers who conduct infringing acts repeatedly shall pay a punitive damages of 1–3 times the amount of compensatory damages.<sup>2</sup>

Inter alia, here are two issues under the *Draft Amendments* which will influence the music industry especially digital musicians as well as the Internet industry especially ISPs.

---

<sup>2</sup> Copyright Law of the People’s Republic of China (Revision Draft), <http://www.cpahkld.com/EN/info.aspx?n=4848717495>.



### 23.2.1 *Statutory Licensing*

A statutory license means that a user can, under statutorily defined circumstances, use a work without getting the permission from the copyright owner, provided that remuneration is paid to the right owner. The Copyright Law provides that a statutory license could be applied under five circumstances, such as editing and publishing textbooks, reprinting newspapers and periodicals, producing sound recordings, and broadcasting of radio stations and television stations. The legislative intent of the statutory license is to promote transmission of works. In practice, however, the copyright owner's right to get remuneration could not be guaranteed.

The NCAC believes that the value and function of the statutory copyright licensing are in compliance with China's actual conditions. In the NCAC's view, the failure in practice mainly lies in the deficiency of remuneration payment and legal remedy mechanisms. Therefore, the **Draft Amendments** adjusted and perfected the statutory licensing system from these two perspectives. In particular, the **Draft Amendments** adopt provisions that require users to file records in advance, pay remuneration in time, and clearly indicate the source of work being used. The **Draft Amendments** also provide that the copyright management administration may, on a case-by-case basis, impose administrative penalties on the users who do not perform such obligations in a timely manner.

Article 46 of the **Draft Amendments** provides that, after 3 months from the first publication of a sound recording, other recording producers may use, under the statutory circumstances, the recorded music to make sound recordings without permission from the copyright owner of the music. Music industry representatives strongly opposed this Article, commenting that the period of "3 months" is so short that the production cost could hardly be recovered. Some musician even teased that "Song is just like our kid but after 3 months it will become other people's kid." Famous musician Gao Xiaosong also argued that Article 46 was a route to encourage cyber piracy (Yang 2012). According to critics, this could seriously harm the innovativeness of music production and will directly threaten the survival of record companies, as well as other music transmission media such as radio stations.

However, Article 46 also sets forth some preconditions for a statutory license. According to Article 48 of the *Draft Amendments*, if a user has filed records of the use of the works, indicated the necessary information such as source of the works and paid corresponding remuneration, he/she can use the published works without permission from the copyright owner. The Copyright Law does not aim to protect the interests of a specific group of people but the interests of the copyright owners, the first recording producer, the other recording producers, and the public in order to balance the interests of different parties.

From a historical perspective, a statutory license of recording of musical works was devised with an aim to prevent big record companies from monopolizing the music recording market. Big record companies can, by signing exclusive license agreements with songwriters and composers, obtain the exclusive right to produce

recording products of relevant musical works. By doing so, big record companies will monopolize the music recording market, so as to control the pricing of the products. However, it is worth discussing whether the period of “3 months” as currently proposed in the **Draft Amendments** is reasonable or not.

In order to reach a balance between the interests of the first recording producer and those of other recording producers, the lifecycle of recording products should be fully considered when determining a reasonable period.

### 23.2.2 Network Transmission

There are three paragraphs in Article 69 of the **Draft Amendments**. Paragraph 1 provides that ISPs which provide pure technical services have no examination obligation. Under the **Draft Amendments**, the ISPs would not be obliged to review copyright rights information where they simply provide storage, search, connection, and other technical Internet services to users. In fact, the *Regulations on Protection of Information Network Transmission Right* (the “*Transmission Regulations*”) also provide a similar rule—the “*Safe Harbor*” Rule of technical neutrality or principle of liability for fault—for the sake of balance between the interests of the creators of works and those of the online transmitters. The “*Safe Harbor*” Rule is commonly adopted by many countries in the world to exempt the ISPs from liability for infringement of copyright. The rule that the ISPs bearing fault liability tracks the general principle when determining liability for infringement damages. It is impracticable and technically impossible to request the ISPs to review the contents on the network. Therefore, such provision takes roots from China’s current situation.

Paragraph 2 of Article 69 sets forth the duty of care and removal liability for an ISP in a copyright infringement dispute. An ISP is obliged to delete the infringing contents upon receipt of notification from a copyright owner. If not, the ISP shall bear joint and several liabilities with the network users. Paragraph 3 of Article 69 provides for the ISP’s joint liability where it knows or should have known of the users’ alleged infringements. Such a provision is usually called the “*Red Flag*” Rule. Under the rule, the ISPs are shouldered with a duty of care and shall bear liabilities if they fail to adopt necessary measures to stop the infringement. This provision aims to distinguish the ISP’s misdeeds according to the theory of direct and indirect infringements. If network users conduct direct infringement, the ISP will be jointly and severally liable if it also bears subjective malicious intent to infringe (i.e., it knows or should have known the infringement was conducted by network users).

Opponents hold that the above provisions do little to protect the rights of copyright owners against numerous infringements from the network enterprises. Considering the difficulty of identifying the network user who has conducted infringement, the interests of copyright owners could not be substantially protected under such provisions. However, creativity will be stifled if the copyright

owner's works can be obtained free of charge through the Internet piracy. As discussed above, the Copyright Law aims to balance the interests of various parties, and partial protection for interests of a certain specific group falls far short of the legislative intent (Jiao 2012).

### **23.3 Is There Other Solution Except Legislation for Musicians to Face Digital Era**

What the digital era mainly differentiates with the past days is the occurrence of many open tools, production, marketing, and community. The obtaining cost reduces, and the resource will no longer be grasped by a few people. Musicians may directly contact the audiences and communicate with their fans. As mentioned above, in recent years, affected by piracy and the Internet, China's domestic music industry has been declining greatly. Some popular singers whose albums used to sell millions of copies can now only generate legal sales of several thousands. However, according to the insiders, it is just that the "industrial chain" has changed dramatically. Singers who used to live solely on royalties have now shifted to digging for money from various live performances (see Footnote 1).

In a latest interview of the American veteran artist Neil Young, he mentioned that in the current era, musicians had more spaces and choices than ever and therefore do not just complain the industry. In fact, in Taiwan, there are companies specializing in operating digital publication service. Some musicians have already opened the foreign market. For example, Taiwanese renowned DJ Eddie Hu's works have been recommended by Electronic Music Digital Indicators Platform—Beatport as "10 Deeo-House and Tech-House songs should be listened." The "Revov Records of Echo Album" operated by Hu has sold songs in many global index digital downloading music stores with the digital publication concept and has become the pioneer of Taiwanese brand of dance music as well (Liu 2013).

### **23.4 Conclusion**

In the Internet era, how to protect music's digital copyright is truly a headache for every country. In one aspect, music products in the digital era rely on Internet transmission's characteristic to reduce circulation costs and make the transmissibility of copyright owners' works reach the unprecedented height. But in another aspect, the original copyright protection mechanism is subverted in the present era and the protection mechanism aiming at new copyright characteristics has not kept pace with the times yet. It cannot be denied that Internet has its own rule of game. Comparing with Internet industry, especially ISPs, the party of copyright owners is in a relatively weak position. Both parties do not have equal strength in playing the game. Actually, this is not a "zero-sum game." To introduce the rule of

game which is beneficial to all attending parties by the presiding agency in China as soon as possible is indeed the way to solve the problems.

## References

- A record tailspin in Music Industry. 2012. [http://www.chinaipr.gov.cn/newsarticle/news/photo/201207/1670236\\_2.html](http://www.chinaipr.gov.cn/newsarticle/news/photo/201207/1670236_2.html). Accessed 07 July 2012.
- CPPCC Deputy. 2012. IPR on copyrighted music needed legislative protection. [http://www.chinaipr.gov.cn/newsarticle/news/local/201203/1282829\\_1.html](http://www.chinaipr.gov.cn/newsarticle/news/local/201203/1282829_1.html). 9 Mar 2012.
- Digital Music Report. 2012. <http://www.ifpi.org/content/library/DMR2012.pdf>.
- Great change in China's Music Industry. 2012. [http://www.chinaipr.gov.cn/newsarticle/news/local/201203/1284181\\_1.html](http://www.chinaipr.gov.cn/newsarticle/news/local/201203/1284181_1.html). 15 Mar 2012.
- Jiao, Hongbin. 2012. Key disputable issues regarding the draft amendments to China Copyright Law. <http://www.chinalawinsight.com/2012/06/articles/intellectual-property/key-disputable-issues-regarding-the-draft-amendments-to-china-copyright-law/>. 14 June 2012.
- Yang, Cheng. 2012. Digital music copyright Protection is in a dilemma (Chinese version), [http://zqb.cyol.com/html/2012-05/03/nw.D110000zgqnb\\_20120503\\_1-12.htm](http://zqb.cyol.com/html/2012-05/03/nw.D110000zgqnb_20120503_1-12.htm). 3 May 2012.
- Liu, Weizhi. 2013. New survival for musicians in the digital era (Chinese version). [http://mag.udn.com/mag/digital/storypage.jsp?f\\_ART\\_ID=404817](http://mag.udn.com/mag/digital/storypage.jsp?f_ART_ID=404817), Aug. Jan 2012.

**Part VII**  
**Third Party E-Payment**

# Chapter 24

## Legal Liability of Online Trade Platform Service Providers

Yimeei Guo, Zhengzheng Fang, Zhou Yu and Yixuan Liu

**Abstract** With the constant development of e-commerce and the innovation of Internet technology, a new form of electronic payment system via third party e-payment platform (EPP) shows a remarkable charm. At the same time, third party EPP faces some unsolved problems of the uncertain legal status and legal risks. Besides, there are many detailed but significant issues to be concerned on the development of third party EPP such as the blind competition and the low profitability situation. By doing case study of Alipay, this article wants to analyze common problems and challenges to third party EPP in China, in order to find some resolutions to the long-term healthy development of third party EPP market.

**Keywords** Third party e-payment platform · Legal status and risks · Competitions strategy · Solutions

### 24.1 Introduction

#### 24.1.1 General Introduction to Third Party EPP

Thanks to the increasingly rapid advancement of e-commerce and Internet technology, third party e-payment platform [hereinafter e-payment platform (EPP)] indicates a vigorous development trend in China. According to *the 2008–2009 Annual Report on China's Third-Party Electronic Payment Market*, China's third

---

Published by "Proceedings of the Eighth Wuhan International Conference on e-Business", May 30–31, 2009 <ISTP indexed>

---

Y. Guo (✉) · Z. Fang · Z. Yu · Y. Liu  
Department of Law, Center for Economic Law, Xiamen University, Xiamen 361005, China  
e-mail: yimeei\_guo@necmail.xmu.edu.cn

party EPP market had grown rapidly in 2008, with payment transaction value exceeding RMB 2,500 billion yuan, and it is expected that the 100 %-plus growth can be maintained in 2009.<sup>1</sup>

In general, third party EPP is an independent entity with certain strength and credit protection, it signs contracts with major banks and then provides services of online payment that connects with the banks' payment and clearing systems. It provides direct money transfer services for Internet transactions and works as a bridge between business, customers, and banks. This Web-based new technology has great potential; it offers consumers and businesses great convenience, choices, security, and substantial cost savings. Since its birth in 1999, it has been flourished and up to now, there are more than 50 enterprises providing third party EPP services in China.

According to a report released by Analysis International, in the third quarter of 2008, the market share of those enterprises are as follows: Alipay placed the first with 58.1 % market share, Tenpay was the second with 17.3 % market share, while Chinapay, 99bill, and Yeepay each held 11, 4.4, and 0.9 % market share.<sup>2</sup>

### ***24.1.2 A Background Case Study of Alipay***

Alipay, the largest third party EPP enterprise in China, first appeared as a site [www.alipay.com](http://www.alipay.com) on [www.taobao.com](http://www.taobao.com) in October 2003, and soon became the prevailing payment method of the Taobao registers. After gaining much popularity, it achieved an independent operation and started to show up as the newly Alipay corporation in 2004.<sup>3</sup> Since then, it provided e-payment services to many entities other than Taobao and expanded its business to B2C and C2C market. In the 4th quarter of 2008, its market share expanded to 59 %, while its registers surpassed 100 million, making it the second largest third party EPP in the world, only inferior to PayPal of America (see Footnote 1).

The basic pattern of an online shopping through Alipay is as follows: a customer pays Alipay first and then Alipay informs the business that it has received the payment so that the business can safely send out the goods. When the customer receives the goods, he/she will inform Alipay to transfer the payment to the business, and then a deal is done (see Footnote 3). During this process, Alipay works as an intermediate and separates money paying and collecting from each other. Thus, it becomes a third party guarantee which gives its registers much sense of security when dealing with it. To a large extent, Alipay solves the problems of credit and safety that hinder the development of e-business for years.

---

<sup>1</sup> iResearch 2008–2009 Annual Report on China's Electronic Payment Industry. <http://www.techweb.com.cn/news/2009-01-02/383093.shtml>.

<sup>2</sup> Monitoring report on China's Third-Party Electronic Payment Market of the third quarter 2008. <http://www.analysis.com.cn/>.

<sup>3</sup> Alipay <http://baike.baidu.com/view/26281.htm> (in Chinese).

## 24.2 Legal Problems to Third Party EPP

### 24.2.1 Legal Status of Third Party EPP

In a sense, third party EPP is a new outcome of the “credit lack” in virtual world. For the lag of policies and regulations and the lack of social credit, the third party EPP market is in a rather awkward position. Its service pattern lies on the overlapping “gray areas” of the network operation and the financial service.

In October 2005, Central Bank of China issued “*The Electronic Payment Guideline*” (No. 1) (hereinafter *the Guideline*) in order to afford a legal protection to the improvement of Chinese e-payment environment, and in 2006, the draft of “*The Payment Liquidation Organization Administration Measure*” (hereinafter “*the Measure*”) was promulgated, but it has not been passed so far. Both *the Measure* and *Guideline* only regulate behaviors of banks offering Internet banking services, and thus the effect is limited to direct payments via Internet banking only. No mention was made to payment by third party EPP, despite the fact that it has been playing an increasingly prominent role in this field.

As for the supervision agencies, as there are no relevant rules, the CBRC, Ministry of Commerce (MOFCOM), State Administration of Industry and Commerce (SAIC), and Ministry of Information Industry and Information Technology (MIIT) can be the possible supervision agencies. Regulatory vacuum and multiple regulations in this field frequently occur.

### 24.2.2 Major Legal Challenges and Risks

- Usage and Safety of Users’ Money

The operation model of third party EPP determines that everyday huge amounts of money stay in third party EPP’s accounts. Payment transferred by a buyer before being paid to the seller will be “deposited” in third party EPP for as short as hours and as long as days; the seller may also leave money in his/her third party EPP account. Rumor has it that the daily transaction volume via Alipay has exceeded RMB 61 million Yuan. The scale of “deposits” with Alipay is thus imaginable.

In the USA, third party EPP such as ebay has to obtain a money transmitter license from each state government to operate within that state. In China, however, third party EPP is not required to obtain a license to run their business, which leaves the door wide open for abuse. Moreover, what would happen to users’ money if third party EPP goes bankrupt? No regulation is in place to effectively provide for returning users’ money as provided for in case of insolvency of banks and other financial institutions.

- Legal risks such as money laundering and illegal cash in

While third party EPP brings us much convenience and progress; it also causes much legal risks such as money laundering and obtaining cash by illegal purchase online



For example, offenders can make pseudo transactions by third party EPP, acting as both the seller and the buyer. Although the purchase price payment is done online, the delivery of purchased goods goes offline and is only between the seller and the buyer. Therefore, third party EPP cannot be alerted to a pseudo transaction and must act upon instructions to pay.

Through this way, the offenders easily transfer their illegal income into their third party EPP accounts, so that the illegal income successfully becomes legal. What similar is, many law violators do arbitrage by false transactions via third party EPP.

## **24.3 Problems on Competition and Profitability**

### ***24.3.1 Fierce and Blind Competition***

First of all, third party EPP faces blind competition from competitors of its own industry. Over 50 third party EPP enterprises appeared within these few years, fighting to seize the market through price war, making the original “Money King” industry unprofitable rapidly. Besides, major banks such as Industrial and Commercial Bank of China and China Construction Bank also joined the competition, while 15 foreign banks were authorized for online bank services in China (Chen 2008).

What is more, major third party EPP enterprises such as Alipay and Tenpay all started to charge since 2007. The charging trend also means that the phase of seizing market regardless of profit is over, a new round of competition focusing on innovation and service quality as well as profitability is being staged.

### ***24.3.2 High Cost and Low Profit***

The input of third party EPP enterprises includes many aspects such as the cost on the safety of the platform, the platform handling, and the exploitation to meet the customers’ diversified needs as well as the market development and promotion, and it is estimated that the expensive cost is still in a great expansion tendency.

The high cost calls for much money, which sets a higher request to the market profitability. However, the status of third party EPP enterprises is far beyond optimistic. When the third party EPP industry just started in 2000, the profit share of the merchant customers and third party EPP enterprises were approximately between 1 and 2 % (Chen 2008). But after these years heated competition, there is almost no one in profit among the over 50 third party EPP companies in China nowadays.

## 24.4 Suggestions and Conclusions

### 24.4.1 *Strengthening the Profession Autonomy, Releasing Self-discipline Norms*

For the legal vacuum on third party EPP, self-discipline may have more practical significance. Thus, a professional industry association composing by leaders of major third party EPP enterprises, experts, and academics as well as representatives of relevant government departments and consumers should be set up.

Meanwhile, the association can formulate statute for third party EPP industry, guiding on those important issues such as how to guard against money laundering and illegal cash in, how to avoid misuse of the clients' money and whether to pay interest or collect earnest money.

### 24.4.2 *Responding to the Supervision Actively*

Central Bank of China sets about granting professional licenses to related companies while *the captioned Measure* is going to release. These two major events put forward higher request to third party EPP.

For specific enterprises such as Alipay, they can increase the scale through integration and acquisition, absorption venture capital from multi-channel approaches and so on to meet the market access requirements stipulated by Central Bank. After the official releasing of *the Measure*, third party EPP enterprises will have definite legal status and may explore in more domains. For those enterprises who fail to obtain the license, they can change to do the customer data analysis, resources investigation, and other consulting services.

### 24.4.3 *Gaining “Economies of Scale” Through Corporation*

The “economies of scale” effect is so obvious in the development of third party EPP that gathering huge amount of customers is of great significance. Therefore, the innovation on technology and service, the construction of a security, good faith e-payment platform, and providing high-quality service for customers and businesses become crucial to the survival of third party EPP enterprises.

In this sense, third party EPP enterprises such as Alipay should vigorously promote the cooperation with financial institutions and establish cooperative relations with the numerous banks. At the same time, they should also build up a good working relationship with the physical distribution, communication, and other related agencies in order to provide the users with diverse terminal product and service.

#### ***24.4.4 Segmentation of Third Party EPP Market***

The market mobility and the intense competition request third party EPP enterprises to accurately locate themselves according to their own advantages, and then make effective segmentation of the market so that they can provide the corresponding product and service.

There are different segmentation forms by different classification; here are the three major segmentations. First is the geographical segmentation. Subdividing the market through geographic view can ease the regional blind competition and in certain extent bring third party EPP enterprises more room for profit. The second is the industry segmentation. Different industries have different e-payment demands; new markets can be cultivated through depth research on the different demands of different industries. So far, third party EPP has already had a wide application in online-game, travel tickets, education, etc. And the last is the e-commerce pattern segmentation. Basically, there are three patterns of e-commerce: B2B, B2C, and C2C pattern. Alipay's starting from the C2C market and expansion to B2C and B2B market can be a suitable example (see Footnote 3).

#### ***24.4.5 Other Suggestions on the Development of Third Party EPP***

- **Value-added services**

For third party EPP companies, how to expand value-added services should be the key to their profit growth. They can innovate services according to the transaction demand and find new profit point. For instance, they can provide good faith service based on their credit and fame.

- **Price strategy—Differential pricing to increase revenue**

Though third party EPP is on the march of charging, it cannot charge its customers too much. This article suggests a differential pricing strategy, i.e., keeping free to the large amount of ordinary users and charging on the businesses that have reached a certain transaction volume or that make deals on some certain products. Be sure that each price level must be acceptable to the users. What is more, incentive measure is also a must to encourage the customers.

- **Vigorous promotion on localization services**

The expansion of local services is not only the profit need, but also the important aspects of third party EPP enterprises' culture and fame. Meanwhile, third party EPP can also be expanded to domains outside e-commerce. For instance, there can be application room for third party EPP on local services such as local e-government, local public utilities payment—such as water, electricity, gas, and cable TV

charge—local culture, and education payment—such as network education and test training—as well as local tourism payment such as travel tickets, line costs, travel products, hotel reservations, and e-tickets.

## Reference

Chen, Xiaosheng. 2008. Third-party payment platform for overseas expansion into E-commerce, business tool. *Journal of Hebei Legal Science* (in Chinese).