E-COMMERCE LAW AND THE PROSPECTS FOR UNIFORM E-COMMERCE RULES ON THE PRIVACY AND SECURITY OF ELECTRONIC COMMUNICATIONS

Naoshi Takasugi*

TABLE OF CONTENTS

I. INTRODUCTION

Along with the development of information technology, electronic commerce (EC) has been increasing in number, quantity, and scale. As parties to EC are often not conscious of national borders, cross-border transactions are very common nowadays even in business-to-consumer (B-C) EC transactions.

According to a report by the Japanese Government,[1] in the year 2013 Japanese consumers made purchases amounting to $1.6 billion USD from China or the United States through the Internet. U.S. consumers purchased $6 billion USD in goods from China or Japan, and Chinese consumers purchased $6.7 billion USD in goods from Japan and the United States, respectively.[2] China is the biggest EC market among those three nations. It is expected that the scale of cross-border EC among those three nations will account for up to $34 billion USD in the year 2020.[3]

For the steady growth of EC in B-C transactions, to build consumer confidence is indispensable. For this purpose, it seems necessary to secure transparency and predictability in applicable law and to establish the effective dispute resolution systems.

---

* Professor of Law, Doshisha University in Kyoto, Japan. He teaches Private International Law (i.e. conflict of laws), International Business Law, and International Civil Procedure Law.

1 *Results of the E-Commerce Market Survey Compiled*, MINISTRY OF ECON., TRADE AND INDUS. (Aug. 2014), http://www.meti.go.jp/english/press/2014/0826_01.html.

2 *Id.*

3 *Id*.

As far as business-to-business (B-B) transactions are concerned, those goals, such as predictability of law and effective resolution systems, have already been attained to some extent. In addition to uniform laws for international contracts, such as the United Nations Convention on Contracts for the International Sale of Goods (CISG), we have some international instruments addressed to EC peculiarity, such as the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce or Model Law on Electronic Signatures. Besides, parties can generally select the applicable law to their transactions and the forum where their dispute shall be resolved.

On the other hand, B-C transactions are not covered with those international instruments. Each nation seeking to build consumer confidence in EC has developed various systems for effective consumer protection that limit the misleading, or unfair, commercial conduct online and maintain the consumer's privacy and security in cyber space.

Existing systems on B-C EC are inevitably different from nation to nation, and they are not always adequate to address the emerging problem of cross-border EC. At this point, comparative research is necessary for both the best and uniform solutions.

This Article briefly reviews the Japanese rules and systems to provide "raw material" for comparative studies. It focuses on some EC rules of privacy (Part II) and those of security (Part III), based on the *Interpretative Guidelines on E-Commerce* published by the Ministry of Economy, Trade and Industry (METI) in Japan.[4]

II. E-COMMERCE RULES ON PRIVACY IN JAPAN

In Internet businesses such as Internet trading, information retrieval sites, and mail magazines, users often input their personal information without being aware that business operators often store and use this information for marketing purposes.

In Japan, the Act on the Protection of Personal Information[5] prescribes the duties to be observed by business operators handling personal information.

---

[4] *Interpretative Guidelines on Electronic Commerce and Information Property Trading*, MINISTRY OF ECON., TRADE & INDUS. (2014) [hereinafter *Interpretative Guidelines*] (explaining how the relevant laws and regulations are applied and interpreted with respect to various types of legal problems in the field of e-commerce and to promote facilitation of transactions by enhancing predictability for the parties involved). This guideline was revised in 2015, but the 2015 revisions have no material effect on my analysis below.

[5] Kojinjōhōnohogonikansuruhōritsu [Act on the Protection of Personal Information], Law No. 57 of 2003, *translated in* (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/law/detail/?id=130&vm=04&re=02 (Japan). (The unofficial English texts are provided by http://www.japaneselawtranslation.go.jp/.).

Article 15(1) of the Act provides that, "when handling personal information, a business operator handling personal information shall specify the purpose of utilization of personal information (hereinafter referred to as "Purpose of Utilization") as much as possible."[6] Article 18(1) of the Act reads that "when having acquired personal information, a business operator handling personal information shall, except in cases in which the Purpose of Utilization has already been publicly announced, promptly notify the person of the Purpose of Utilization or publicly announce the Purpose of Utilization."[7]

Under the provisions of this Act, where certain personal information is acquired via the Internet and where such personal information (e.g., website browsing history) is collected in a form that particular individuals cannot be identified, the business operator is not obligated to notify the person of the Purpose of Utilization.[8] However, if the business operator scans the information against identifying information registered when the users subscribed for a membership, the business operator must notify the individual of the Purpose of Utilization.[9] If the business operator collects personal information for marketing purposes without notifying them, it might be illegal due to non-compliance with Article 18.[10]

Furthermore, Article 17 of the Act provides that "a business operator handling personal information shall not acquire personal information by a deception or other wrongful means."[11] The following four cases may fall under the definition of "wrongful means."

The first case is concerning the acquisition of personal information by falsifying the intention or purpose of such acquisition. This case is clearly an acquisition of personal information by "deception." Therefore, it is no doubt considered illegal.[12]

The second case is about the acquisition of personal information from the targeted person while concealing the fact of such acquisition. For example, when a product is sold and delivered to the consumer with an integrated circuit (IC) tag that can perceive information from remote places, business operator(s) may obtain personal information of the purchaser. This case also may be considered highly illegal.[13]

The third case involves the acquisition of personal information through the information retrieval site. For example, if the business operator of an information retrieval site acquires individual users' log information, such as a history of search conditions in a form where particular individuals can be

---

6 *Id*. art. 15(1).

7 *Id*. art. 18(1).

8 *See* Act on the Protection of Personal Information, Law No. 57 of 2003, art. 2(1); *Interpretative Guidelines*, *supra* note 4, at ii.62.

9 *Interpretative Guidelines*, *supra* note 4, at ii.62.

10 *Id.*

11 Act on the Protection of Personal Information, arts. 15(1), 18(1).

12 *Interpretative Guidelines*, *supra* note 4, at ii.62.

13 *Id.* at ii.64.

identified, and the operator does not disclose the fact of such acquisition to the users, such acquisition of personal information might be considered illegal.[14]

The fourth case pertains to the acquisition of personal information via spyware programs. Some programs designed to acquire certain personal information (spyware) are incorporated into other pieces of software such as freeware. Such freeware, which contains hidden spyware, is installed with the consent of the user. In the license agreement for the freeware, the acquisition occurs once the user has clicked the "agree" button. He/she has been deemed to agree not only to the license agreement of the freeware, but also to the acquisition of his/her personal information referred to in the license agreement. This also may be considered illegal. According to the *Interpretative Guidelines*, the business operator should find ways of drawing the attention of users to the existence of the provision on the acquisition of personal information by, for example, indicating "Agreement on the License and Consent to the Provision of the Acquisition of Personal Information" instead of "License agreement."[15]

III. E-COMMERCE RULES ON SECURITY IN JAPAN

Concerning the EC rules on security, two issues are addressed: (1) providing identity (IDs) and passwords on the Internet, and (2) identity fraud.

A. Providing IDs and Passwords on the Internet

Business operators usually incorporate technical sanction programs for viewing, listening, or accessing their digital contents or programs (known as "access controls"), as well as for copying them (known as "copy controls"). They provide their digital contents only to users who pay a fee. Only those users can access the digital contents based on user IDs, passwords, serial numbers, and the like by which technical sanction can be removed.

Such IDs or passwords can be sold and disclosed easily through the Internet, and those who get them could gain access to and copy the digital contents without paying. In addition, some manuals (circumvention manuals) that indicate methods to avoid the access controls or the copy controls, are also sold and disclosed on the Internet. As a result, business operators are suffering loss of profits from those who access and copy their digital contents without paying.

In these circumstances, some legal issues are raised with respect to the sale and disclosure of IDs, passwords, and circumvention manuals on the Internet. First, where a contract has been concluded between a provider and a user that prohibits communication of IDs and passwords to third parties, the sale or disclosure of the IDs or passwords on the Internet by the users constitutes breach

---

[14] *Id.* at ii.65.

[15] *Id*.

of contract. The users thus bear contractual liability (i.e., liability for the non-performance of contractual obligations) pursuant to Article 415 of the Civil Code.[16]

Second, where IDs and passwords are provided for the purpose of using computers via the Internet, the Act on Prohibition of Unauthorized Computer Access[17] prohibits leaking the IDs or passwords to a person other than the authorized user of such IDs and passwords. This does not apply when there are justifiable reasons.[18] Those who perform such a prohibited act are subject to criminal liability.[19]

Third, the act of assigning devices or programs with a function to enable unauthorized access or copying by means of circumventing the effect of technical restrictions of access and copying may constitute unfair competition under the Unfair Competition Prevention Act.[20] Those who perform such an act are subject to civil[21] and criminal liability.[22]

Fourth, a person who has disclosed or provided IDs or passwords on the Internet may be liable for compensation of damages pursuant to the provision on tortious acts.[23]

---

[16] *Id.* at ii.50; MINPŌ [CIV. C.], Act No. 89 of 1896, art. 415, *translated in* (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=02&dn=1&x=57&y=6&co=01&ia=03&ky=article+415+of+civil+code&page=6 (Japan) ("If an obligor fails to perform consistent with the purpose of its obligation, the obligee shall be entitled to demand damages arising from such failure. The same shall apply in cases it has become impossible to perform due to reasons attributable to the obligor.").

[17] Fusei akusesu kōi no kinshi-tō ni kansuru hōritsu [Act on Prohibition of Unauthorized Computer Access], Act No. 128 of 1999, *translated in* (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=02&dn=1&x=0&y=0&co=01&ia=03&ky=act+on+prohibition+of+unauthorized+computer+access&page=8 (Japan).

[18] *Interpretative Guidelines*, *supra* note 4, at ii.50-ii.51. *See* Act on Prohibition of Unauthorized Computer Access, Act No. 128 of 1999, arts. 5, 12(ii), & 13.

[19] *Interpretative Guidelines*, *supra* note 4, at ii.51. *See* Act on Prohibition of Unauthorized Computer Access, Act No. 128 of 1999, arts. 4, 6, 12(i).

[20] *Interpretative Guidelines*, *supra* note 4, at 186. *See* Fusei kyōsō bōshi-hō [Unfair Competition Prevention Act], Act No. 47 of 1993, art. 2(1)(x), *translated in* (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=02&dn=1&x=0&y=0&co=01&ia=03&ky=unfair+competition+prevention+act&page=18 (Japan). The sale or disclosure of IDs and passwords on the Internet as such is not deemed to constitute unfair competition with respect to technical sanctions, but may be regarded as an act to facilitate the infringement of reproduction right on the ground that such act foments the infringement of such rights. *Interpretative Guidelines*, *supra* note 4, at ii.49.

[21] *Interpretative Guidelines*, *supra* note 4, at ii.51; *See* Unfair Competition Prevention Act, Act No. 47 of 1993, arts. 3, 4.

[22] *Interpretative Guidelines*, *supra* note 4, at ii.51; *See* Unfair Competition Prevention Act, Act No. 47 of 1993, art. 21(2)(iv).

[23] MINPŌ [CIV. C.], Act No. 89 of 1896, art. 709 ("A person who has intentionally or negligently infringed any right of others, or legally protected interest of others, shall be liable to compensate any damages resulting in consequence.").

B. Identity Fraud (Identity Theft)

In EC, parties can make a contract without meeting, and it is possible for a person to falsely represent himself or herself as another person in making a contract through the Internet. When there exists no prior agreement on how to identify users, the expression of intention by a fraudulent user does not belong to the identity theft victim. Thus, no contract has been formed between the identity theft victim and the operator.[24]

However, where the requirements of apparent representation are met, a contract may be formed between the operator and the victim, and the latter must perform his/her obligations.[25]

IV. CONCLUDING REMARKS

In this paper some EC rules on privacy and security in Japan have been examined. As parties in the Internet are often not conscious of national borders, the uniform solutions are desirable for effective consumer protection. Nevertheless, the degree of interest in consumer protection is different from nation to nation and the need for regulating B-C EC is also varied among states. From the global viewpoint, it is difficult to unify or harmonize the rules on privacy and security in EC in the near future.

For attainment of unifying rules, however, comparative studies are helpful and necessary. Based on comparative studies, we can identify and distinguish what is different and what is the same in each nation's rules. It would be my unexpected pleasure if this paper could make any, even small, contribution to this goal.

[24] *Interpretative Guidelines*, *supra* note 4, at ii.42.

[25] *Id*.; *See* MINPŌ [CIV. C.], Act No. 89 of 1896, arts. 109, 110, 112 (regarding apparent representation).