February 17, 2017

Opinion on Formulation of "Intellectual Property Strategic Program 2017"

BSA |The Software Alliance

BSA | The Software Alliance (BSA)[1] welcomes this opportunity to provide comments concerning the formulation of the "Intellectual Property Strategic Program 2017."

BSA members invest billions of dollars globally in research and development every year. This investment fuels an ecosystem of innovation and manufacturing that benefits individuals and organizations at all levels of the economy around the world. Intellectual property protection for software products and services is a vital part of this ecosystem in which Japan plays a key role. BSA members strongly rely on intellectual property protection to continue innovating and contributing to the development of the digital economy. We therefore share your goals and interests in protecting intellectual property rights and offer these comments to assist with your efforts.

Amendment of laws for further protection of license authentication mechanisms as technological restriction measures/technological protection measures

Changing Business Models in the Software Industry: The software industry has evolved from days when software was made available exclusively on physical media (such as floppy disks or optical disks). Increasingly, software is acquired on-line, where the user downloads the executable files that install the software on the user's device(s). A more recent trend is offering software as an

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, IBM, Intel, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

Internet-enabled service, such as cloud computing, where the consumer accesses software functionality remotely via broadband Internet connections.

Many software companies adopt license authentication mechanisms to verify that the user is using a lawfully acquired version of the software. Such license authentication methods confirm the right of the legitimate licensee to access and use the software through technical means, often referred to as technological protection measures (TPMs) or technological restriction measures (TRMs) (hereinafter TPMs).

TPMs are important for many software companies because they support the ability to provide tailored options, at different price points including free access, while protecting software developers' investments in innovation and software solutions. For example, some versions are tailored to students or academic institutions. Some are introduced as trial versions which require payment upon the expiration of the trial period.

Considering these circumstances, it is very important to give appropriate legal protection against circumvention of TPMs. BSA urges the regulatory changes below be considered by the Japanese government to ensure proper intellectual property protection of innovative software products and services.

1. Amendment of Unfair Competition Prevention Act

BSA appreciates that the Trade Secret Protection and Utilization Committee under the Ministry of Economy, Trade and Industry ("METI") is discussing whether the current provisions regarding circumvention of technological restriction measures under the Unfair Competition Prevention Act ("UCPA") should be amended. In the sections below, we describe the issues currently facing the software industry and offer recommendations to amend relevant provisions of the UCPA.

Current Issues - Offering of Unauthorized Software Cracking Programs or Product Keys

There are numerous offerings on e-commerce sites – mainly over Internet auction sites – of product keys and software-cracking programs that circumvent license authentication systems. These offerings enable the unauthorized use of software. Thousands of such offerings are available monthly on Internet auction sites monitored by BSA, and these are just for BSA member software.

The following is an explanation of the function of a license authentication system, using the example of a free trial version that is subsequently converted to a full-function version.

First, upon downloading a free limited period trial version of the software on the user's device, the user is required to enter a product key specifically assigned to the trial version. Upon the installation of the software, the trial version of the program that is tied to the trial version product key and the trial status of the software will be recorded on the device. Once the consumer connects to the Internet, the authentication data (e.g. electromagnetic information) recorded on the device along with identifying information about the device (e.g. hash value of the device's unique identifier) is transmitted to a server for authentication and recordation in a database. Upon authentication, the server transmits (by electromagnetic means) information back to the user's device that confirms authentication, allowing the use of trial version on the user's device.

If the user enters an additional product key for the full function software prior to the expiration of the trial period, this new (electromagnetic) information along with identifying information about the device is again transmitted to a server for authentication and recordation. If this authentication is not completed prior to the expiration of the trial period, the trial version will be deactivated or disabled and the software will no longer function after the trial period.

The technical details of how various authentication methods identify different software versions (e.g. trial version, full function version), usage period and the legitimacy (or authenticity) of the product key itself, differ from company to company. Software-cracking programs enable users to activate (or maintain activation of) installed software, for example by rewriting code to prevent the software from initiating the connection to the server for authentication, creating falsified data which has the same characteristics as valid authentication data, and storing it on the device.

The Need to Amend the Unfair Competition Prevention Act (UCPA)

(1) Sale/Making Available of Software-Cracking Programs: To fight against the sale of software-cracking programs, BSA member companies have filed complaints for criminal violation of the UCPA against sellers of cracking programs to police departments in Japan. However, investigations to such claims are often not developed, leaving the sale of such circumvention technologies unpenalized. The reluctance of enforcement bodies to investigate and prosecute is due, in part, to overly narrow interpretations of the definition of technological restriction measures in the UCPA.

BSA recommends simplifying the language of the UCPA to eliminate ambiguity and ensure that modern and increasingly prevalent methods of license authentication are adequately recognized and protected legally. As such, we recommend deleting the indicated text (see below), as it seems to provide no useful function and only creates the impression that the protections of the law are narrower than appropriate and intended.

The current description of technological restriction measures in Article 2(7) does not match up with the business models and authentication systems adopted by many software vendors. The overly prescriptive stipulations related to recording on recording media and transmission systems will likely become further mismatched with the development of new authentication systems in the future. Therefore, we respectfully recommend that the underlined text below be removed from the provision:

Article 2(7): Proposed Revision
“The term "technological restriction measures" as used in this Act means measures which restrict the viewing of images or hearing of sounds, or running of programs, or recording of images, sounds or programs through electromagnetic means (which means electronic means, magnetic means or other means that are imperceptible by humans)~~, and which adopt a method of recording on data storage media or transmitting signals that make machines for viewing and hearing (which means machines used for viewing images or hearing sounds, running programs, or recording images, sounds or programs; the same shall apply hereinafter) react in a specific manner along with the images, sounds or programs, or a method of recording on data storage media or transmitting converted images, sounds or programs, which require specific conversion by the machines for viewing and hearing.~~”

(2) Sale/Making Available of Product Activation Keys Directly: UCPA Articles 2(1)(xi) and (xii) define “acts of providing programs having only such function [i.e. the sole function of enabling…the running of programs…which are restricted by technological restriction measures] through an electric telecommunication line” as acts of unfair competition. However, selling the authentication codes themselves is not considered an act of unfair competition.

Sellers of product keys have been found, upon investigation by rights holders, to obtain product keys by wrongful means. For example, these sellers may acquire the keys via unauthorized access of company information. When a product key is entered by an unauthorized user, the authentication system recognizes the authentication request as a legitimate request from a licensed consumer, and the system will activate the relevant version of the program. The inability to penalize sellers of such keys allows this behavior to proliferate and results in significant use of unlicensed software.

Therefore, we recommend Articles 2(1)(xi) and (xii) be amended to stipulate as unfair competition acts making available product keys or other license activation codes unauthorized by the rights holder, for purposes of commercial advantage or private financial gain.

2. Amendment of Interpretative Guidelines on Ecommerce and Software related Transactions issued by the Ministry of Economy, Trade and Industry

BSA recommends amending the description at “III-10 Liability in the case of providing means to circumvent the restriction on the function or use term etc., of software (iii69~iii78)” (the “Description on Circumvention of Software Restriction”) in the Interpretative Guidelines concerning Electronic Commerce and Information Property Trading issued as of April 2015

(“Current Interpretative Guideline”). This section analyses and determines the applicability of the Unfair Competition Prevention Act (“UCPA”). Such amendment should take into consideration technological changes adopted by the software industry and recent court decisions. Although METI revises the Interpretative Guidelines from time to time, BSA was disappointed that the Description on Circumvention of Software Restriction was not subject to the amendment during the development of the April 2015 Guidelines.

The Intellectual Property Strategic Program 2016 described, as a measure to be taken in FY2016, “Support the creation of appropriate rules in the private sector by developing interpretation of issues related to the Trademark Act and the Copyright Act, etc. in the Interpretative Guidelines on Electronic Commerce and Information Property Trading which describes the interpretation of laws related to electronic commerce, etc.” (item 14 on page 8 of the time schedule). We therefore anticipated an expeditious revision to the Current Interpretative Guideline. However, as discussed above, no revisions were made to this item as of now.

BSA expects the Interpretative Guidelines will be revised if, based on the ongoing discussion by the Committee under METI, the relevant TPM provisions of the UCPA are amended. But regardless of the amendment of UCPA, we continue to request that the current Interpretative Guidelines be revised.

The Description on Circumvention of Software Restriction of the Current Interpretative Guideline (iii77) concludes and describes that “any signal to which a machine specifically reacts but is not stored with the program or does not cause a specific conversion of the program is not a technological restriction measure. Thus the acts subject to analysis are not deemed to be unfair competition against technological restriction measures in any manner and the UCPA does not apply to those acts.” This means the Description on Circumvention of Software Restriction of the Current Interpretative Guideline (iii77) takes an overly narrow approach to the definition of technological restriction measures and does not take into account the license authentication systems commonly adopted by software makers. The Interpretative Guideline should be amended to clarify that providing crack tools which circumvent such license authentication systems constitute acts of unfair competition under the UCPA.

Up to now, there are three cases in which the court has convicted a person who had provided the crack tool circumventing the license authentication system in violation of the UCPA.[2][3][4] In those cases, the crack program circumvented the license authentication system and falsified

[2] Judgment issued by Utsunomiya District Court on December 15, 2014

[3] Judgment issued by Kobe District Court on September 8, 2015

[4] Judgment issued by Nagasaki District Court on January 12, 2016

unauthorized product identification, which was a signal enabling the use of the computer program without any restrictions, such as restriction of the use term or function. In another case, the court ordered a person who had provided the crack tool circumventing the license authentication system to compensate damages to a right holder.[5] In those judgements, the court clearly admitted and ruled that license authentication systems widely adopted by software makers are technological restriction measures under the UCPA and that the crack programs had the function of interfering with the effectiveness of such technological restriction measures, enabling the computer program to operate without restrictions. In this regard, the Description on Circumvention of Software Restriction is not based on enough understanding of the license authentication system. The Description's conclusion that providing crack tools is generally deemed not to be unfair competition is clearly inaccurate. It is therefore not acceptable to leave the Description on Circumvention of Software Restriction as it is since the interpretative guideline has great influence on the concerned parties.

Therefore, the IP Strategy Program 2017 should specifically recommend METI to amend the Current Interpretative Guideline or entirely delete the Description on Circumvention of Software Restriction. If amending, the Interpretative Guideline should clearly limit the application of the Description on Circumvention of Software Restriction, taking into consideration the fact that the Current Interpretative Guideline is not based on the existence of current license authentication system and there is a gap with the current technology trends, and the new court rulings. BSA hopes the Description on Circumvention of Software Restriction will be amended or deleted soon so that software makers suffering serious damage by the provision of crack tools which enables unauthorized use of software will be able to conduct enforcement activities smoothly.

3. Amendment of Copyright Act

Although the circumstances surrounding the Trans-Pacific Partnership (TPP) have changed, effective technical measures to manage the use of copyrighted works, etc. (e.g. access controls) is one of the items to be addressed during domestic implementation of Japan's TPP commitments. Accordingly, the Copyright Act was amended, although the amended law has not come into force. The abovementioned necessity of amending the UCPA is precisely the same as the necessity of amending the Copyright Act concerning access controls and their circumvention. Accordingly, when amending the Copyright Act, the basic approach should be that the definition of technological protection measures allows for a broad incorporation of these technologies since there are a wide variety of access control technologies available for protecting copyrighted works. Furthermore, the Copyright Act should be amended to broaden the definition of technological protection measures and not to limit the definition of circumvention to the distribution of

[5] Judgement issued by Osaka District Court on December 26, 2016

circumvention devices or programs. This should be done to combat issues of stolen authentication codes and crack programs through review of actual case studies thereof.

- End -