Software Asset Management Changes in Developing and Developed Economies

Darren Bean!
Hankuk University of Foreign Studies

Abstract: This paper will discuss how changes to intellectual property laws can cause a need for changed business and management practices, particularly in regards to software asset management (SAM). I will examine various stances regarding intellectual property, causes for the divide in attitudes, and how developed nations (particularly the U.S.) are forcing the world towards a stronger intellectual property regime, regardless of its detriments. As a case study this paper will use information from the Korean "crackdown" against illegal software use in 2011-2012 and discuss changes to Korean law resulting from the Free Trade Agreement (FTA) with the United States as well as prospective changes in Korean SAM practices. The potential for harm to businesses (through losses due to legal defense and lawsuits) is tremendous and therefore I will also discuss how management attitudes must change to respond to ever-intensifying legal pressures and threats, including a basic outline of the goals of SAM.

Keywords: Software Asset Management (SAM), Developing Economies, Intellectual Property, Software Copyright

Intellectual property (IP) is an unavoidable part of modern life and business management. Even if an enterprise never creates a piece of software, publishes a work, or otherwise generates IP, the use of others’ IP in the form of guides, programs, or inventions is almost inevitable. This usage is not a problem in two common scenarios: First, in legal regimes and societies that give limited protection to IP and are less-than-zealous in IP right enforcement, regardless of if infringement takes place, there is likely to be little practical trouble due to prevailing attitudes less sympathetic to IP owner than IP user. Second, in legal regimes and societies that give strong protection to IP and have zealous

1 This work was supported by Hankuk University of Foreign Studies Research Fund of 2013.
enforcement, where most are aware of the procedures they should follow, there is likely to be very little infringement at all; the stringent punishments and liabilities are well-known and thus businesses will take great pains to avoid running afoul of IP laws.

During a transition between the two, however, management can find itself caught in a new legal system and subject to tremendous liability—all for following "business as usual" practices from the "old way." As the products of a nation change, and as that nation is subject to political and economic pressure by the U.S. and other pro-IP nations, the domestic IP legal regime is likely to strengthen. Recently, many Korean business owners were caught somewhat unaware in a "crackdown" against illegal software use; some were bankrupted, some escaped with only a minimal payment to counsel for defense, and others fell somewhere in the middle, suffering moderate to severe losses in the form of settlement moneys and legal fees (which were always greater than the legitimate software would have been). The goal of this paper is to help the attendees avoid the fate of those owners by direction attention early and preventatively towards the goals and practices of Software Asset Management (SAM), so that management can prevent or emerge victorious from SAM IP enforcement actions.

1. Changes in Intellectual Property Perception and their Causes

Copyrights (which protect creative works and computer software) and patents are quite similar from an economic and political perspective. Both are based on the belief that granting a limited monopoly to a creator (author or inventor) will encourage greater proliferation of new works and technology, thus resulting in more creation and work and ultimately a richer public domain and a more informed and wealthy society. The temporary distortion of competition (through monopoly) is seen as a necessary step in the path towards maximum welfare in society. (Shadlen, Schrank, & Kurtz, 2005, p. 48-50.)

This simple idea has some basis in economic reality but it also has its detractors. Simply put, that which is private is not public. If I must pay extra to
the monopoly holder, the immediate effect to me is welfare-negative, that is, the cost to me of accessing the work is greater than it would be without the copyright. One can easily see this in the price difference between generic and brand-name drugs, or the price difference between a blank DVD and one that contains a movie or program. In recent years, the "essential medicines" issue in the World Trade Organization (WTO) and World Health Organization (WHO) has highlighted the winners and losers of IP--developed countries' pharmaceutical companies rarely research drugs that could improve the quality of life in developing countries, and in any case when such drugs exist they are usually priced out of reach of the poorer people of the world. (Trebilcock, 2011, p. 142-46.) Software, as we will see, exists in a state analogous to, if less tragic than, pharmaceuticals.

Even outside of patents and drugs, IP protection is generally less in developing countries; this may be due to several factors, but I will note two here. First, until a nation develops a strong creative or research industry, the citizens stand more to gain by the absence of monopolistic inflation of prices; it is likely welfare-maximizing for those citizens to give away their comparatively fewer creations and take the work of the rest of the world. As an example, the U.S. refused to join one of the most important copyright treaties in the world for nearly a century because consumers in the U.S. were enjoying British novels effectively free of charge. (This stance was reversed partially due to growing numbers of U.S. content producers wanting protection for their works abroad.) (Bean!, 2012, p. 186-87.)

Second, IP--though it may affect life and its quality, as the "essential medicine" issue highlights--does not have strong direct effects on the quality of life. Political instability, unhygenic conditions, and poverty (inasmuch as it leads to a lack of nutrition or basic care) are the impending issues that must be dealt with before IP becomes an issue. If a person is sick, hungry, or fearing a violent death it is not too likely that person will have any concern as to whether a drug was made under license or whether the contents of a book or computer were made with proper royalty payments.
Irrespective of the issues I just mentioned, and concomitant with globalization, one can see a steady increase in the strength of IP laws around the globe. Developed economies (including the U.S. and its rather short memory) are generally "pro-IP" and they have succeeded in changing global law and other nations' laws through trade-based negotiations. Perhaps the most powerful instrument used globally is the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"), a WTO agreement enforceable through that organization. (Trebilcock, 2011, p. 138-41.) The U.S. has also used two other means to strengthen the IP laws of its trading partners: bilateral agreements, including Free Trade Agreements ("FTAs") and trade sanctions; these have been used for political coercion and had tremendous negative effects on consumers and trading partners while protecting narrow special interests. (Shadlen et al., 2005, p. 48; Dames, 2009.)

What is most relevant to business management, however, is not the law in theory but the law in practice. For an illustrative case study of how quickly practices can change (and thus threaten small businesses), I now turn to the recently changed tide of IP enforcement in South Korea, focusing on the 2011-2012 "crackdown" against illegal software use.

II. Case study: Korea

South Korea's development was legendary. It was the first nation to change its status from aid recipient to aid donor, and it did so in only a few decades. But this speed of change left some uncomfortable side effects. Unsophisticated mindsets, including corruption and xenophobic tendencies, clash with modern global ideas on a daily basis. (Wagner & VonVolkenburg, 2012, p. 225-39; Bean!, 2012, 187-89.) Relevant to the current concern is the clash between old practices in SAM (essentially laissez faire or willfully blind to illegal software use) and modern, aggressive software right holder enforcement.

In 2011 software right holders began aggressively pursuing businesses that used illegal copies of software. They were able to do so quite inexpensively, due to a provision of Korean law that provided for criminal sanctions against the
use of copyrighted material "in business." (This term means simply that the illegal software was being utilized in a place of work, not that the business was selling or otherwise distributing illegal copies.) The police, of course, were obligated to help free of charge, and so the right holders could avoid the cost of hiring an attorney and filing suit; the unfortunate defendants, however, were faced with the expense of paying for a defense or paying settlement (a situation criticized by this author in another paper). The cases were typically settled out-of-court and without prosecution, at a price of around 170% the price of the software. (Bean!, 2012, p. 187-92.)

At first blush, the business owners (some of whom were forced out of business by these suits) may seem somewhat unsympathetic, as they were using illegal copies of software. But some claimed a lack of knowledge, suggesting that the vendors of software and hardware may have been the actual culpable parties. Such lack of knowledge, moreover, may be insufficient legal grounds for a defense, highlighting the need for adequate SAM procedures to ensure that management is aware of what it legally needs to be aware of.

Another case reinforces the notion that more knowledge, not less, is generally desirable. In that instance, an employee downloaded software illegally without management's knowledge. The defense was able to establish that the business and owner should not be liable, however even that defense rested on dangerous ground: Management needed to establish lack of knowledge, but other provisions of law mandated a duty of reasonable supervision of employees by management; showing both diligence and ignorance involves walking a thin line, but it is easier to tread that path with proper SAM procedures in place. (Bean!, 2012, p. 192.)

In the past year, Korean copyright law has changed, but in a one-sided fashion worsening the imbalance between right holder and user. The introduction of statutory damages last year (2012) granted a right holder up to ten million won ($9,200 USD) per infringement in a civil suit and up to fifty million won ($46,000 USD) if such infringement is willful; meanwhile, right holders still enjoy the luxury of police help. This legal change, which is unique
and antithetical to most Korean law (which disdains damages set by law), was mandated by the Korea - U.S. FTA. (Bean!, 2012, p. 193-94.)

Of course one must admit that the reach of Korea's law is limited to Korea, but the lesson learned is applicable to most developing economies. As greater wealth is obtained, and trade with the U.S. is increased, generally IP protection will also be increased. When IP protection is increased, enforcement of IP and the cost of noncompliance with IP will increase, resulting in a legal minefield that threatens businesses that may have held lax attitudes towards IP compliance, particularly with respect to software.

One perhaps positive aspect of the crackdown, even from a software consumers' perspective, was the birth of Korea Software User Protection Associates ("KOSUPA"). This group offered low-cost consulting and legal defense to businesses affected in the crackdown, effectively saving more than one defendant. In a forward-thinking manner, KOSUPA is now in the process of developing SAM standards comparable to ISO's SAM standards to guide Korean businesses and help avoid lawsuits like those mentioned above. (Yeon-su "Jon" Han, personal correspondences, March 2012 - April 2013.)

KOSUPA's development illustrates two key points regarding the transition in IP laws previously mentioned: First, business opportunities stem from the IP crackdown: As the cost of compliance increases, the market for compliance assistance (both SAM assistance and legal counsel) also increases, and suppliers are needed to fill the void. Second, the sooner and more thoroughly SAM is addressed (from either a management or legal perspective), the more likely it is that a business will prevail in an IP enforcement action against it.

III. Application of SAM to Business Practices

A. Determining the Level of SAM Needed

The question for business executives then is, "What level of SAM do I need?" A simple cost-benefit analysis would weigh the cost of a certain level of
legal compliance ("C") against the likelihood of legal action against the business ("L") multiplied by the likely degree of harm that the business would befall in an appropriate judgment or settlement ("H"). The ideal level of SAM keeps C beneath L x H; however there are many unknowns that must be initially addressed. If the business is not in the habit of practicing SAM then C may be difficult to estimate. L may also be not only difficult to estimate but subject to tremendous change. In the Korean example, L changed almost overnight for several business owners. H is also difficult to estimate; given that many laws provide for maximum statutory damages ("up to" an amount) and one must study court judgments to predict H, but even then the researcher can only make an educated guess. Finally, as L and H are likely to be better known by attorneys in those fields, businesses may have to consult counsel (yet another expense) before having any idea what the values of L and H are.

Businesses may take basic and likely inexpensive steps, however, to make themselves aware of SAM, which will make them aware the possibility of liability (is L > 0?); these same steps will likely also give the business a rough estimate of what C may be for total compliance. In the terms of the International Standards Organization (ISO), which has promulgated SAM standards, "any organization fully conforming to the requirements of Tier 1 [the lowest tier in ISO] will know whether it is compliant with its software licensing, and it will only be a question as to how management is acting on the knowledge." (International Standards Organization, 33.) Many businesses may wish to carry their improvement further, but space prevents a discussion of those practices. (ISO, vi.)

B. Becoming Tier 1 Compliant

To be Tier 1 compliant, the business must have adequate processes for the following areas:

First, there should be a master "register of stores and inventories." This register will typically include, at a minimum, "1) the defined type of SAM asset, 2) the name of the person in charge of managing this information, and 3) the
location where this store or inventory can be consulted." Duplicate use of assets should only be allowed if recorded in the source record and permissible by the license governing the SAM asset. The goal for this process "[i]s to ensure that the necessary classes of assets are selected and grouped; and defined ... [so as to] enable efficient control of [the assets]." (ISO, 2012, p. 16-17.)

Second, management should take various steps to control software asset inventory management, with an eye towards "ensuring that physical instances ... are properly stored, and that required data ... is accurately recorded." This goal is divided into four subcategories for Tier 1: (1) management of inventories, (2) inventory existence, (3) inventory and store existence, and (4) inventory definition for license compliance. (ISO, 2012, p. 17-18.)

Regarding the first subcategory, the inventories and stores should be "protect[ed] from unauthorized access, change or corruption" and "a means of disaster recovery" should be provided. If access and ability to install are not controlled, management may find its employee's conduct has created a violation of the licensing agreement or law, as at least one unfortunate Korean business experienced. Backup copies of software and data are also wise in case of emergency, but even the backup process should be handled with care. Most legal regimes allow a single backup copy (per legitimate licensed copy) at most; excess "disaster protection" could potentially be seen as piracy. (ISO, 2012, p. 18.)

With respect to the second subcategory, inventories, three kinds should exist: (1) Inventories of "all devices or platform instances on which software assets can be installed or run"; (2) inventories of "all authorized installed software showing (a) packages and versions which can be individually licensed ... and (b) update/patch status of software; all by platform on which installed"; and (3) "underlying licenses and effective full licenses held." Regarding the third category, inventory and stores, again three kinds of stores should be kept: (1) software, (2) contracts, and (3) proof of license documentation. Finally, management should take steps to create and maintain metrics to measure license compliance. (ISO, 2012, p. 18.)
The procedures of the second, third, and fourth subcategories are closely related, and spring from the complexity of some licensing requirements. Software licensing "gotchas" can be numerous and complex; entire conferences are dedicated to navigating the intrincacies. For our purposes, however, it is sufficient to note that a software license may be limited to one machine, may be limited to a specific number of machines, or may contain limitations based on the size of the business (total workstations, total employees, or number of employees that may have access to and use the software), the number of locations of the business, and other factors.

As an illustration, consider the following (fictional) "qualified limitless" software license: "This software may be installed on any number of workstations within any single location so long as the total number of potential users does not exceed 10 people." If our business has 10 potential users in one location then it need not worry about where the software is installed. If, however, our business expands into a second location, it would have to choose one location only for installation (or pursue a new license). If our business increases its personnel it may also forfeit the unlimited nature of the license. Though oversimplified, this example begins to illustrate the issues that can arise with software licensing.

With these complexities in mind, we can turn back to the above criteria and recognize its usefulness in practice. Only when an employer knows how many devices, capable of using software, are in use in his business can the employer begin to ask, "Am I exceeding the license?" Similarly, management must be aware of other rubrics (locations of branches, total personnel employed, relevant personnel employed) and compare these to the rubrics of applicable licenses. To do this, the SAM manager will need to be able to refer to the licenses, hence the need for storage. Contracts of sale or purchase from third-party vendors have a hidden merit: In case the vendor unscrupulously sells illegitimate software, the business may be able to defeat liability by showing an absence of knowledge, or deflect liability on to the vendor.

SAM, like any form of management, is not a single-step process, but rather an ongoing process. As the business evolves, compliance must be
monitored; licenses may also have time restrictions that compel monitoring, and version changes and updates may also trigger the need for review. The remaining Tier 1 criteria are thus largely forward-focused and ongoing. Management should develop procedures for the following areas: (1) Validations of any change in scope of SAM; (2) quarterly (at a minimum) self-auditing, reconciling the actual status of SAM with the authorized use; (3) biannual (or more frequent) verification of hardware inventory; and (4) at least annual verification of software contracts (for both the physical storage of the contracts and compliance therewith). Where problems are discovered, in any of these areas corrective action should be taken. (ISO, 2012, p. 20) Related to the need to review contracts, businesses should also reconcile their licenses quarterly, analyzing and correcting any discrepancies. (ISO, 2012, p. 21.)

The key to SAM, however, is not merely creating policies but reviewing the actual practice. Just as deviations from authorized software installations can cause legal liability, internal deviations from SAM practice can cause the same liability. Thus, the final requirement for Tier 1 certification is an ongoing self-audit process: The business should ask itself if it is following its own SAM procedures, "at least on a sample basis annually" and correct any deviations. (ISO, 2012, p. 22.)

For all SAM practices, typical management concerns must also be addressed. Concerns of responsibility and authority, chain of command, adequate (but not excessive) oversight must inform management's decision when tailoring the policies. The cross-disciplinary aspects of SAM (involving IT, management, and legal issues) need to be addressed by people competent in each field capable of understanding the other fields' contributions to SAM.


ISO's somewhat general and vague standards do not illustrate specific best practices to follow. Those can be found in other documents created by organizations such as the International Business Software Managers Association
(ibsma.com), the International Association of IT Asset Managers (iatam.org) and the Information Systems Audit and Control Association (iisaca.org). These and other organizations often offer training in specific areas as well as various kinds of examinations and certifications. In other nations (particularly those that may not use English as a common language), other groups such as SAMAC (Japanese) and KOSUPA have arisen to meet the demand for SAM improvement that stems from increased IP laws.

Businesses may also greatly reduce their software IP risk by switching to open-source software, which is available (legitimately) free of charge. Suites such as Open Office (openoffice.org) are available as alternatives to Microsoft products, and other more specialized applications are available as well (typically at sourceforge.net). Though these products do not require a purchase, there is still a license agreement to be followed, which will typically prevent the business from selling the software (or any modifications thereto), and may contain other restrictions, so SAM procedures should still be considered.

Conclusion

The trend towards stronger IP protection globally shows little sign of slowing. As IP standards evolve, SAM practices must also change. It is not a matter of "if" but "when" businesses face greater liability and stronger enforcement, as many in Korea have already learned. Those currently directing operations in developing and transitioning countries, however, need not fear the same painful lessons. With minimal upfront expenditure and awareness, management can be aware of the cost of compliance and the risk of noncompliance, and make intelligent decisions to prevent the threat of copyright liability for infringing software use.
References


