UDC 004.4(5)
004.738.5:339

SOFTWARE PIRACY AS A SHADY E-COMMERCE MARKETING VEHICLE

Radomir Mihajlovic[1], Vito Leggio[2], Jelena Mihajlovic[3]

[1]NYIT, New York, NY, USA, rmihajlo@nyit.edu
[2]NYIT, New York, NY, USA, vleggio@nyit.edu
[3]Faculty of Business Studies and Law, Univ. UNION-Nikola Tesla, Belgrade Serbia, jelena.mihajlovic@fpsp.edu.rs

Abstract: *Faced with the persisting phenomena of software and data content piracy Industry and legislators are actively engaged in resolving this alleged plague of the modern technological era powered by the digital computing and communications. In the work of which we present only a part of, we take more optimistic point of view of the general piracy, focusing specifically at the software piracy. Our position stated in this paper is that software piracy plays major positive role in the cyber space revolution and in particular in the evolution of e-commerce, namely, e-commerce applied to illegal trading of software may have some legal and positive attributes, i.e., parameters, which we address here. We introduce novel classification of the e-commerce participants and expand the definition of the e-market to the market that covers legal as well as illegal sales transactions where some illegal transaction may have overall positive effects on the profit line of the original software developers, producers and vendors.*

Keywords: *Software piracy, copyright, counterfeit software, e-commerce, shady e-commerce, implicit e-commerce, marketing, commerce model.*

1. INTRODUCTION

More than half of personal computers (PCs) globally, contain installed software by illegal means. In countries like China, Nigeria or Vietnam over 80 percent of all PC programs are installed without proper license [1]. Although software manufacturers may find these figures alarming, we take the opposing point of view and try to better model this allegedly totally negative phenomena. In fact we try to discover positive parameters that work in favor of original software manufacturers.

According to reports from Business Software Alliance (BSA), a Washington industry

study group [2] [3], in absolute figures, the value of illegally used software worldwide rose to the levels exceeding 60 billion dollars (See Figure 1).

We find that reported estimates of the commercial value of all unlicensed PC software installations and the revenue losses totaling $62.7 billion in 2013 are not fair and are based on the relatively incomplete models of sales, profits and losses. Although not precise and based on various methods of market parameter estimation, these reports clearly outline certain acceptable measures and indicate gigantic dimensions of the illegal software use phenomena. Based on our research we conclude that the major reasons for such astonishing growth of what we call software shady market, are:

- The growth of legal software market itself,
- Expansion of the Internet and e-commerce as trading friendly platforms,
- The growth of the user knowledge of how to counter technical software protections, and
- Very likely consciences software vendor compliance with the software piracy.

In this work, we do not present arguments in favor of the first three above mentioned points and focus only at the last one. Under developed countries like Ex Soviet republic Georgia, Zimbabwe, Yemen, Bangladesh and Moldova are at the top of the list of countries with the highest rates of illegal software use. This fact was one of the major reasons why our approach to the phenomena of the so called software piracy is fundamentally different from the approaches reported so far in the relevant literature.

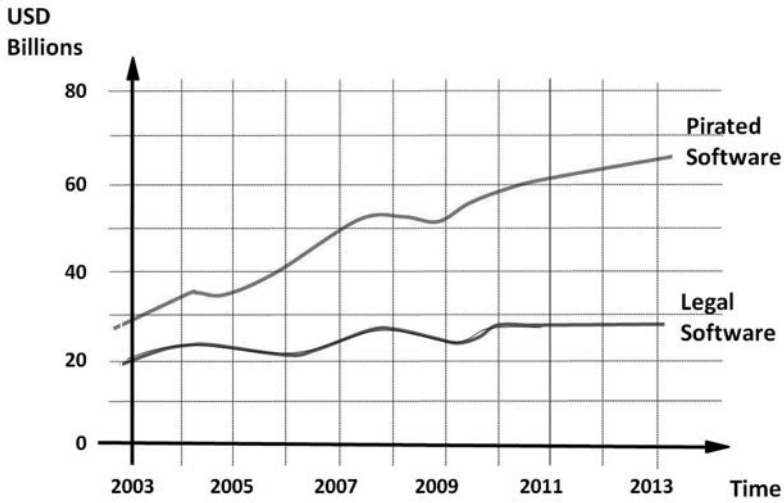

Figure 1: Rise of pirated software through the years, (Courtesy of BSA [4]).

Our work complements and contributes to the work performed by others on the relatively hot topic of software piracy and counterfeiting of software by not resisting this, in some cases, useful phenomena. In other words, the trend illustrated in Figure 1 of rising use of pirated software globally brings positive news to software manufacturers and distributors.

2. SOFTWARE LICENSE AGREEMENT

Systems software status alert message report shown in Figure 2, is frequent event on the PCs used in the countries of the under-developed world or used in poor neighborhoods in the cities of the Western developed world. The report shown in Figure 2, warns the user that software patches will not be provided to illegally installed systems. Apparently, Microsoft is applying software patch policy to their efforts to minimize their software use without proper license.

Software Licensure Agreement (SLA) is a document presented to the end user when acquiring and installing software via e-commerce and Internet or via physical commerce (p-commerce) using portable physical storage media such as CD/DVD or Flash RAM stick.

End software users are expected to agree with all explicit terms and conditions itemized in the SLA before

proceeding with the software use. Some of these terms and conditions prohibit:

- Replicating software and using it on more than allowed number of host computers.

– Replicating software more times than specified in the SLA and passing copies to family members, friends or passing copies to coworkers to be used in the place of business.

– Uploading software via social networks and sharing it without explicit permission which is not commonly found in a typical SLA.

Figure 2. An example of the illegal license detection interrupt triggered alert program form.

Before proceeding with the discussions of explicit and implicit use of the SAL we are making several definitions.

Definition 1. Software license is a certification type of a document issued by the original software vendor, presented to, and accepted by, the software end user as a proof of compliance with the software use conditions itemized in the software use agreement.

As a certificate, a typical software license is issued upon legitimate software purchase to the user. By the acquired license, user is certified as a legitimate or authorized user. To better

understand software license it is good to consider the following definition of the specific SLA issued to end users and supported by the specific contractual agreement.

Definition 2: An End User License Agreement (EULA) is a legally enforceable contract between a software owner (e.g., software developer, publisher, reseller, etc.) and the user of that software.

The very nature of the EULA as a binding contractual document justifies involvement of the judicial and law enforcement government agencies in all cases when license agreements are violated. Different contractual documents are created between the original software producer or Intellectual Property (IP) owner and software distributor or reseller, which apparently are not end users.

Depending upon the financial compensation requirements, software licenses typically are either:

- Proprietary and for sale,
- Open source free, where certain open source rules apply, or
- Trivially free of charge without any limitations or preconditions of use.

The EULA sometimes wrongly used for "software license," appears as lease or rental agreement; where users agree to pay for the license, i.e., for the right to use the software, and promise not to share software or perform any act explicitly not permitted by the EULA document. When purchased via e-commerce software EULA user agreement is followed by a simple check box that signifies user acceptance of the EULA document content.

As a rule, rare users read the EULA agreements which, as a common practice, may cause some realistic problems in the common law based legal systems such as systems found in the USA or Great Britain. In the common law based systems judges are at liberty to apply common sense and their understanding of justice when making their decisions [5].

When software is purchased in the physical market (p-market), EULA acceptance is demonstrated by the user when opening the shrink wrap of the software physical package, when breaking the seal on the CD/DVD media case, when sending a warrantee card back to the software publisher, when installing the software and entering the license number or code, when downloading license patches or other patches or by simply starting to use the software.

Typical EULA allows fair reproduction of the licensed copy for original media backup and disaster recovery purposes without obtaining explicit permission and at no extra cost. Purposes permitting the application of fair use generally include:

- Academic use:
  - Instructing and teaching,
  - Scholarly research.
- Commercial use:
  - Pre sales product testing-out and review, or
  - Marketing relevant product review and technical news reporting,

Interesting case of illegal software license use is acquiring academic or other discount-

ed and restricted software license to use it for an unqualified purpose such as home business.

The authors would like to add to the above list of fair use one implicit case that could expand the formulation of the "fair software use". The case in question is that any unpaid use of proprietary software for self-training and self-education should be considered fair. Third author of this work has repeatedly made public statements [6] that computing should not be exclusive privilege of wealthy, i.e., that any use of software license for self training and self education does not have necessarily to go through the rigid and time consuming appropriate licensing procedure.

3. SOFTWARE PIRACY

Common definition of software piracy found in the relevant literature is all inclusive that we summarize as follows:

Definition 3. Software piracy represents any act of unlicensed use of software.

However, in our classification, software piracy refers to the specific way of use of unlicensed software, i.e., it refers to the unlicensed software reproduction for distribution free of charge or for profit.

Unlicensed software use can be classified as:

- Trivial illegal personal use and reproduction by private individuals or business establishments,
- Pirating use for unlicensed distribution, free of charge or for profit, and
- Counterfeit use for unlicensed media production, packaging, sale and misrepresentation of the product original label.

What we refer to trivial illegal personal (TIP) use is better known as End-User Piracy (EUP), sometimes referred to as Soft-Lifting Copying (SLP). TIP/EUP/SLP is prevalent in the corporate workplace, where one copy of software has been licensed and that same copy of software is installed on multiple computing platforms without the proper multiple host licensure. In some cases, people would also install that same software on their home PCs.

One specific case of TIP use is where user believing that the purchased license is legitimate becomes an unknowing victim of end-user piracy by using illegal license. Fortunately for such users, laws against knowing or unknowing "fencing stolen property" are rarely applied. According to laws of this sort [7] notified user of "stolen property" must stop using and must surrender "stolen property" immediately. Severe penalties are applicable for knowing users of "stolen property" [8].

E-commerce driven piracy is rapidly becoming the fastest growing sort of piracy. Many businesses allow employees to purchase at unrealistic discounts, (frequently free of charge), and download software via the Internet. The use of Internet apparently simplifies software acquisition procedure. However, such simple and time saving e-commerce driven procedures enhance piracy. Typical e-commerce driven illegal software purchase may take place over the popular auction sites such as ebay.com or craigslist.org. Numerous new explicit and implicit e-commerce sites are appearing daily. Smaller sites with shorter time to live (TTL) may be used to promote what we may call a "shady e-and implicit commerce." Shady e-commerce is harder to track and supervise and as such may provide convenient business

platform to software pirates and counterfeit software distributors. Implicit e-commerce sites have, by definition, non commercial purpose, but offer features that can be used for trading, (e.g., various blogs and social networks may be used to connect sellers and buyers).

The most frequent software piracy law violators are engaged in some sort of business of assembly and sale of personal computers loaded with illegal versions of Microsoft operating systems and office suite programs. Such violators are bundling their hardware with illegal software to enhance hardware sale. Since such violators mainly keep buyers in illusion that their systems and application software installed is legitimate, we may consider illegal bundling of hardware with the unlicensed software a counterfeit software distribution. No less frequent are the cases of business use of one host computer license on multiple computers loaded with the replicated single purchased software copy.

As a rule, legal procedures against software license violators are initiated by the disgruntled employee who is looking for the ransom award to be paid by the original software manufacturer, in most cases by the local Microsoft dealership. An exemplary legal case against one such software license violator reported and handled by Majmudar & Co. [9] serves as a good illustration of real world obstacles faced when violators are hard to identify, hard to arrest and even harder to punish financially. Under Indian law, as well as laws of most of the nations, a copyright holder is entitled to the compensation for damages and account of profits against an infringer. However, such compensations are frequently hard to realize. In the particular case reported [9] instead of the imprisonment and nominal compensation of $46,500.00, the court has decided to award Microsoft only amount of $1,037.00. Seemingly very low sum of just $1,037.00 was estimated by the court as the only sum that realistically could be collected and large enough to serve as a relative warning and a sort of a deterrent to potential violators of the same law after the court decision would be publicized in the media. Indian court decision points to the fact that in general, legal systems are facing true difficulties when trying to effectively enforce anti-piracy laws, especially in the countries of the third world or in the communities of financially unprivileged users.

There is no country where the law enforcement agencies can easily search each private residence or business facilities looking for illegal copies of copyrighted software. In countries such as Russia, India or China, with large populations and large segments of their societies financially not capable to purchase legal software copies, effective enforcement of anti-piracy laws is almost impossible. Our findings are that their legal systems are less to blame than the wide spread poverty. Following this argument, back in 1986 [6], third author has explicitly made very clear statement that users of software without proper license which cannot possibly afford to pay for it should not be prosecuted. Placing software license violations in the same plane with other crimes is not fair and should be avoided. The very nature of the software as a product that without a computer as implementation engine has no value whatsoever, the fact that software use requires sophisticated training, and that software replica has marginal cost when compared to other physical product replicas, should be taken into an account when judging software license violation crimes.

Illegally traded software can be classified into the following groups:

- Pirated software, and
- Counterfeit software.

Both pirated and counterfeit software are illegally distributed with subtle distinction,

namely we may refer to counterfeit software as "value added pirated software." Pirated software can be offered:

- Openly, as illegally copied and distributed, or
- Covertly, miss-represented as genuine when in fact it is not.

Counterfeit software is pirated software that could be delivered with minor changes and that is commonly miss-represented as licensed and genuine.

4. E-COMMERCE AND SOFTWARE PROTECTION

In the common business jargon e-commerce refers simply to buying and selling goods and products over Internet.

Marketing activities are frequently not recognized as a part of this common understanding of e-commerce and neither are all pre sale and post sale activities that truly are elements of what is considered as a commerce. We look at sales as the central point of commerce, and consequently of the e-commerce too. However, we recognize that sales are impossible without any pre sales activities. Following up on this view of sales, demonstrating software as a part of marketing effort is quite hard when software is well protected from easy or unauthorized use.

Software protection can be implemented through:

- Technical means using dedicated hardware and software,
- Legal means based on the well defined, clear, fair and enforceable laws. and
- Marketing and sales means.

The scope of this report does not allow us to elaborate on numerous technical and legal means of unlicensed software protection. Instead, we focus on the last implementation of software protection from illegal use, i.e., we pay particular attention to marketing and sales means.

Legal means are without a doubt very effective with business users. The major motivator not to use pirated software exists primarily in business communities which is capable of responding financially to possible court decisions with regard to unlicensed software use. The primary motivator is potential financial loss which can be significant when business organizations are SLA violators. Businesses being audited by the law enforcement authorities for use of unlicensed software results in:

- High penalties which are typically hundreds of times higher than the costs of licenses,
- Business operation disruption which may last not only during the auditing but may be extended until the licenses are purchased and fines paid, and
- Reduction of the customer base caused by the loss of the reputation, (Temporary loss of business services availability caused by the software audit and published news of business noncompliance with the law have negative marketing effects on the business market profile and position).

In situations described above, we state that individual end users should not be prose-

cuted whenever their financial capacity would not realistically make possible fine collection and alleged loss compensations. This should be a default rule when legal costs could exceed all realistic compensations. We are confident that impossible sales to realize with customers that are not capable of paying for the legal software license, are not sales at all and that alleged lost sales due to unlicensed software use in financially under privileged communities are not losses at all, but marketing expenses that as such could be applied against yearly income tax balance sheets as costs of doing business. We have numerous indicators that industry leaders such as Microsoft, Adobe and Apple allow use of their pirated software. The rational is that in order to expand the base of self trained future customers software licenses should be gifted to all willing to train themselves in using given software package. The larger number of self trained users would translate into the larger number of word-of-mouth software promoters at the place of their future employment. Users typically glorify those software packages that they may be the most familiar with. Our current investigations are oriented towards quantifying piracy as innovative marketing vehicle based on preplanned policy not to use strong technical means to prevent piracy.

5. CONCLUDING REMARKS

Software is one of the easiest products to "steal," reproduce and distribute for profit using e-commerce infrastructure. However, besides profiting from selling pirated software, numerous such software distributors tend

to use modified pirated software to launch various cyber attacks. Cyber attacks launched by software pirates probably constitute the main deterrent against illegal software end use. According to the BSA study [10] the main reason why individual users avoid unlicensed software are potential security threats from malicious programs that may be installed with the illegally acquired software. As an extension of [10], our current study that will be presented elsewhere is dealing with the malware as software piracy prevention tool and as possible marketing vehicle used to promote new versions of extra exposed to cyber attacks current versions of software. Our preliminary evaluations point at Microsoft as the leader in exotic marketing practices such as piracy tolerance and benefiting from the cyber crime escalation to promote new products sales. It is indicative that any government attempt to mandate by law various piracy protection mechanisms was faced with the industry split and even open disagreements [11].

We are in agreement with the mentioned pro-piracy exotic marketing practices, in our notation labeled as shady marketing practices. To be more specific, counter piracy solutions that we propose are of a marketing type. We have very strong indicators of the validity of such solutions and their use by the leading companies in the software industrial complex, such as Microsoft, Adobe or Apple corporations.

Based on our findings the most effective solutions of the software piracy problem should be based on the marketing and presales policies. To mention just a few of the existing solutions and the solutions that we value, let us consider counter software piracy:

- Lower cost and larger market using customer friendly e-commerce. Potentially large market that Internet infrastructure facilitates provides an opportunity to sell and to educate much larger number of future users than it was possible before.
- Temporary licensing with further reduction of the software price by eliminating

permanent software license ("ownership license"), and replacing it by the per-use license and per-use pricing, i.e., by the introduction of charges in installments. e.g., with per month use charges. For instance, Microsoft charges as little as $5.00 for their Office product temporary monthly license, [12].

- Free license issued to all individual users from the third world country or poor neighborhoods tracked and identified by the GPS and statistical income level research.

REFERENCE

[1] "BSA Global Survey of PC User attitudes," BSA Study Report, May 2011. http://globalstudy.bsa.org/2010/downloads/opinionsurvey/survey_global.pdf

[2] Dina Bass, "Software Piracy Losses Jump to $59 Billion in 2010, Report Says," Bloomberg Technology, May 12, 2011. http://www.bloomberg.com/news/articles/2011-05-12/software-piracy-losses-jump-to-59-billion-in-2010-report-says

[3] "Security Threats Rank as Top Reason Not to Use Unlicensed Software," The Compliance Gap, BSA Global Software Survey, 2014. http://globalstudy.bsa.org/2013/

[4] "Shadow Market, 2011 BSA Global Software Piracy Study," Ninth edition, MAY 2012. http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf

[5] S. F. C. Milsom, "A Natural History of the Common Law," Columbia University Press, December 6, 2003

[6] Spalevic Nevenka, "O Kompjuterima i Ljudima; Racunari u Razgovoru sa Prof. Dr. Radomir A Mihajlovic," Galaksija Racunari, br. 11, Duga, BIGZ Beograd, Januar 1986, pp.16-18.

[7] "18 U.S. Code § 2315 - Sale or receipt of stolen goods, securities, moneys, or fraudulent State tax stamps," Legal Information Institute, Jan. 2, 2013, 126 Stat. 1963 https://www.law.cornell.edu/uscode/text/18/2315

[8] Steffensmeier, Darrell F. "Fencing Stolen Property". In Bailey, William G. The Encyclopedia of Police Science, 1995. Taylor & Francis. pp. 291–296.

[9] Anoop Narayanan, "Software Pirates in India be Aware," Majmudar & Co., International Lawyers, Mumbai and Banagalore, India, 2000. http://www.majmudarindia.com/pdf/Software%20Piracy.pdf

[10] John F. Gantz, Pavel Soper, Thomas Vavra, Lars Smith, Victor Lim, Stephen Minton, "Unlicensed Software and Cybersecurity Threats," IDC report sponsored by BSA, January 2015, http://globalstudy.bsa.org/2013/Malware/study_malware_en.pdf http://globalstudy.bsa.org/2013/cyberthreat.html

[11] Nick Wingfield, Don Clark, "Trade Groups Are Split Over Combating Piracy Music and Computer Industries Oppose Government Rules; Studios Back Them The Wall Street Journal, Jan. 14, 2003. http://www.wsj.com/articles/SB1042509178176423064

[12] "Get the most secure Office for your business," Microsoft Corp., 2016. https://

products.office.com/en-us/business/get-latest-office-365-for-your-business-with-2016-visit-office?WT.mc_id=PS_Google_O365SMB_%2Bms%20%2Boffice&Dimension=&WT.srch=1