Competition and collaboration in e-commerce

Business, E-Commerce

Abstract

E-commerce and dotcom companies have changed the way businesses conducted in internet era. In 2000 alone, according to one report, the electronic commerce recorded the annual volume estimated to be between $100 billion and $200 billion (Litan 2000).

The huge number soon encourages more and more startups to open their online stores while generating revenue from it. However, protecting information and content has not received enough attention.

Concerning security issue, in this paper, we will elaborate the impact of security on e-commerce. There are two methods that will be discussed: encryption and watermarking. The discussion is based on the fact that currently we only know encryption technologies that have gained increasing prominence in the protection of sensitive data transmission over computer networks. In fact, nowadays, only digital watermarking has the potential to provide protection even after data is decrypted

Moreover, we will discuss the digital security in today’s software market especially in some countries in Asia and other developing and under developing world. The company that we will discuss is Microsoft that its products are almost in every desktop, laptop, and handheld computers all over the world.

In addition, we will also discuss the win—win solution occurred in recording industry to encourage the growing trends of downloading MP3musicformat from a remote host in Internet.

Furthermore, in the next section, we will discuss about the impact of security on electronic commerce. Amazon. com and eBay. com are two examples of e-companies that also pay attention to increasing needs of protecting personal data of their costumers.

TABLE OF CONTENTS

I. Introduction

I. 1 Internet Revolution

Unlike industrial revolution that it takes many decades to mature, Internet revolution has a tangible impact on the daily lives of many people all over the world —at work, at home, and how they communicate each other - in relatively short period. However, people still question whether Internet just a different way to communicate—an alternative to phone, fax, or mail—and thus not likely to have a fundamental impact on the functioning of the economy, as some skeptics have claimed or vice versa?

E-commerce and “ dot-com” that mark the way businesses conducted in internet era, record unbelievable annual volume. In 200 alone, the volume of e-commerce estimated to be between $100 billion and $200 billion (Litan 2000). However, skeptics say that the number is still much lower in relation to overall size of the economy to have had much impact on productivity growth.

I. 2 Economic Potential of the Internet Revolution

Concerning productivity issue, Litan further reveals that Internet has the potential to increase productivity growth in a variety of areas as following:

a) Reducing the cost of many transactions necessary to produce and distribute goods and services

b) Increasing management efficiency by enabling firms to manage their supply chains more effectively and communicate more easily both within the firm and with customers and partners.

c) Increasing competition, making prices more transparent, and broadening markets for buyers and sellers.

d) Increasing consumer choice, convenience and satisfaction in a variety of ways

One of the major features of the Internet revolution is its potential to make the whole economic system, nationally and internationally, more competitive. The Internet could bring many markets closer to the economists’ textbook model of perfect competition, characterized by large numbers of buyers and sellers bidding in a market with perfect information.

The results should be lower profit margins, more efficient production, and greater consumer satisfaction.

Moreover, for internet supporters, the enhanced productivity can be fulfilled through enhanced competition, which in turn results in the improved consumer convenience and expanded choices.

I. 3 E-Commerce: Virtual Competition

In 1990s, the dotcoms building out have made merely a temporary excitement to the investors. The reason is that those companies faced difficulty amidst security and behavioral issues that makes online commerce or e-commerce records no profit.

Amazon. com and buy. com becomes good example of dot-com companies that encourage the exponential growth of retail Internet sales from a tiny base although at the first stage of their development in late 1990s. Amazon. com said to be the symbol offailureDot-com Company since it records huge loss instead of profit. Under such circumstance, one might have expected analysts to project significant increases in retail competition and productivity.

Amazon. com, the famous model of online commerce, also experience similar condition for a few years although later the company finally records profit. There are two lessons from Amazon case, the key to success in e-commerce turns out to be creating consumers database together with the persistence to conduct business in hard times. That fact put Amazon as builder of the world’s finest consumer profile database rather than a retailer.

While e-commerce still poses attractive challenges for dotcom companies, security issues continue rising for fear of new kind of e-crime that enable the criminal to steal personal information like credit card information and copyright violation.

I. 4 Security in E-Commerce

In addition to the increased productivity that Internet provides, we witness factors that support productivity becomes nothing if e-commerce over the Internet does not provide high-level of security. This is vital since in e-commerce, any companies deal with growing customer bases in which each of them demands for secured transaction.

An article in The Internet Security Alliance website reported that 80% of 52, 000 reported incidents are common to all corporations, regardless of industry, location or size. To strengthen the discussion on social-technological aspects, the writer addressed the issue of common platforms and applications that most corporations use to communicate and collaborate among peers over the Internet, which in turn speed up the corporation networks' exposure to attack. The common platforms mean the dominance of Microsoft's products that embedded in all IBM-compatible desktop and laptop computers.

In addition, the article also provides appropriate elaboration on socio-technical aspects by addressing six trends on security of Internet. The six points are automation, sophistication of attack tools, faster discovery of vulnerabilities, permeability of firewalls, increasing asymmetric threat, and increasing threat from Infrastructure attack.

Furthermore, based on the STS (Science, Technology, and Society (STS) perspective, the internet security developers should also promote the healthy competitiveenvironmentin the internet security industry amidst the fierce competition towards the invention of security products.

I. 5 Research Objectives

Amidst the attractive potential that Internet provides such as increased productivity and enhanced industrial competition, we might expect whether companies are racing towards better services including security or just aiming at recording huge sales volume.

Based on the fact, we witness that today’s e-commerce is getting fascinating since no single strategy works well for all dotcoms enterprises. In this manner, there will be various achievements coming from different strategy in e-commerce. Marketing strategy, view of web sites and types of security the dotcom companies provided are becoming consideration in e-commerce.

Concerning the security issues, under the main topics of competition and collaboration in e-commerce, we will discuss about the development especially in the needs of providing copyright protection amidst the increasing number of piracy that violate intellectual property. Therefore, the objective of this paper is to answer three questions regarding the security, collaboration in e-commerce, and competition in e-commerce.

To be specific the three research objectives can be derived into three specific questions as following:

1. Does digital security like watermarking and encryption successfully and effectively discourage e-crime especially piracy?

2. Is there any method that turns illegal actions into legal ones in order to increased collaboration in e-commerce? And

3. How e-companies promote competition in relation to customer's personal data?

In order to address the three separated questions but interconnected each other, we determine to compose this paper in the following order:

§ Introduction: this section gives general info or knowledge on issues that related to the three objectives above. The info is internet revolution and its economic potential, e-Commerce and virtual competition, security in e-commerce, and research objectives

§ The second section is literature reviews that address more detailed underlying info that support the clarification or claims for the three research objectives. Therefore, this section provides more detailed and focused information on issues than the introduction section

§ Methodology. This section provides us with information on what kind of research and its tools we employ to make this research valid and worthy

§ Result. In this section we provide arguments that answer all three research objectives. The answers or claims are generally based on the info we provide in literature reviews section.

§ Conclusion or summary. This section provides comprehensive information on what we have done in this research. it composes of reasons why we choose a specific research method, potential pitfalls of this research, and many more.

II. Literature Review

II. 1 Security and E-Commerce Competition

According to a global survey on financial service industry conducted by Cap Gemini Ernst & Young's it is found that security in e-commerce becomes important issue since it reached peak in 1997 and 1998 when e-commerce started taking off the ground of traditional commerce. Furthermore, in the 1999 survey we witness that competition still become the greatest concern for e-commerce in 36 per cent of financial services firms, while only 17 per cent cited security. Despite recent needs of increasing security in e-commerce, the situation is more extreme in Europe where only 11 per cent of firms are most concerned about e-commerce security (" Fear of Competition").

II. 2 Security in E-Commerce

II. 2. 1 Racing Towards Digital Security

This section is basic information to answer the first research objective concerning the effectiveness of digital security like watermarking and encryption in discouraging e-crime especially piracy

Digital technology that comes from a manipulation of data has created many opportunity for users all around the world. There is people who take benefits from the growing e-commerce, for instances, but in contrast there are also people aim at destroying the current steady e-commerce by creating malicious software or using Internet as a tool to promote piracy like happened in software and music industry.

Under such circumstances, people realize that Internet and e-commerce

should protect such kind of e-crime by providing techniques that discourage and protect the evil intention.

II. 2. 2 Needs of Protecting Copyright

Intellectual property is the codified physical descriptions of specific knowledge that can be owned and readily traded. Intellectual properties that receive legal protection become intellectual property.

There are five forms of intellectual property: patents, copyrights, trademarks, trade secrets, and know-how. The five forms have been existed since hundred years ago. In 2010, the implementation of copyright will celebrate its 300th anniversary dating back to England's Statute of Anne. During these period, copyright laws at any form has favored creative author to protect their intellectual properties (Bauchner 2001).

Stephen Fishman in The Copyright Handbook says, “ Copyright is a legal device that provides the creator of a work of art or literature, or a work that conveys information or ideas, the right to control how the work is used.” Therefore, copyright is central issue concerning the intellectual property in which any violation on the law will harm the public interest.

II. 2. 3 Technology and Copyright Protection

Protecting intellectual property has received a lot of attention lately, both in terms of revised intellectual property laws (Goldstein 1996), as well as new technology-based solutions. It must be absolutely clear that any technological solution must be backed up with the appropriate legal framework to resolve disputes. Most existing techniques that have been

invented to solve the problem of piracy fall into two categories: copy prevention and copy detection.

Underlining the importance of copyright protection, below we provide two kind of technology-based copyright protection methods that are commonly encountered in today’s business.

II. 2. 3. 1 Encryption

Encryption is a useful method of protecting copyright by providing codes along with message. In this manner only desired person who can decode the message since the person has the correct key. Anyone else without proper key views this encrypted messages like a random series of letters, numbers, and characters.

Unfortunately, this method of security does not seem complicated since it merely uses public key that is common in most email clients. Therefore, actually anyone can decrypt any encrypted message once he/she know the keys (“ Encryption”).

II. 2. 3. 2 Watermarking

However, protecting information and content has not received enough attention. While encryption technologies are gaining increasing prominence in the protection of sensitive data transmission over computer networks, only digital watermarking has the potential to provide protection even after data is decrypted (Koch et al 1996).

Unlike encryption, digital watermarking does not prevent illicit acts but rather provides evidence and the eventual proof of such an act after it has

taken place. Digital watermarking is the embedding of unobtrusive marks or labels that can be represented in bits in digital content. The embedded marks are generally invisible (or imperceptible) but can be detected or extracted through computing operations and is why they are called digital watermarks.

The watermarks are bound to and hidden in the source data, becoming inseparable from that data (such as images and audio and video clips) so they can survive operations that do not degrade the data beyond its utility value in the intended applications. Watermarks can also be used to communicate copyright, ownership, and usage-control information even after such format conversions and compression.

Watermarking technology, if designed properly, can be used as proof of ownership, as a content authentication tool, and as a means of imprinting fingerprints into the data to allow tracing of the recipient should the data be misappropriated. At present, there are two main approaches to digital watermarking, namely visible and invisible watermarking.

A. Invisible Watermarking

The first method (Brassil et al. 1995), called line shift encoding, encodes the document uniquely by vertically shifting the locations of text-lines. One bit is transmitted in each line that is moved. During decoding, the digital image of the document is obtained and text-lines are located using horizontal projection profile.

The distance between adjacent text-lines is measured. This can be done by either measuring the distance between the baselines of adjacent lines or the

difference between centroids of adjacent lines. This method works for formatted documents only.

Figure 1 Examples of text watermarking

Source: Lan, Eric ; Ben Huckaby, ‘ Digital Watermarking’, Retrieved May 15, 2005 from http://ecommerce. ncsu. edu/csc413/student-work/watermarks/DigitalWatermarking. html

The second method (Brassil et al., 1995), called word-shift encoding, is a method of altering a document by horizontally shifting the locations of words within text-lines to encode the document uniquely. Unencoded lines are included to detect and compensate for nonlinearities that occur in printing and copying. However, this method is only applicable to documents with variable spacing between adjacent words, and because of the variable spacing requirement, decoding requires the knowledge of the space between words in the unaltered document. Again, this is useful only for formatted text documents.

The third method (Brassil et al. 1995) is called feature encoding. The formatted document is examined for chosen features, and these features are altered, or not altered, depending on the codeword. Decoding requires a specification of the change in pixels at a feature.

B. Visible Watermarking

Meanwhile, visible watermarking has also been investigated by some research groups, though the target of watermark has never been text documents. The watermarks are mainly used to provide copyright protection for high quality images and video.

Figure 2 Two Examples of Visible Watermarking in Images

Source: Lan, Eric ; Ben Huckaby, ‘ Digital Watermarking’, Retrieved May 15, 2005 from http://ecommerce. ncsu. edu/csc413/student-work/watermarks/DigitalWatermarking. html

The IBM group has done some research on visible watermarking (Braudaway, Magerlein and Mintzer 1996). A visually unobtrusive watermark is embedded into a large area of the image by modifying pixel luminance. A pixel in the image is darkened or brightened according to where the brightness of the corresponding mask pixel is located in the linear brightness scale. Randomization is added to the strength and the location of the watermark to make it less vulnerable to automated removal.

Another visible watermarking technique is proposed in (Kankanhalli, Rajmohan and Ramakrishnan 1999) by placing various intensity of the watermark in different regions of the image depending on the underlying content of the image.

C. Visible Vs. Invisible

Amidst the different benefits each method of watermarking poses, there is a clue for copyright holders whether to choose visible or invisible watermark. According to Lan and Huckaby, copyright holder should determine what purpose the watermark is supposed to serve. If they aim to deter a would-be thief from stealing an image or video document, then a visible watermark is the best choice. This is due to visible watermark has benefits of simplicity to implement.

However, visible watermark poses weaknesses as well since it lacks ability to prevent digital manipulation by cropping the image to get rid of the watermarked area or by clever image manipulation. Another weakness is that visible watermark also makes the watermarked images become severely damaged since the original images are changed in some way.

In addition to a visible watermark, it seems an invisible watermark becomes the right and attractive method for any copyright holders. This is due to the method undoubtedly useful in tracking files and being legal proof against whoever may illegally copy and distribute it (Lan and Huckaby).

Another benefit of this method is that it enables the encoding of information about the media such as the year produced, artist, and title, for instances. The invisible watermark can also be used as a form of authorization, such as in a scan able identity card (Lan and Huckaby).

However, like visible watermarks, these invisible watermarks also poses demerits since they are likely difficult to implement, especially when determining the balance between robustness and transparency (Lan and Huckaby).

Furthermore, concerning the demerits of invisible watermark, Bergnel ; O’Gorman’s propose several items that copyright holders should pay attention to as following:

“ The invisible watermark should be in someway is difficult or even impossible to remove it. This can be achieved at least by creating a method that does not visibly degrade the original image
The invisible watermark should created in a way that is still exist even

people try to remove it by using high-end image modifications software that are common nowadays

An invisible watermark should not alter the way people perceive about the watermarked images

Above all, invisible watermarks should be readily and easily detectable by the authorized copyright holders even common observers could not perceive the difference. In this manner, there should be appropriate method of decoding without requiring the original un-watermarked image (Bergnel ; O'Gorman)

II. 3 Cyber Media and Its Traps

This section become underlying information of explaining any method that is able to turns illegal actions into legal ones in order to increased collaboration in e-commerce.

Moreover, the maturity of web technology together with the contents that enrich the cyber media has provided unlimited information resources in which students, teachers, designers, engineers, and other scholars to gather materials that are needed to finish their intellectual projects. Unfortunately, the plethora of intellectual property on the cyber media also provides people traps in terms of copyright that any people should not violate it.

Stephen Fishman in The Copyright Handbook says, " Copyright is a legal device that provides the creator of a work of art or literature, or a work that conveys information or ideas, the right to control how the work is used (" Copyright and Fair Use" 2004)."

Moreover, in relation to the invention of new media technologies, especially Internet, Forness reveals, “ there are currently two main pieces of legislation that address the topic of copyright on the Internet. They are The Digital Millennium Copyright Act (S. 2037), which unanimously passed the Senate on May 14, 1998 and the Digital Era Copyright Enhancement Act (H. R. 3048), which is still awaiting approval in the House” (Forness).

Furthermore, Reed Library suggests since copyright relates to the further need to receive permission from the source or a legal representative for the direct use of certain material covered by law, ones that use materials made available through the library are responsible for complying with copyright law (“ Legal and Ethical”).

II. 4 Security Roles in E-Commerce

The wide range of potential applications for the technology means great business opportunities and makes for a large base of potential customers. The technology's functions orgoalscan be classified into four application categories: copyright protection, hidden annotations, authentication, and secure and invisible communications. Each involves its own special requirement sets with regard to robustness, security, imperceptibility, and the volume of data that needs to be embedded. For instance, when digital watermarks are used for copyright protection, the need for robustness, security, and imperceptibility is obvious, while the amount of data to be embedded is of only marginal interest.

When digital watermarks are applied to copyright protection, the potential market includes electronic commerce, the online and offline distribution of

multimedia content, and large-scale broadcast services. A long list of potential customers includes content creators (artists, authors, movie studios); content providers (photostock archives, libraries, professional photographers), electronic commerce and graphics software vendors, and manufacturers of digital still images, video cameras, and digital video discs.

For proof of authenticity of documents, digital watermarks are of particular interest in the fields of electronic commerce and distribution of multimedia content to end users. The surfaces of ID cards, credit cards, and ATM cards could be watermarked; so could bank notes, personal checks, and other bank documents.

The watermark, which might be detected automatically, could provide proof of authenticity. Digital watermarks may also find a huge market in forensic applications. Digital still-picture and video cameras could have integrated modules for embedding digital watermarks so pictures and videos are " fingerprinted" with the time and device identifier of its creation. Scanners, printers, and photocopiers may refuse operations if they find a watermark specifying permission to manipulate the document but does not authorize them to scan, print, or copy it.

II. 5 E-Commerce and Customers’ Personal Data Protection

To be precise, everyone has a secret just like companies does. While companies’ secrets might come in the form of detailed specification of a manufacturing process, lists of customer names and addresses, secret formula like the recipe for Coca Cola, people have invaluable secret information: their personal data. All of which share similar characteristics

that they should be protected. Therefore, this section is underlying information on explaining the way e-companies promote competition in relation to customer’s personal data.

Vivien Irish says that in recent years, many countries have introduced laws on the protection of confidential business information along the lines proposed by the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), which states that for information to be legally protect able as follows:

1) the information must be secret, i. e., not generally known ore readily accessible to persons that normally deal with that kind of information

2) it must have commercial value because it is secret

3) the owner must have taken reasonable steps to keep it secret (2003)

In the case of e-commerce in which personal data could be sent out easily on the cyber world, it is important for a company that has personal data of their customers to mark documents with a word such as “ confidential” in order to prevent misuse by their staffs. Other security precautions may be needed, such as imposing password protections or providing limited access to few people to look at the information.

However, in a normal business, it is sometimes necessary to share a secret with another company. For example, a credit card company has a joint marketing agreement to market ahealthinsurance in which the card company should provide detail information of their customers who agreed to buy the insurance to their partners.

Under such circumstances, the solution is to get the company to which the confidential information is to be disclosed to sign a Confidentiality Agreement, sometimes called a Non-Disclosure Agreement (NDA).

II. 5. 1 Model Non-Disclosure Agreements

The Agreement names the owner of the information (Owner), the company receiving it (Recipient), and there is a space to fill in the reason for handing over the information - the Permitted Purpose. It briefly defines what the information is, and it says that records of the information (which may be documents or drawings or software) should be marked " Confidential" or " Proprietary".

The Agreement says how long the information must be kept secret - this can be set as the length of time the secret will give the owner a market advantage, plus a little bit of leeway. Once the Recipient has signed the NDA, the Owner can pass over the confidential information with improved peace of mind (Irish 2003).

II. 5. 2 Law on Protecting Customers Secret Information

In the English law, if there has been misuse of the confidential information, the English courts are willing to act very quickly to hear the arguments and to stop any repeated misuse. Although the information cannot be “ made secret” again, at least the misuse can be quickly stopped so that the company misusing does not continue to profit from it.

In a cross-border disclosure, often the owner of the secret will provide the text of the NDA and will suggest use of the law applying in the owner’s home

country. This is not essential; if the parties can agree, the law of any country could apply.

Companies should not use a Non-Disclosure Agreement too often. The best way to keep a secret will always be not telling anyone. If a secret really must be shared, like the case on credit card and insurance companies, tell as little as necessary to achieve the commercial objective, sometimes a general outline is all that is needed. Sometimes an NDA sets out a period so that information disclosed, say within a defined year or months, falls within the agreement.

Therefore, the best practice to keep secret is not telling anyone any confidential information of our products and our customers' personal data and ensures to set Non-Disclosure Agreement in the event we should share some secret to another company.

III. Methodology

In general, there are two approaches to research: Qualitative and Quantitative. Qualitative approaches are research that is carried out through interviews and observations. This kind of research enables a researcher to investigate in little more detail on the individual perceptions of a phenomenon. Since the research deals with the personal, therefore, such an investigation is limited in its scope.

To be specific, in this paper, we would employ qualitative approaches to research. There are two approaches in qualitative research, interviews and observations, but in this paper we merely consider observations methods. By

using this method, we enable a researcher to investigate and find out a phenomenon in much from individual perceptions.

Moreover, observationbecomes an important technique for collecting data concerning what occurs in a real-life situation. This method also helps us to reach an understanding about the perceptions of those who are being studied, in that situation. To be specific, we employ non-participant observation method especially by analyzing qualitative information from journals, books, magazines and many more.

The reason we choose observation method is because it is an important research tool in which it allows us to observe other people in a natural setting or in a more artificial experimental situation. Moreover, by using observation method we can collect and gather data in natural settings concerning what is really going on in a real-life situation.

The most important of conducting observation is it provides researchers with an understanding about the perceptions about things or people we observe. However, since observation deals with someone’s perception, we plan to avoid preconceptions since it would provide this research with some bias.

In this paper, methodology research that we employ is observation, especially non-participant observation. The reason we choose non-participant observation method is because this method allows us to observe people or organization in a natural setting or in a more artificial experimental situation.

The method does not involve direct interviews which will slightly reduce objectivity and the accuracy of information. We are retrieving more reliable

data from experts' analysis, journals and various publications from available media. Using the data resources above, we are hoping to present an independent and objective analysis toward the contemporary issue.

Concerning the security issue, we will also provide an example of a well-known company that equips its product with digital security in order to discourage the growth of software piracy that is widely found in today's software market especially in some countries in Asia and other developing and under developing world. The company that we will discuss is Microsoft that its products are almost in every desktop, laptop, and handheld computers all over the world.

In addition, we will also discuss the win—win solution occurred in recording industry to encourage the growing trends of downloading MP3 music format from a remote host in Internet. By using non-participant observation, we can obtain experts' and music industry players' analysis regarding the need to cope with the technological changing in digital distribution over Internet for the benefit of the recording companies and the customers.

In addition, to answer the question on whether customers pay attention to security issue while doing online transaction, we will provide sample case of Amazon. com that currently becomes the largest online stores. The methodology we use in this part is by using both participation and non-participation observation since we also experience buy books and other gadgets via Amazon. com.

In the end, we provide analysis on what makes e-companies win e-commerce. This part is mainly using non-participative observation since we

do not have our own online stores so that we do not have enough experience to tell what makes a company wins e-commerce. Therefore, non-participant observation is the appropriate method to describe factors of winning e-commerce.

IV. Result

IV. 1 Digital Security and Microsoft Antitrust Case

This section provides related example of the use of digital security like watermarking and encryption in preventing e-crime especially piracy in software industry. We use Microsoft as an example of company employing digital security in their products,

Talking about information technology, we cannot overlook Microsoft as the dominated software manufacturers that make computers work properly. Its products range from operating systems to today’s famous Java language programming. Unfortunately, the domination of Microsoft products in almost personal computers all over the world has invited competitors and government to questions the company’s business practices since there is indication that Microsoft products, especially its operating systemfamilynamed Windows, also bundled with applications that will prevent other companies to provide such applications.

The type of security that Microsoft implements are invisible watermarking. In this manner, the company assesses a registering Windows product from a desktop computer, for example, and evaluates whether it is original or a pirated one. In order to encourage every Windows software to register online, Microsoft create some applications that computer users heavily need

and ask them to assess their software at first before downloading the desired application. One example is through the creation of Microsoft Anti-Spyware that Microsoft gives the software for free.

Concerning the issue we found that the growing piracy especially on Microsoft products is due to the company dominates the software market in every level. This situation has also brought the company into many court cases within the last decades.

The antitrust case against Microsoft is somewhat similar to other antitrust cases in which Microsoft’s domination in computer software has prevented other software firms to grow and compete fairly. Therefore, the antitrust case against Microsoft is about restricting consumers to choose a variety of software. However, such action reflects what Americans fear about that Japan and Europe will take over their domination in economy.

According to Mike Ingram in Settlement Reached in Microsoft Antitrust Case, there are a lot of evidence that show how Microsoft had subverted new technologies such as the Java programming language, in order to ensure the dominance of the Windows desktop. The situation obviously reflects a growing feeling that in protecting its dominant place in the market for desktop computers, Microsoft was retarding the development of new technologies emerging around the Internet.

Another question arises from this case is that is it legal to continue the monopoly on software market. The question reappears since within the four years since the case was begun, it has been business as usual at Microsoft

that the company has succeeded in laying the basis for a further expansion of its monopoly.

Within the sales of its operating system, Windows XP, consumers who purchase a new computer will have to go out of their way to avoid it being pre-loaded with the operating system, as well as Internet Explorer, Media Player and other software Microsoft chooses to integrate into the system.

Back to a decade ago when the Internet fever hit market, Netscape was by far the most popular browser. Concerning the potential of Internet in the future, Microsoft consider the famous Netscape as huge problems for Microsoft since the Seattle-based company assumed at that time that Netscape browser were potential to become a platform for developing alternative application software, thus preventing Windows' monopoly of the PC operating system market.

To continue its monopoly, Microsoft responded by releasing his own Internet Explorer browser free of charge, then immediately bundling the Explorer with Windows 95 as the default browser thus undermining Netscape user to install the browser due to simplicity.

Another fact on the monopoly of Microsoft lies on the so-called activation requirements. Under the guise of fighting piracy, consumers who bought Windows XP must send their personal information about an individual user to Microsoft's websites. In which XP registers particular hardware configuration of the consumers' computer and prevent other computer to use the same XP installer.

The fact immediately invites critics that say Windows XP is part of the company’s drive to protect and broaden its monopoly. Timothy Bresnahan, an economist at Stanford and former senior official in the antitrust division of the Justice Department, says while XP is a new and improved operating system, but it is also part of the company’s effort to further bias the future of computing and Internet commerce in Microsoft’s favor (Ingram).

However, this case poses dilemma for users since although we hate the way Microsoft prevent other software developers to install their application under XP platform, yet we still use XP preloaded with Internet Explorer and Media Player for the reasons of simplicity and easiness.

Fundamentally, the antitrust case against Microsoft was about how best to defend the US capital in an increasingly competitive market for computer software and related technologies.

At a basic level, the antitrust case shows the increasing conflict between the development of new technologies, especially the Internet, and the capitalist market and the system of private property upon which it is based.

This fact soon raises a question is it appropriate to prevent other software installed under Windows (Microsoft Operating System) platform. In Microsoft case, therefore, we as consumers might say that it is unfair and inappropriate to prevent other providers to build software, which works under Microsoft’s operating system platform. However, Microsoft might respond that their operating system only dedicated to their products, for instances.

This situation will further pose a problem since most computers in this planet earth use Windows operating system, only small portion that uses IBM’s OS/2, Linux, and other operating systems. Thus, we also face dilemma to eliminate Microsoft monopoly not only in operating system but also in almost computer applications.

Concerning the spyware program, the company also plans to embed the program into next generation operating system. This situation as explained above will likely to rouse other companies’ ire that cause many attacks aimed at Microsoft’s products.

Therefore, the implementation of digital security will enhance and improve Microsoft’s dominance in software market. This also will discourage and minimize the incidence of software piracy.

However, it turns out that the creation of high-level security in Microsoft’s products turn out to encourage e-crime to find the way to hack the software and distribute it over the Internet. Therefore, watermarking, encryption, and other security techniques do not seem to discourage e-crime especially concerning piracy since the criminals continues search for keys to break the secured system.

IV. 2 Legalizing the Illegal Services: Case of Recording Industry

In addition to Microsoft’s strategy behind the digital security, we also found that copyright protection can be achieved through the reformation in an industry in order to legalize what formerly illegal services like one in recording industry. Therefore, this case of recording industry best describes

the method that effectively turns illegal actions into legal ones in order to increased collaboration in e-commerce.

Formerly, recording industry faced intense pressure from the emerging technology like MP3, a digital compression technology. Such technology soon bore new kind of industry: file-sharing over the Internet. However, while this attractive industry continues growing, the traditional recording industry sued companies like Napster for violating copyright.

Napster was a worldwide network that enabled and this encouraged peer-to-peer file-sharing network. In this manner, users of Napster were able to search the hard drives of all other Napster in order to locate MP3 file of their desired songs. Afterwards, the users could download the desired music files for free. Historically, this kind of music sharing once reached 72 million registered users before court decided to shut down the services.

The above situation occurs since recording industry once depended upon traditional supply chain that involves MFR and Distribution system that soon become obsolete in today’s e-commerce.

IV. 2. 1 Traditional Supply Chain of EMI Music

In traditional supply chain (figure 1), we witness that recording companies make huge revenue and thus the profits from the two elements (in blue boxes). However, this model soon changes considering technology advancement in music like MP3 that immediately spawned illegal peer-to-peer music download over the Internet.

Concerning the issue, coupled with wide coverage of high-speed Internet access, recording labels realize that they should change their supply chain to

adopt the advancement in information technology as described in the following section.

In this web-based supply chain model, we witness that recording labels are massively legalize licensing strategy that significantly fire up a legal digital music subscription (in contrast to Napster that was illegal).

Figure 1 Traditional Supply Chain of EMI Music

Source: Daugherty, Tyson. 2002, ‘ Creating a Digital Music Marketplace’, [Online] Retrieved May 15, 2005, Available at lab. insead. edu/publications/mbareports/ Creating%20a%20digital%20music %20marketplace. pdf

IV. 2. 2 Web-based Supply Chain of EMI Music

Figure 2 Web-based Supply Chain of EMI Music

Source: Daugherty, Tyson. 2002, ‘ Creating a Digital Music Marketplace’, [Online] Retrieved May 15, 2005, Available at lab. insead. edu/publications/mbareports/ Creating%20a%20digital%20music %20marketplace. pdf

Therefore, in recording industry we witness that there is a good breakthrough in protecting and discouraging illegal actions (piracy) in term of music content distribution by changing old supply chain employing MFR into one that adopt web-based supply chain.

The new web-based supply chain cast by two giant recording companies in the world has helped reducing music piracy over the Internet although it is still occurred in small pieces between personals. But al least the mediator

like Napster that encourages music piracy between millions of users will not exist in the future.

It means that there is a way or a solution to turns illegal actions (music piracy over the Internet) into legal ones (web-based supply chain) in order to increase collaboration in e-commerce especially in recording industry.

IV. 3 Protecting Customers' Confidential Data: Amazon. com

In internet era, companies need to remember that the Web is inherently global - when a company launches a Web site, it is accessible by a worldwide audience.

In compliance with the new model of e-business, companies should aware that they are facing various customers from diverse countries, implying that they should cope with different needs.

Within the past few decades, the terminology " mass customization" has taken off the ground. It is the result of various customers' demands, which need products/services tailored in specific fashion. From outfits to private airplanes and sport club's members to telecommunication services, people are demanding that their products and services exactly fit their specific needs.

Under such circumstances, the customers and manufacturer/service providers are closely related. It further influences the way the manufacturers/service providers interacts with their suppliers in order to ensure the products tailored to fit their customers' needs and faster delivery.

At Nokia, for instance, the terminology of mass customization has come by providing customers with various Xpress Color Covers to cope with different customers' tastes. At recent days, Nokia floods the market with various types of handhelds, each with different features, size, models, and accessories.

IV. 3. 1 Amazon. com and Customers Data Base

In order to explain the way e-company promote competition in relation to customer's personal data, we choose Amazon as the company that best describe and provide good example of the objective.

In late 1990s and early 2000, the dotcoms building out have made merely a temporary excitement to the investors. The reason is that those companies faced difficulty amidst security and behavioral issues that makes online commerce or e-commerce records no profit. Amazon. com, the famous model of online commerce, also experience similar condition for a few years although later the company finally records profit.

There are two lessons from Amazon case, the key to success in e-commerce turns out to be creating consumers database together with the persistence to conduct business in hard times. That fact put Amazon as builder of the world's finest consumer profile database rather than a retailer. However, security issue cannot be separated from the success of Amazon since in the past people rarely doing online buying since they fear of e-crime especially concerning their credit card information that is prone to be spied.

Under such circumstances, direct marketers have acclaimed the web as the promotional medium of the future due to its potential for sales and for

communicating a message. Some benefits of doing online direct marketing are:

1) It Allows them to closely target their advertising (important in reducing their costs and in avoiding the fallout from approaches to consumers who don't want the product/service)

2) It can be seamlessly integrated with databases (e. g. to measure the effectiveness of online campaigns, tie them to offline promotional activity and underpin incentive or other schemes)

3) It can be trialed for a national audience or particular demographic more cheaply (and more quickly) than marketing via print, radio, television or other media

4) It is a step closer to one-to-one marketing (“ Direct Marketing”).

IV. 3. 2 Winners of E-Commerce

Similarly, we witness that electronic commerce has driven vendors to set applications for customers to design products or services the customers need at a click away. Automobiles, motorcycles, furniture, personal computers and toys are products that customers can customize their needs through online stores.

Considering the advantages of addressing various customers’ needs, it is important that any vendors and online portals owners enrich their website with the capability for customization in which customers can design according to their tastes and buy online. This is the key to win in e-

commerce in which most vendors in late 90’s fail to comply, resulting in the bankruptcy of many dot-com companies.

Amidst the crowd that says dot-com era only creates an euphoria of having new technologies (Internet), I would insists that dot-com era have bought us to the era where we can set commerce at much easier, simpler, and better ways. Many bankruptcies of dot-com companies at late 90’s or early 2000 does not reflect the fail of Internet technology, instead, it showed us how the companies fail to comply with the real customers’ needs and lack of knowledge to do online business.

It is therefore the dot-com crisis in late 90’s or early 2000 convinces that just like traditional business, there will be companies who win the business, leaving others who fail. There is no reason to say that e-commerce is a fake fortune, instead, it is the hidden fortune that well informed entrepreneurs must find it to win the new era of e-commerce. Look at eBay. com and Amazon. com, they are not traditional companies that do online commerce, instead, those successful companies are the real dot-com companies that grew from zero customer base.

The plethora of increasing online commerce is therefore need improved security in order to increase the number of hits. Therefore, things Amazon does in their online stores are to improved security issues to make their customer comfortable.

Therefore, in term of C2C (customer to customer) e-commerce we witness that protecting customers’ personal data plays significant role in marketing strategies since customers like people in common do not like their data

disclosed to anybody else. This kind f protection also helps e-companies promote competition between them.

V. Conclusion

Digital technology that comes from a manipulation of data has created many opportunity for users all around the world. There is people who take benefits from the growing e-commerce, for instances, but in contrast there are also people aim at destroying the current situation by creating malicious ware (malware) and spyware that steal personal data.

Furthermore, the advancement in communications and internet technologies has spawn a new model of the world’s economy, borderless economy. The terminology refers to the existence of cross-nations or even cross-continents trade, commerce, and other economics process. In internet era, companies need to remember that the Web is inherently global - when a company launches a Web