Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2003 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2003

A Multi-Dimensional Framework for Digital Content Commerce

Mayur Kamat
Texas A&M University

Joobin Choobineh
Texas A&M University

A MULTI-DIMENSIONAL FRAMEWORK FOR DIGITAL CONTENT COMMERCE

Mayur Kamat
Texas A&M University
mayur@tamu.edu

Joobin Choobineh
Texas A&M University
jchoobineh@cgsb.tamu.edu

Abstract

It is estimated that the current annual loss to US economy due to piracy of digital content is about $9.2 billion. Currently, there are two solutions to this problem. One is a technical solution where copying of content is rendered infeasible. The other is legal in the form of copyright, digital theft and other laws. Neither of the two, by themselves or together, is effective. Hackers develop counter measures to new technical solution. Furthermore, there could be a consumer backlash against the content providers who burden the consumers with additional technical steps for content installation and reuse. Due to the small monetary value of each piece of content, laws cannot be equitably enforced or not enforced at all. In this paper, we propose a four-dimensional solution to this problem. Two of these dimensions are technical and legal. The other two are business and social dimensions. We hypothesize that the latter two, combined with the first two, provide a rounded and holistic solution to the digital content management problem. We will present the role of each of the four in the framework. More importantly, the role of some of the intersections of these four dimensions will be presented. Testing the hypothesis remains to be done.

Introduction

As reported in PWC Technology Forecast 2002-2004, Meta Group predicts that by 2005, the market for digital content will be around $300 billion USD. Of this amount, $100 billion USD will be transacted via the Internet. Of this, in the same source, IDC predicts that the market for providing digital rights management and related content dissemination services will be about $3 billion USD [PWC Technology Forecast 2002-2004]. Hence, the digital market is witnessing a high proliferation of digital rights products and services, both from major market players like Microsoft, IBM and Sony to boutique firms such as Content Guard, Intertrust, and Content Directions who provide specialized services.

Technology forms the core focus of most current industry solutions. Technology allows creation of digital supply chains to substantiate a value system. Technology also can add accountability and provide tracking features allowing inventory management of digital goods. Theoretically, substantial amount of security for rights protection can be provided. The questions to ask are "Is it required?" and "Who is going to pay for it?" Issues are lack of flexibility in wide scale distribution of digital content and intrusion of consumer privacy. We hypothesize that technology alone cannot address all the requirements of an emerging and sustainable economy for digital content commerce. Additional factors must be considered.

We propose a four-dimensional model consisting of technical, legal, business, and social aspects. See Figure 1. We have not found other frameworks in the literature. Via this unique approach, we do not just address the sellers' needs for protection and usage tracking but also the end users' need for flexibility and value-for-money. By addressing the needs of both of the parties involved in transactions on digital goods, our research provides impetus for targeted efforts which should lead to emergence of an ecosystem conducive for conducting commerce of digital content.

Current Environment for Digital Content Commerce

The current environment for digital content commerce relies mainly on technical and legal domains. Both strive independently for establishing a sustaining economy for content commerce. A brief overview of these domains follows.

Legal Environment

In the United States and most other countries, copyright laws provide legal protection for digital content by giving the creator exclusive rights to control the usage of content [SIIA Report on Global Software Piracy, 2000]. Digital Theft Deterrence and Copyright Damages Improvements Act of 1999 allows for stringent measures, both prosecutionary as well as economic in case of infringement of digital copyright laws. Legal machinery exists for digital economy in forms of Legal acts like No Electronic Theft (NET Act) and Digital Millennium Copyright Act 1998 [DMCA].

Despite the existence of these laws, software piracy amounts to more than $11 Billion USD globally [SIIA Report on Global Software Piracy, 2000]. This figure does not include revenues lost to government due to income tax, sales tax, or indirect losses like job losses in software industry. International Intellectual Property Alliance [IIPA 2002] estimates the loss to US economy due to piracy of digital content to be about $9.2 Billion.

Hence, the mere existence of laws is not enough of a deterrent for piracy incentives. Considering the fact that today the legal machinery is only one of the two sources of protection for the digital economy, several concerns are raised. These include feasibility of legal acts, extent to which these laws are enforced, and the reaction of the public if they are enforced vigorously. According to a survey conducted by Internet News, more than 53% of Americans are not receptive to strong enforcement of legal acts as far as piracy is concerned.[Internet News]. Digital economy needs a well-thought out legal mechanism that addresses needs of both the producers and consumers.

Technical Environment

With the legal domain insufficient to provide a sustaining environment for the digital economy, content producers have started putting more thrust on use of technology solely to protect their interests and revenue systems from the attack of piracy. This can be seen in efforts taken by industry stalwarts like Microsoft (mandatory online registration for personal software, Tungsten DRM server and Palladium project) and IBM (EMMS - Electronic Media Management System)[IBM]. Boutique firms like Content Guard [XrML], Content Directions (Digital Object Identifier services)[DOI] have sprung up to address specific technology needs like content markup (XrML) and content identification (DOI).

The majority of these efforts concentrate on prevention of illegitimate distribution of content and thereby curbing piracy. Our research is based on the assumption that perfect protection against illegitimate replication and distribution of digital goods is not possible and more importantly, not required. Content piracy can be defined as a combination of illegitimate distribution and usage. Unless the distribution negatively affects the revenue streams of the content producer, it cannot be considered as piracy. Change in outlook leads us to the emergence of a new distribution paradigm known as superdistribution. We will discuss this idea in more detail in a later section. A major shift in the direction of the efforts in technical arena, hence, is required – from prevention of illegitimate distribution to effective tracking and monitoring of content usage.

A Framework for Content Commerce

Given the shortcomings of the current environment, we propose a multi-dimensional framework, based on which, a successful ecosystem can be formed that will encourage establishment of a digital content commerce. The framework has four overlapping dimensions. These are technical, legal, business, and social. The stakeholders from each dimension need to address needs depicted in their domain. Cross-domain efforts need wider and much more involved participation from all sectors of the economy.

Technical Domain

Technical security includes security at the server side, trusted environment, and tamper resistant software. Each of these sub-domains is critical for the success of the business because security is the weakest link phenomenon [Schneider 2001]. A breach in either of these sub domains will lead to failure of the entire system.

Server-side Security - Specialized servers for rights management like Microsoft's Windows Rights Management Server and IBM EMMS are in the offering. These will help fortify the server side security, at the same time providing requisite flexibility.

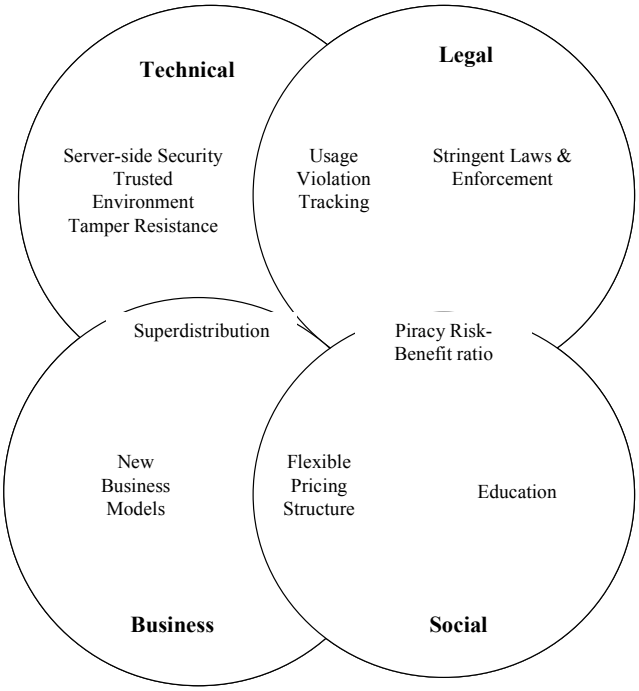

Figure 1. Framework for Digital Content Commerce

Trusted environment – In case of digital communications, security efforts have always been targeted at server-side and in-transit security. This is because the client is assumed to be trusted. In digital rights management and content commerce, the client has to be assumed hostile [Kamat, 2001]. Given a protected content (software, e-book or music), the user has to be assumed to have unlimited time and resources to break the protection mechanism [Cheng, Litva, Main, 2001]. The most important requirement hence is to create a trusted environment on the user domain – one, which will be able to protect the interest of the content producers [Kamat, 2002]. Tasks involved in the process of creating a trusted environment are: identifying sensitive modules, making them tamper-resistant and building integrity checking mechanism.

Initiatives are being taken in this direction. Trusted Computing Platforms Association (TCPA) has been in existence for more than 4 years. Started by Intel, it has garnered wide-spread industry support from Microsoft, IBM, HP-Compaq and more than 170 organizations.

Tamper Resistance Software (TRS) – Debacle of Content Scrambling System (CSS) for DVD and Stephen King's online E-book was because the systems were not made tamper proof. This is also the major factor why most shareware and demo-ware software are easily cracked [Trialware Professionals Association]. TRS implements content-dependent information inside the content (watermarking for images or music, tamper-resistant modules for software), which make it possible for the application using the content (or the application itself in case of software) to detect reverse engineering [Spinellis, 2000]. TRS ensures the integrity of the software and forms the basis of creating a trusted environment [Kirovski, et al, 2002]. Using TRS modules, consummate security can be provided in the user domain.

Performance issues are of prime importance as well. If the overhead of the usage tracking and transaction modules is substantial compared to the original digital good, then the usability of the good is affected creating adverse reaction from the consumer.

Legal Domain

The protection of digital goods is to a great extent dependent on the legal machinery. Copyright Acts like DMCA are widely debated [Clark, 2002] because of the ambiguity in the interpretation of laws. Stringent and unambiguous rules with effective enforcement machinery are a prime necessity for consummate legal security.

One such proposal is making rounds in the US Congress. Proposed by Senator Fritz, the bill is called as Consumer Broadband and Digital Television Promotion Act. [CBDTPA 2002]. Though the demands made by this bill are pretty controversial and are claimed by few to be outrageous and unfair, it has to be taken as a starting step in the right direction.

Business Domain

Forrester Research claims that most rights management initiatives are bound to fail [Garrity, 2000]. While this statement can be considered extreme, the fact remains that digital commerce and rights management initiatives have not bloomed. The most important realization to be conceived is the fact that the reason for this phenomenon is not due to technical shortcomings. Technologies have been developed to cater to the technical needs of rights management and commerce. Minor modifications and improvements will lead to feasible and secure solutions. But the important question is: Would these technologies lead to what is being desired by the stakeholders of the digital economy? A recent example is that of the decision of Intuit Corp. to copy protect its most popular software, Turbotax, in 2002. There was a huge consumer backlash with several anecdotal evidences to the effect that many of its loyal customers switched to competitors products. This leads to the need for further research in the business needs for successful digital content management.

The market in digital properties (computer software, digital music, videos, pictures, documents) is in a primitive state compared to the tangible markets [Cox, 1993]. The easy-to-copy nature of digital goods has prevented the emergence of digital supply chains where sub-suppliers provide subcomponents that higher levels of the chain assemble into high-level goods. In other words, multi granular digital goods are not viable on a pay-to-copy basis.

For a digital business to be financially secured, it has to enlist participation from all its stakeholders. To satisfy the producers of digital content (Music companies, software firms, publishing houses), support for new business models is necessary. This will include micro-business models like pay-per-use, digital rentals and Superdistribution. Various other business models can be chalked out, which provide granular control over sale of digital goods. This enable the producers and publishers to be responsive for the volatile needs of the consumer. These include preview, roaming content, Library (check-in & check-out), gift and subscriptions. For the consumers, flexible pricing structures have to be devised so as to cater to the needs of the diverse audience. Micro-transaction is an imminent need in this direction. With secure and reliable micro-transaction machinery in place, the needs of all the stakeholders can be satisfied.

Social Domain

Due to lack of stringent rules and lower chances of enforcement, the risks associated with piracy are very low. The cost of acquiring the digital goods legally is very high due to lack of price flexibility. Hence, the comparative benefits associated with piracy are high. This low risk-benefit ratio is the main reason for widespread piracy.

This has lead to a warlike scenario in the digital economy. Sellers are viewing consumers as thieves. Hence, industry builds vault-like solutions (Microsoft Palladium, Trusted Computing Platform Alliance) which will bind the user and prevent piracy. Buyers feel duped as they are being charged exorbitantly. They reply by using illegitimate content sharing systems like Kazaa and Morpheus. Lack of commensurate legal machinery fuels the situation.

Flexible pricing structures, consumer education in copyright laws and increasing the risk-benefit ratio by strong legal enforcement are among the social factors that can be influenced by stakeholders.

Cross-Domain Factors

In our opinion, of all the possible intersections between the four dimensions, only four are significant. Each is discussed below.

Technical-Business: Superdistribution – Traditionally, software piracy protection efforts have been concentrated on preventing illegitimate replication and distribution of digital goods. Superdistribution introduces a fundamentally new paradigm for content commerce. By definition, it removes all constraints on the distribution of goods, while introducing constraints on the usage of these goods [Mori & Kawahara, 1990]. In fact, ease of duplication and distribution now becomes an asset to digital commerce than a liability.

Small players in the digital market are often daunted by the task of acquiring consumers. Given the limited marketing budget, most small players have to make-do with a small fragmented market. In addition, it is a very high-risk proposition as illegitimate usage cannot be easily tracked leading to substantial losses. Digital Commerce needs a mechanism that allows players to reach consumers on an individual basis [Peppers, et al, 1999]. Superdistribution is a plausible solution that facilitates content proliferation by allowing unrestricted distribution while still maintaining the seller's revenue system by tracking and monitoring product usage.

To allow for this radical new model, several technical requirements need to be satisfied. The first stage is to identify the critical modules in superdistribution software. These are usage tracking, transaction, and content storage modules. The next important step will be making these modules tamper resistance.

Technical-Legal: Usage Violation Tracking – Foundation of Superdistribution rests on the assumption that usage monitoring can be implemented successfully. [Mori & Kawahara, 1990]. Usage violations can occur if attempts are made to do away with the protection mechanism of the usage modules. In case of such events, a violation tracking mechanism is imperative. This mechanism will allow for monitoring illegitimate activities and curbing them at the root level. This will prevent proliferation of crackz (software that break protection mechanism of shareware and demoware software) and warez (illegal hosting of software, games and music) sites.

Business-Social: Flexible Pricing Structures - Large volumes of very small transactions are beyond the scope of traditional banking infrastructures. For example, penny-per-plan tunes are not possible because banks and credit cards cannot handle transactions smaller than a few dollars [Online Tactics 1997]. The sellers' only option is to sell tunes on a pay by the barrel basis. The recent decline of the music industry [WSJ, August 2002] shows that consumers are beginning to rebel by using illegal music sharing services like Kazaa, Morpheus and Gnuetella. This does not reflect unwillingness to pay a reasonable by the song fee, but unwillingness to pay far larger amounts of a commodity they will only consume a finite number of times.

Flexible pricing structures will provide several options to buyers and sellers for conducting digital transactions. Allowing users to choose the granularity of the product or service they wish to purchase will lead to a conductive environment for digital business.

Piracy Risk-Benefit Ratio - Lack of stringent legal enforcement and the fact that flexible pricing mechanism is not in place has resulted in low risks and high benefits in favor of piracy. With the suggested improvements in legal and business domains, we can hope to achieve a state-of-affairs wherein the risks associated with piracy will surmount the corresponding benefits. A user will think twice before pirating a song, which he can listen to for a dollar if the probability of getting caught was substantially higher. Thus, the potential for digital piracy will decrease.

Domains like technical-social, legal-business and technical-legal-business-social are not highlighted by this paper. The constituents of these domains do exist. For example, superdistribution can also be touted as a technical-legal-business-social effort as it involves all four, but the majority of its constitution comes from the business and technical domains. Technology adoption model [Sherry]

Summary and Future Directions

We have formulated a general structure and model for digital content commerce. The four dimensions of this model are Technical, Legal, Business, and Social. More important to the success of this model is the intersections of these dimensions. Of particular interest to us is superdistribution which is the intersection between technical and business dimensions. Currently we are studying and analyzing various factors that contribute to the successful creation of a superdistribution environment. Additional efforts will include analysis of industry solutions, such as Microsoft's Tungsten and Palladium, Trusted Computing Platform Alliance, and IBM's EMMS. Analyzing shortcomings of these solutions will lead to improvement in the requirement specifications for the framework. Our focus will remain on developing a comprehensive model, which will serve as a reference for future research and development in the field of digital rights management.

References

CBDTPA – Bill S.2048 - http://cryptome.org/broadbandits.htm
Cheng, S. Litva, P. and Main, A., "Trusting DRM Software", W3C Workshop on DRM, 2001.

Clark, D. "Future of Intellectual Property: How copyright became controversial", Proceedings of the 12th annual conference on Computers, freedom and privacy, 2002, pp 1-10.
Cox, B. "From reuse repositories to global area networks: Dempsy dumpsters of the information age", Proceedings of the tenth annual Washington Ada symposium, 1993.
Digital Millennium Copyright Act 1998, U.S. Copyright Office Summary **http://www.loc.gov/copyright/legislation/dmca.pdf**.
Digital Object Identifier – **www.doi.org**.
Electronic Media Management System – International Business Machines - **http://www-3.ibm.com/software/data/emms/**.
eXtensible Rights Markup Language – **www.xrml.org**.
Garrity, G. "Music and Book Industries to Lose $4.6 Billion by 2005", Billboard, Vol. 112 Issue 40, p9, 2p.
IIPA, "IIPA 2002 Report on Global Copyright Protection and Enforcement", 2002
Internet News, "Survey: Consumers Oppose Anti-Piracy Laws", Internet News, Jan 24, 2003.
Kamat, M. "Security Considerations in DRM". Proceedings of International Conference on Electronic Commerce (ICEC) - ECRML Workshop 2001.
Kamat, M., "Security Requirements of DRM", Proceedings of ISECON 2002.
Kirovski, D. Drinic, D. and Potkonjack, M., "Enabling trusted software integrity", Proceedings of the 10th international conference on architectural support for programming languages and operating systems.
Morim R. and Kawahara, M." Superdistribution: The Concept and the Architecture", Transactions of The IEICE, Special Issue on Cryptography and Information Security, Vol. E-73 No.7, 1990.
Online Tactics, 1997 "Building revenue a dollar at a time", Online Tactics, Oct97, Vol. 3 Issue 10, p1, 3p
Ordonez, J., "Sales of Recorded Music Decline", Wall Street Journal, Aug 27, 2002
Peppers, D. Rogers, M. Dorf, B. "Is Your Company Ready for One-to-One Marketing", Harvard Business Review, January/February 1999, pp. 151-160.
PWC, 2002, "Digital Rights Management", PWC Technology Forecast Vol. 1, 2002
Schneider, B. " Secrets & Lies: Digital Security in a Networked World", Wiley, John & Sons Inc., 2001.
SIIA, 2000 SIIA Report on Global Software Piracy **-http://www.siia.net/piracy/pubs/piracy2000.pdf**.
Sherry, L. "An Integrated Technology Adoption and Integration Model", International Journal of Educational Telecommunications (1998) 4(2/3), 113-145
Spinellis, D., "Reflection as a mechanism for software integrity verification", ACM Transactions on Information and System Security, Volume 3, Issue 1, 2000.
The No Electronic Theft (NET) Act - Relevant portions of 17 U.S.C. and 18 U.S.C. as amended - **http://www.usdoj.gov/criminal/cybercrime/17-18red.htm**.
Trialware Professionals Association – **www.trialware.org**.