Post-Payment Copyright System versus Online Music Shop: Business Model and Privacy

Heikki Kokkinen
Nokia Research Center
Helsinki, Finland
heikki.kokkinen@nokia.com

Mikko V. J. Heikkinen
TKK Helsinki University of Technology
Helsinki, Finland
mikko.heikkinen@tkk.fi

Markus Miettinen
Nokia Research Center
Helsinki, Finland
markus.miettinen@nokia.com

***Abstract*—A post-payment copyright system is used to legalize copyrighted music files which a user has obtained illegally. We compare a post-payment copyright system to an online music shop by analyzing three scenarios using both qualitative business and quantitative techno-economic modeling. We analyze the privacy challenges and solutions related to the post-payment copyright system. According to our quantitative analysis, the post-payment copyright system is potentially a more profitable business than an online shop when no media replacement is required. Our qualitative analysis suggests benefits in bundling post-payment copyright system with online music shop and customer sensitivity to the marketing message. The privacy threat analysis and the list of suggested solutions show that privacy is a key factor in the system success, but it is possible to develop adequate protection for the user privacy. Our research is a continuation to the trend of studies suggesting peer-to-peer networks as a part of a viable business model for media distribution.**

Keywords-business model; copyright; post-payment system; privacy; risk analysis; security; techno-economic modeling

I. INTRODUCTION

This paper analyzes a post-payment copyright system with three methods: (1) qualitative business modeling; (2) quantitative techno-economic modeling; and (3) the attack tree method for security analysis of user data privacy. It extends and refines our previous work on quantitative techno-economic modeling of such a system [1] with extensive qualitative analysis on business model and privacy issues. In a post-payment system the users are able to legalize the unauthorized music files on their hard disks and memory cards. In order to understand the service, let us consider a user of peer-to-peer (P2P) networks. The user has downloaded music files on his computer from a peer-to-peer network. With the post-payment copyright system, the user can pay the required fees to copyright agencies and avoid potential litigation, resulting in both personal and commercial security. In this paper we study the cost efficiency of such a system in comparison to two related systems: a conventional online music shop and a post-payment copyright system where the illegal file is replaced with a legal file.

We study the following research questions: what are the main differences in the business models of post-payment copyright systems and conventional online music shops; what are the differences in profit, risk and cost distribution between post-payment copyright systems and conventional online music shops; and what is the role of privacy in the post-payment copyright system.

For our qualitative analysis we use the STOF (Service-Technology-Organization-Finance) business model analysis framework established by Bouwman et al. [2]-[5]. In our quantitative analysis, we conduct techno-economic analysis for digital music sales complemented with risk analysis using Monte Carlo simulations.

The term business model has been defined in several ways in the academic literature. Timmers [6] concentrated on technology elements, whereas Amit and Zott [7] emphasized revenue generation aspects, and Chesbrough and Rosenbloom [8] design aspects. Based on the previous research, Bouwman et al. [3] proposed a unified definition, which acts as a basis for the STOF business model analysis framework.

The other bases for the STOF framework are several componentizations of business models. Alt and Zimmerman [9] recognized mission, structure, process, revenues, legal issues, and technology as the main elements of business models. Osterwalder et al. [10] proposed product, customer interface, infrastructure management, and financial aspects as the basic elements of business models. Shafer et al. [11] identified strategic choices, value creation, value capturing, and value network as the main components in 12 componentization publications. Bouwman et al. [3] decided to focus on four components in their STOF framework: service, technology, organization, and finance.

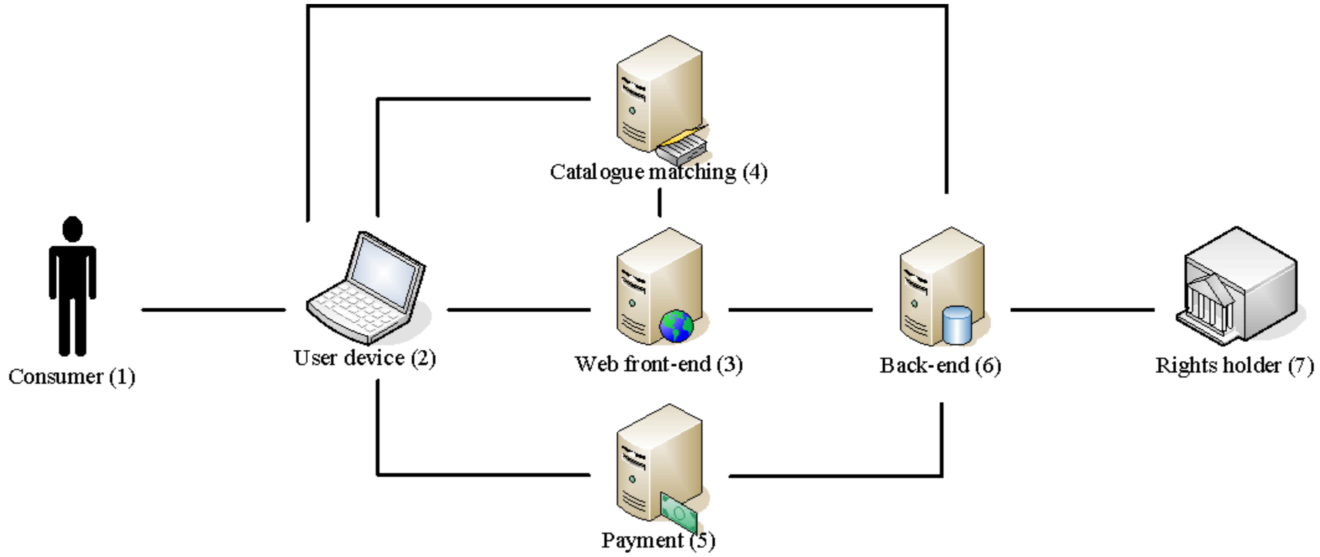

Figure 1. Post-payment copyright system architecture

The post-payment copyright system was introduced by Kokkinen et al. [12]. The legal framework for the service was discussed in [13], and the method for illegal vs. legal classification of MP3 files in [14]. In an online survey Hietanen et al. [15] identified post-payment copyright system as the second most attractive new P2P related business model for consumers, following a monthly paid file sharing service with unlimited access to music and video.

Consumers, copyright authorities and legislators have varying views about P2P. Cohn and Vaccaro [16] apply neutralization theory to the ethics of P2P music file sharing. The P2P file sharing divides opinions about its impact on music business. Peitz and Waelbroeck [17] show that P2P music file sharing has a positive impact on music sales through wider sampling of music by consumers. Bhattacharjee et al. [18] simulate online music sales with different strategies in the presence of P2P-based piracy.

Techno-economic modeling can be considered as a quantitative extension to qualitative business modeling. It analyzes profitability of a new technology or service. Techno-economic modeling and its application to broadband access networks is introduced in [19] where a quantitative framework for conducting techno-economic analysis on broadband networks and several case studies based on it are depicted. Elnegaard and Stordahl [20] demonstrate the use of Monte Carlo simulations as a method for risk analysis in quantitative techno-economic models. Both qualitative and quantitative techno-economic modeling have been used in several studies related to telecommunications: Monath et al. [21] on fixed broadband access network strategies, Jerman-Blažič [22] on network backbone upgrade investments, Kumar and Kueh [23] on international mobile roaming, Smura et al. [24] on virtual operators, Kivisaari et al. [25] on mobile broadcast, Rokkas et al. [26] on fixed-mobile convergence, and Heikkinen and Luukkainen [27] on mobile P2P communications.

Security is essential in deploying the post-payment copyright system. Schäfer et al. [28] studied security in P2P networks from a general perspective, Suomalainen et al. [29] from a mobile perspective, and Merz et al. [30] from a grid perspective. Koshutanski et al. [31] analyzed security in digital ecosystems. Without underestimating the concerns in the web generally, the post-payment copyright service raises even more serious concerns than an average web or e-commerce site, because the post-payment copyright service requests user to give information about past illegal activities. Such information is very sensitive to the user, and in normal circumstances past illegal activities are not disclosed to anyone. Storing so sensitive information also requires special measures.

Privacy in the general context is understood as a “right to be left alone”. In the digital information world, privacy can be interpreted as a right of the user to control what personal information is disclosed to whom, and under which circumstances [32]. In the post-payment copyright service, privacy means among other things that the user of the service can control the information that is submitted to the service and that the exposure can be limited to only such data that will not have negative consequences for the user.

Already in the early days of online commerce, consumer privacy concerns were prevailing. However, during the last decade, consumers have learnt to trade private information for personalized services. Wang et al. [33] classify privacy concerns in Internet marketing as follows: data is acquired improperly including access, collection, and monitoring; data is used improperly including analysis and transfer; privacy is invaded as unwanted solicitation; and data is stored improperly. Kobsa [34] has found the following privacy principles in the European legislation: personalized services based on traffic or location data require the anonymization of such data or user's consent; users must be able to withdraw their consent to the processing of traffic and location data at any time; the personalized service provider must inform the user of the type of data that will be processed, of the purposes and duration of the processing, and whether the data will be transmitted to a third party prior to obtaining the user's consent; personal data obtained for different purposes may not be grouped; and usage data must be erased immediately after each session. Lu et al. [35] classified the elements of privacy in a peer-to-peer system to be identity of peers, content, and interests.

The major privacy concerns of the user arise due to the fact that in the course of using the post-payment copyright service, the users are submitting indirect evidence about their past illegal activities. Users want to be absolutely sure that there is no considerable risk of their data being used in any other way than what it is necessary for fulfilling the purpose of the service, i.e., legalizing the user's content.

The nature of the service itself can feel for the user like being accused as a criminal. Such feelings raise easily negative reactions. An example of this was the blog discussion triggered by a questionnaire study investigating internet users' perceptions on peer-to-peer file sharing. The study was published in [15]. The blog writers used very strong language when they expressed their outrage. They felt that the survey questions blamed all peer-to-peer file sharing content to be illegal and that the creators of the questionnaire allegedly accused the respondents as criminals.

Many web and e-commerce sites use methods which decrease privacy concerns and build trust in users. Kobsa [34] has found the following aspects to decrease the privacy concerns on web sites: positive past experiences, design and operation of the site, reputation of the site operator, presence of a privacy statement, presence of a privacy seal, privacy laws, pseudonymous users and user models, client-side personalization, and privacy enhancing techniques for collaborative filtering. Hoffman et al. [36] discussed how to build trust online by anonymity or pseudonymity, cooperative interaction between site owner and consumers, and privacy policies. Palmer et al. [37] showed how trusted third parties and privacy statements increase the trust on an e-commerce site. Freenet [38] protects the peer-to-peer users from privacy infringements and uses anonymity to decrease privacy concerns.

The post-payment copyright service provider should use the known methods of creating trust on web sites and e-commerce sites. In Table 1, we list the web site privacy enhancing techniques, and how they could be applied in the post-payment system. In addition to the generic challenges of a typical Internet site or peer-to-peer network, the post-payment system has its own privacy and trust challenges. The web and online shop-related privacy challenges in the post-payment copyright system can be solved by utilizing the methods suggested above.

TABLE I. ONLINE SHOP AND WEB PRIVACY SOLUTIONS AND THEIR APPLICATION IN POST-PAYMENT SYSTEM

Web site privacy solutions	**Application in post-payment copyright system**
Positive past experiences	Objective to meet the customer expectations
Design and operation of the site	Simple and reliable workflow on the site
Reputation of the site operator	Established site operator brands visible on the site
Presence of privacy statement	Use of privacy statement
Presence of a privacy seal	Not applied
Privacy laws	Finnish and EU privacy legislation
Pseudonymous users and user models	Possibility to use the service without giving personal information before actually paying for the content.
Client-side personalization	Not used in the beginning
Privacy-enhancing techniques for collaborative filtering	Web analytics tools, which have privacy enhancing techniques

In this paper, we study the digital music business from the perspective of copyright owners. According to our analysis, the post-payment copyright system is potentially a more profitable business than the online shop when no media replacement is required.

Our paper is structured in a following way: Section 2 portrays the post-payment copyright system; Section 3 describes our qualitative business modeling, quantitative techno-economic modeling, and privacy threat analysis methods; Section 4 presents our scenarios; Section 5 contains our results; and Section 6 discusses our findings.

II. POST-PAYMENT COPYRIGHT SYSTEM

The post-payment copyright system allows the user to pay the copyright fees of illegally copied files. The system was introduced by Kokkinen et al. [12], and it is described here in more detail.

In the system, the payment process and distributing the copyright fees to the rights holders are similar to the respective functions of an online music shop. After creating the shopping basket, the user is directed to a payment page. Depending on the payment method, the user interface for typing in the payment details may belong to an online shop or to a financial institute. Typically, credit card information is given through the online shop user interface and bank account information through the financial institute interface. The details of the shopping basket are not visible to the financial institution and the online shop does not know the specifics of the payment arrangement. A transaction identification code ties together the operations in these two systems.

The payments for the rights holders are regulated by the legislation and signed contracts between the online shop operator and the rights holders. In most jurisdictions a value added tax is reported and paid to the tax authorities. Artists, composers, writers, technicians, and other people involved typically get their share through record labels and copyright organizations. The contracts between the online shop and these organizations define the method and amount of payments for the rights holders.

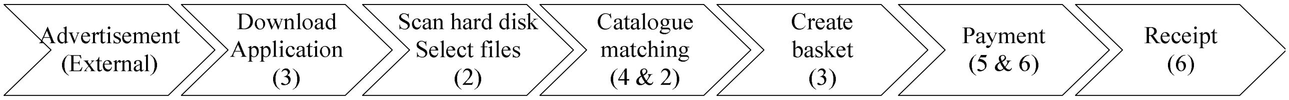

Figure 2. Post-payment copyright process

The architecture of an online music shop is similar to that of a post-payment copyright system; see Fig. 1 for component numbering. Rights holder (7), back-end (6), payment (5) and consumer (1) are identical. The web front-end (3) and user device (2) are present in both architectures, but their functionality differs from each other. The catalogue matching server (4) is unique to the post-payment copyright system.

We use corresponding numbering to describe the components involved in the post-payment copyright process, see Fig. 2. Compared to online music shops, the post-payment copyright specific part takes place prior forming the shopping basket.

Consumers are made aware of the post-payment copyright site through advertising. A consumer enters the post-payment copyright site and downloads an application, which is used to scan user’s hard disk. The application helps the user in selecting the files for legalizing. This phase consists of classifying the illegal and legal files, creating a shopping basket, and matching the selected files to the titles in the music catalogue of the system provider. The music catalogue is a list of tracks and albums, which are available in the service.

With the user device and the user application, the consumer can access the storage where the user has content files. The user application scans the device for illegal files and stores the information locally. The user application helps the user to select the relevant files. With the user client it is possible to access the services on the web front-end and on the payment system, although also a web browser interface is needed as a part of the process. The client communicates with the catalogue matching server and allows the consumer to operate the system through the user interface.

The web front-end provides the user with information about the service and the capability to download the required client. The web-front end manages the transfer of the content catalogue from the back-end to the catalogue matching server. The transfer requirement is due to an organizational setup. The web front-end manages the contents of the shopping baskets.

For an overview of the privacy related issues of the system components, see Table 2. For using the web front-end, the user does not need to provide an authentication, i.e., the user can interact with the service in a pseudonymous fashion. The only personal information that the user has to provide to the service is an email address as contact information. The contact information is cryptographically embedded in the purchase receipt, and its purpose is to discourage users from copying and redistributing fake licenses to other users. The user address in the receipt can not be forged without making the forgery detectable and invalidating the receipt.

TABLE II. PRIVACY RISKS OF THE SYSTEM COMPONENTS

System component	Required private information	User identifi-cation	Re-identification risks
Front-end and back-end	User contact address and list of content in shopping basket	Pseudonym	User's contact information is available as long as it has not been deleted
Catalogue matching server	Illegal and legal content in user's possession	Anonymous	User's IP address can be tracked
Payment system	Payment information, possibly including user identification	Payment information	Linking of payment information to actual user identification

The catalogue matching server matches the user file information with the music catalogue items. When there is a mismatch between the user file information and the catalogue, the catalogue server returns one or more closest matching items from the catalogue. Respectively, when there is more than one match in the catalogue, the matching server returns all matches. Catalogue matching server collects only statistical data about the matching requests. Individual catalog matching requests are anonymous and no private information is stored on the catalogue matching server. The requester can only be identified based on the source IP address of the device. However, the catalogue matching server does not track source IP addresses. It only collects statistical information about the incoming requests.

The payment server has a commercial online payment security level. The user can pay with major credit cards, online bank, and a selection of micro-payment systems. The payment system collects all data that are required for the payment and stores them as long as legislation requires. The payment system does not store information about the contents of the shopping basket but only the transaction identification codes. Linking of payments to shopping carts happens via transaction identifiers and only the back-end server has access to the actual shopping cart information. The payment system has the most specific information about the user in the whole system, since the user has to provide payment information in order to fulfill the payment process. The payment information typically consists of credit card information. The payment information may include information that identifies the user.

The back-end system maintains the catalogue by communicating with the rights holders. It sets the prices of the catalogue items based on the rights owner price, value added tax, payment method, and the target margin of the service. The back-end system maintains records of the payments. It may have a username database, and it stores the information about the shopping basket, payment, and the username. The back-end does not contain any information about illegal files. The purchase information and the related personal information are kept as long as the legislation requires. Currently, the retention period in the book-keeping legislation is six years in Finland. However, no direct link to the user identity exists.

Before issuing a receipt, the back-end communicates with the payment service to make sure that the payment has been completed. Each paid basket is assigned a transaction identification code, which is used to link basket information to payments in the payment system. The only personal information required by the service is the email address of the user. It is used to send the payment receipt to the user by email. The receipts issued by the system also include the email address of the user in order to reduce the temptation to copy and resell the receipt to other users, i.e., to gain financial benefit by selling fake authorizations. The user email addresses are deleted in the back-end daily.

In the post-payment copyright system model, the rights holders are customers of the system. The music right holders include record labels, and copyright organizations representing the rights of the artists. Tax authorities belong to the rights holder category from the system point of view. The rights holders receive periodically a share of the user payments. The content owners cannot track personal payments in the system without consulting the post-payment service provider.

III. Methods

A. *Qualitative Business Modeling*

The STOF framework for business model evaluation by Bouwman et al. [2] consists of four domains: Service, Technology, Organization, and Finance. A business model outline based on the four domains is evaluated based on Critical Design Issues (CDIs) and Critical Success Factors (CSFs). Finally, after internal and external issues are taken into account, a viable and feasible business model design should have been reached. Together these steps form the STOF method of business model evaluation, see [5] for an elaboration.

In the following paragraphs we summarize the discussion of Bouwman et al. [3] on the four domains of the STOF framework. Value is the main component of the service domain in the STOF model. Value is further divided into intended and delivered value for the provider, and expected and perceived value for a customer. Service domain has additional components. Context encompasses both concrete situations and larger socio-cultural aspects of the usage environment of the service, and co-determines perceived value of the service. Tariff is the price paid for the service, and effort is made by a customer to use the service, both affecting perceived value of the service. Bundling of services generally increases perceived value of the service. Security can be an essential co-determinant in the value of the service.

The Technology domain focuses on technical architecture, which is used to deliver technical functionality. The technical architecture consists of applications, devices, service platforms, access networks, and backbone infrastructure. All these generate costs and affect the delivered value of the service. Intended value in turn puts requirements on the technical architecture and the value network behind the service. Security is generally a cost item.

The main component in the Organization domain is the value network, which consists of several actors and their interactions. Actors have strategies, goals, resources, and capabilities. They perform value activities which together with organizational arrangements are combined into roles. The organizational arrangements affect both interactions and financial arrangements of the actors. Value activities sett requirements on the technical architecture, and generate investment sources, costs, and delivered value. Security aspects can be included in the strategy of an actor.

The Finance domain determines pricing of the service. It consists of four sources which generate capital, costs, revenues, and risk.

Each domain has Critical Design Issues; see Bouwman et al. [4] for a detailed discussion on them. The Service domain has the following CDIs: targeting, creating value elements, branding and customer retention. The Technology domain CDIs include security, quality of service, system integration, accessibility for customers, and management of user profiles. The Organization domain consists of partner selection, network openness, network governance and network complexity. The Finance domain incorporates pricing, division of investments, division of costs and revenues, and valuation of contributions and benefits. Security aspects affect most CDIs.

Critical Success Factors exist for both customer and network value creation; see Bouwman et al. [4] for an elaborated discussion on them. The CSFs for creating customer value consist of clearly defined target group, compelling value proposition, unobtrusive customer retention, and an acceptable quality of service. The CSFs for creating network value include acceptable profitability, acceptable risks, sustainable network strategy and an acceptable division of roles. Reaching high scores on CSFs in both categories is expected to result in a service capable of generating both customer and network value, i.e., a service capable of meeting user expectations and motivating actor participation. Again, security aspects affect most CSFs.

B. *Quantitative Techno-Economic Modeling*

Our techno-economic model is depicted in Fig. 3. We calculate net present value (NPV) with revenues, operational expenditure (OPEX) and capital expenditure (CAPEX), tax percentage, and discount rate as inputs. *NPV* is defined as

$$NPV = \sum_{t=1}^{n} \frac{C_t}{(1+r)^t}\,, \qquad (1)$$

where t is the time of the cash flow, r is the discount rate and C_t is the net cash flow at time t. The cash flow is calculated by subtracting OPEX, CAPEX, and tax from revenues:

$$C_t = \sum_i R_i - C_{EX} - r_{tax} (\sum_i R_i - C_{EX}), \quad (2)$$

where C_{EX} is the sum of OPEX and CAPEX, and r_{tax} is the tax percentage.

The revenues R_i for product i are calculated by multiplying the following factors: number of product i purchased by one user n_i, the price p_i per product i, content legalization percentage, i.e., the percentage of content available to legalization, r_{CL}, and the number of users n_U. Value-added tax (VAT) and reimbursements after VAT to copyright holders and to users based on respective multipliers r_{VAT}, r_{RCH} and r_{RU} are deducted from revenues:

$$R_i = n_i p_i r_{CL} n_U \cdot \frac{1 - r_{RCH} - r_{RU}}{1 + r_{VAT}}. \quad (3)$$

The number of users n_U is calculated by multiplying the total population n by illegal downloading r_{ID}, broadband connectivity r_{BC}, market interest r_{MI}, and market penetration r_{MP} rates:

$$n_U = n r_{ID} r_{BC} r_{MI} r_{MP}. \quad (4)$$

The OPEX C_{OPEX} consists of content delivery network (CDN), user support, and marketing C_M costs:

$$C_{OPEX} = \frac{r_{PH} T \cdot 8}{3600} \mathrm{C}_{\mathrm{Mbps}} + C_F + C_{SR} n_{SR} + C_M. \quad (5)$$

The CDN cost has two elements: cost of a megabit per second (Mbps) C_{Mbps} and fixed cost C_F. The Mbps requirement is a multiplication of the total traffic T in MB and a peak hour load percentage r_{PH}. An even distribution of traffic during the peak hour is assumed. The user support is calculated by multiplying the cost per support request (SR) C_{SR} by the number of SRs n_{SR}.

The CAPEX C_{CAPEX} is a sum of person months (PMs) for both contract negotiation (CN) and software (SW) development & maintenance:

$$C_{CAPEX} = n_{CN} C_{CN} + n_{SW} C_{SW}. \quad (6)$$

Security aspects influence both OPEX and CAPEX, but due to the scope of our techno-economic model, they are only implicitly included.

We also carry out risk analysis by running Monte Carlo simulations. In a Monte Carlo simulation, uncertain variables are assigned random values according to predefined distributions. The simulation is repeated for thousands of trials. The impact on the results of the calculations is recorded for each trial. Based on the records, several statistical variables can be calculated. The statistical variables can then be used to assess the risk related to each scenario.

We perform the risk analysis with 100,000 trials for each scenario. The selected uncertain variables are assigned triangular distributions with expected, minimum and maximum values corresponding to mode, lower limit, and upper limit of the distribution, respectively.

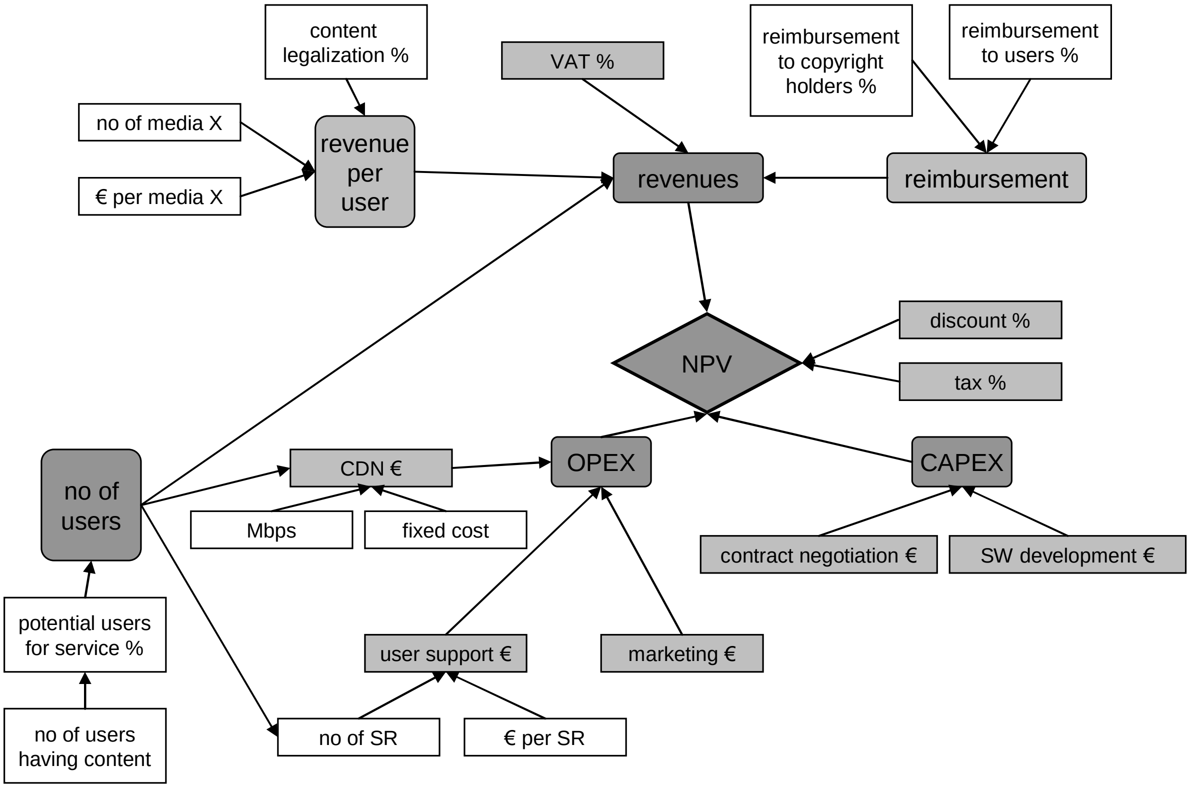

Figure 3. Quantitative techno-economic model for scenario comparison

C. *Privacy Threat Analysis*

To assess the privacy risks facing the users of the post-payment copyright system, we perform a threat analysis of identified key elements in the system. Threat analysis is an important part in security engineering and it forms the basis for the security design of the system [39]. For the threat analysis we form an attack tree as introduced by Schneier [40] covering possible attacks against the privacy of user's data. In our threat analysis, we consider following information items to be of special relevance to the post-payment copyright system: user identity, user contact information, information about the illegal content of the user, and the list of content paid with the post-payment copyright system.

The main goal for attacks, which we assume in our analysis, is to obtain potentially incriminating information about the user. The threats are considered to be related to illegal combining of user records in different parts of the post-payment copyright system, or to the threats introduced by direct external eavesdropping and active intrusion into system components. The attack tree used in our analysis is shown in Fig. 4.

IV. SCENARIOS

We compare three different online media rights purchase systems. They are an online media shop (A), a post-payment copyright system where the user's downloaded files are replaced with new files (B), and a post-payment copyright system where only immaterial rights are purchased by the user but existing files remain untouched (C).

The consumer price per content item is the same in all three cases. The rights for a song in the post-payment system cost exactly as much as the same song in an online music shop. Also, the reimbursement to the content owners is the same in all three cases.

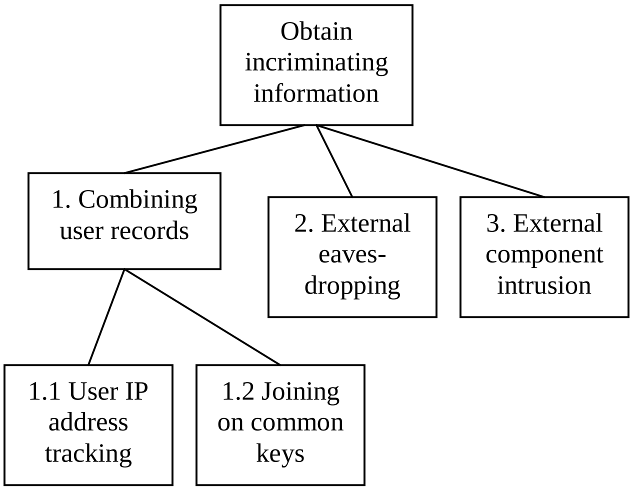
Obtain incriminating information
1. Combining user records
2. External eaves-dropping
3. External component intrusion
1.1 User IP address tracking
1.2 Joining on common keys

Figure 4. Attack tree identifying privacy threats against the post-payment copyright system

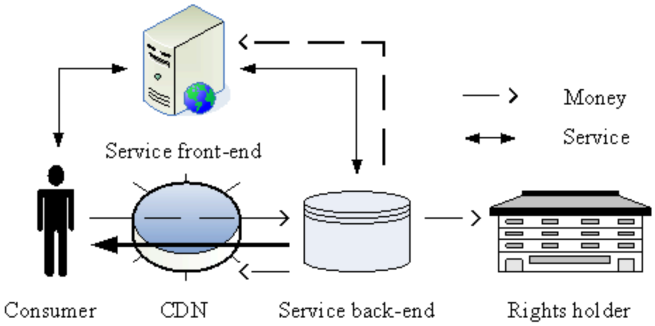

Figure 5. Online shop model

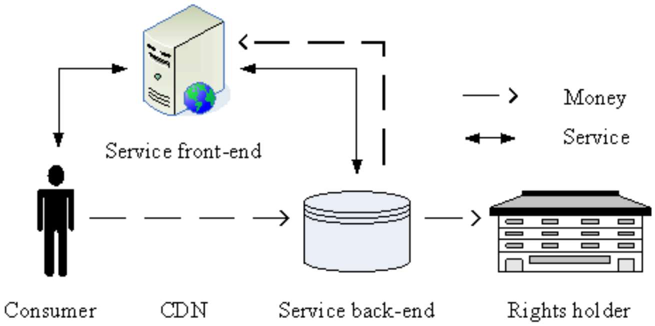

Figure 6. Post-payment copyright model

In the online shop model (see Fig. 5) the media companies and organizations representing artists are called rights holders. The service back-end company makes a distribution contract with the rights holder. The back-end service provider acquires the files, delivers them to the consumer and handles the payment of the user. The service visible for the consumer is provided by the service front-end. The service front-end is a web site marketing the service and building consumer's shopping cart. The service back-end provider uses a CDN to ensure a satisfactory content download service for the consumer.

The post-payment copyright system, where the files are replaced with new files, does not differ from the online music shop model. The post-payment part of the service is just a marketing tool for the content in the service back-end.

In the post-payment copyright system (see Fig. 6) no files are distributed. The service legalizes the unauthorized files on user's hard disks and memory cards. The service front-end handles the rights shopping cart for the user and the service back-end distributes the copyright fees to the rights holders.

The basic differences of the three scenarios compared are based on the market size and delivery cost differences depicted in Table 3. The online shop has all users of the potential market; post-payment variants have only the past users of illegal file sharing systems. The delivery and storage costs are considerable for both online shop and post-payment with file download. In practice the post-payment download services have the market potential of the online shop, but in this simplified comparison we study only the potential of the post-payment download feature.

TABLE III. COMPARISON OF THE SCENARIOS

Scenario	Market size	Delivery cost
Online shop (A)	Full	Full
Post-payment download (B)	P2P users	Full
Post-payment (C)	P2P users	Nominal

CDN adds additional security considerations and cost to the scenarios A and B. Additional cost related to security considerations is also present in contract negotiations, software development and user support for the post-payment scenarios B and C.

We use Finland in 2009-2013 as a case for our study. We use the population n of Finland in 2006 (5,276,955) as a basis for our population calculations and assume a 0.4% annual growth [41]. Table 4 summarizes the annual usage input values for our scenarios. In all scenarios, the initial value for the broadband connectivity r_{BC} is 53% in 2006 [42] which is extrapolated using a simple logistic saturation function with a saturation value of 65%.

In the scenarios B and C, the illegal downloading r_{ID} vector is an estimate based on [15]; the market interest r_{MI} is assumed to be a constant 20% based on [15]; the market penetration r_{MP} and its distribution into different user groups are hypothetical; and the penetration of a fourth user group "long tail small" is calculated by subtracting the other user group penetrations from 100%.

In the scenario A, r_{ID} is 100% every year because it is not relevant to the calculation of usage; an estimate of 15% in 2007 [43] with 16% annual growth [44] is used as a basis for r_{MI}; r_{MP} is hypothetical; and no user group distribution is used: only "long tail small" user group is in use.

We use only one product category: song with a price of €0.99 including VAT. A "parent," a "heavy user," a "long tail large" customer and a "long tail small" customer purchase annually 250, 500, 400 and 50 songs, respectively. In scenario A, a user buys annually 50 songs. Content legalization r_{CL} vectors are depicted in Table 5. In the scenario A, r_{CL} is 100%. Users are reimbursed (r_{RU}) 5% of their total purchases in the scenarios B and C, 0% in the scenario A. VAT r_{VAT} is 22% and reimbursement to copyright holders r_{RCH} is 80% in all the scenarios.

We use the following values for the calculation of OPEX. For the CDN cost, a base transfer of 10 MB per user is assumed in the scenarios B and C, 5 MB in the scenario A. In the scenarios A and B, a song transfer generates 5 MB of traffic. In the scenario C, each item generates only 1 kB of traffic (i.e., a transfer of a checksum). The peak hour load r_{PH} is 0.05% of total traffic assuming a 95th-to-mean ratio of 4:1 [45] in all the scenarios. In the scenarios A and B, the data transfer capacity cost C_{Mbps} is €5±0.5 per Mbps and the fixed cost C_F is €24,000±2,400 annually. In the scenario C, the prices are €1,000±100 and €8,000±800, respectively. The data transfer costs decrease annually by 5±0.5% in all the scenarios. For calculating the user support costs, we assume a fixed cost per SR C_{SR}: €5±0.5 in all the scenarios with an annual growth of 5±0.5%. In the scenario B and C, a parent generates 0.6 SRs annually, a heavy user and a long tail large user 0.4 SRs annually, and a long tail small user 0.2 SRs annually. In the scenario A, a user generates 0.2 SRs annually. The post-payment system is more complex, thus generating more SRs. Fixed marketing costs C_M are €50,000±5,000 in all the scenarios in 2009. In the scenario A they decrease by €3,000±300 annually; in the scenarios B and C by €10,000±1,000 annually. The difference in the marketing costs is based on the assumption that the online shop is marketed to a broad audience, whereas the post-payment systems are marketed to a limited audience. We estimate the catalogue matching costs in the scenarios B and C to be marginal; therefore they are not included in our calculations.

PMs for calculating CAPEX are depicted in Table 6. Regarding the cost of a PM, C_{SW} is €10,400±1,040 and C_{CN} is €20,800±2,080. Both have an annual growth rate of 5±0.5%. We assume the online shop is less complex to develop and deploy due to several existing solutions. The tax rate r_{tax} is 26% and the discount rate r is 10% in all the scenarios.

V. RESULTS

A. *Qualitative Business Modeling*

The dynamic business model framework in STOF has three phases, and each of them includes a STOF analysis. The phases are Technology R&D, Roll-out and Market. In this paper we analyze the Technology R&D phase empirically based on the literature presented in previous Sections of this paper. The business model is discussed from the post-payment copyright system operator point of view.

TABLE IV. ANNUAL USAGE INPUT VALUES (%)

	2009	2010	2011	2012	2013
r_{ID}	40±10	45±10	47.5±10	45±10	42.5±10
r_{BC}	55.4	59.9	62.1	63.3	64.0
r_{MI}[a]	20	23	27	32	37
r_{MP}	0	4.5±2.5	7±2.5	10±2.5	12±2.5
r_{MP}[a]	0	5±2.5	7.5±2.5	12.5±2.5	15±2.5
parent[b]	80±5	70±5	60±5	40±5	20±5
heavy user[b]	1±0.5	2±0.5	3±0.5	2±0.5	1±0.5
long tail large[b]	10±2.5	15±2.5	13±2.5	11±2.5	8±2.5

a. in the online shop scenario (A)

b. not in use in the online shop scenario (A)

TABLE V. CONTENT LEGALIZATION R_{CL} VECTORS (%)

	2009	2010	2011	2012	2013
parent	70± 10	74± 10	78± 10	82± 10	86± 10
heavy user	60± 10	62± 10	64± 10	66± 10	68± 10
long tail[a]	40±5	41±5	42±5	43±5	44±5

a. applies to both "long tail large" and "long tail small" user groups

TABLE VI. PERSON MONTH VECTORS

	2009	2010	2011	2012	2013
n_{SW}	24±3	3	1	1	1
n_{SW}[a]	8±1	3	1	1	1
n_{CN}	6±1	2	1	0.5	0.5
n_{CN}[a]	3±0.5	2	1	0.5	0.5

a. in the online shop scenario (A)

1) Service, Technology, Organization and Finance

The Service is the post-payment copyright service, which is discussed in detail in Section 2 of this paper. In the service the user can legalize the earlier illegally copied music files. In the early phase of deployment, the target customer group is Finnish peer-to-peer file sharing users. Most of them are males in the age group of 25-35 [15]. The value for the customer is that they can legalize the illegal music files, to which they listen a lot. The availability of Digital Rights Management free (DRM-free) online music is still very limited in Finland, and the service may attract consumers who prefer DRM-free music files.

The most of the Technology in the system is available in the existing online music shops. The technical architecture is described in Section 2 of this paper. The new technology in the system includes an algorithm to analyze illegal vs. legal status of the user files, catalogue matching server and user client. The user client integrates different system and service components together to form a smooth and compelling user experience. The illegal vs. legal music file classification may have serious legal consequences. Considering the early stage of the technology, the feature is introduced to consumers rather as a tool to help them to select the files they may want to legalize than to prove if the file is from an illegal or a legal source. The catalogue matching is also a critical component. The user payments are made according to the catalogue matches, not according to the real user files. The catalogue matching results are shown to the user and the user accepts to pay for the matching results, not for the music files. It is a considerable challenge to get correct matches from the multitude of music file descriptions to the limited coverage of the music catalogue.

The current state of the music industry impacts on the Organizational setup strongly. The digitalization of media, multimedia computers, and broadband connectivity has lead to a strong trend of illegal downloading and copying. The music industry continuously searches for new models for revenue and profit. At the same time they make effort to get publicity for the copyright issues in order to decrease the impact of illegal copying. From this perspective the rights holders, i.e., record companies and copyright organizations, have research interests in post-payment copyright system in addition to direct revenue and profit. For the existing online shops the incremental effort to take the post-payment copyright system into use is relatively small, and it opens the potential market of legalizing illegally copied media.

However, organizing the different actors into a viable value network is challenging. Users do not have strong incentives to legalize their content unless there is strong legislative pressure for it. Even though copyright legislation has developed partially according to the lobbying of the music industry, consumer rights advocates and the proponents of freedom in the digital domain are resisting with increasing force the sanctions of copyright infringements done by consumers. On the other hand, new actors to the digital media industry are establishing new business models where the ultimate goal is to possess the leading platform for digital media distribution. The new actors include both device manufacturers with their own distribution platforms (e.g., Apple iTunes and Nokia Comes with Music) and independent distribution platform providers (e.g., Amazon and Spotify). The role of devices and distribution platforms as part of digital music experience is under constant change and subject to re-definition.

The Finance of the business model is very similar to the online music shop business model. Artists, composers and technicians have contracts with record labels and copyright organizations. The back-end system provider has contracts with record labels and copyright organizations to pay them a certain portion of the consumer price. The back-end provider has a contract with financial institutions to enable payments in exchange for a fee.

The post-payment system operator has a similar role as the web front-end in the online music shop white label business model. It concentrates on the marketing of the service and operates as a reseller, whereas the back-end system provider acts like a wholesales organization. The consumer is the customer paying for the service. More indirect revenue models also exist: capitalizing on the copyright campaign nature of the service, reselling the information about consumer music preferences, and advertising in various parts of the system, but they are not evaluated in this paper.

2) Critical Design Issues

The first Critical Design Issue is targeting by making the choice between the business to consumer (B2C) and business to business (B2B) models. In B2C the post-payment service provider markets the service to consumers and receives payments from them. In the B2B model the post-payment service provider offers the service to rights holders or to an existing online music shop. In first service trials the model must be B2C, but when the service establishes itself on the market, dedicated B2B post-payment service providers are to be expected.

In creating value elements for the basic post payment copyright, the system can be enhanced by providing access to high quality music files, album art, and song lyrics. An important issue in the value context is Digital Rights Management (DRM). In some cases a file without DRM is of higher value to a consumer, even when its source is illegal, compared to a commercial legal file with DRM.

The service branding is closely related to the choice between the B2B and B2C options. The possible branding alternatives include own branding, use of an existing online music shop brand, or a connection to a rights holder brand, e.g., a brand of a record label or a copyright agency.

The customer retention of a post-payment copyright system to an online music shop can be arranged so that the user account or the payment information of the post-payment copyright system is bundled with the online music shop. The customer retention to the post-payment copyright system itself can be obtained through personalization: the system can store the user classification of files to be legalized, being legal, being illegal, among other possibilities.

The security of the post-payment copyright system has two distinctive parts. The information related to payment has very high security requirements which are met by established solutions. The unique security challenge in the system is privacy. The personal information in the system basically describes evidence for copyright law violation. The collection, communication and storage of the personal information must be well understood both by the operator and the consumer. Generally, it is an advantage if the communication is transparent and it is possible for an advanced user to check if the communication contains only the promised information. On the other hand, unencrypted transfers are prone to eavesdropping, so the data sent should be protected by encryption.

The quality of service consists of the time needed for downloading the application, scanning the hard disk, analyzing the legal status of files, and the catalogue matching. From the privacy point of view it would be beneficial to carry out the catalogue matching in the user application, but it would increase the download time dramatically. In this respect the quality of service consideration exceeds the privacy concern. In order to improve the time consumed at each phase of the process it is possible to develop algorithms which optimize the time used for processing while maintaining the accuracy of the results.

In the early phase when the market is building up, system integration to several other systems may not seem relevant. But especially in the B2C model the possibility to integrate the system to various online backend systems is crucial. A generic modular structure and well defined simple interfaces using common technology components decrease the time needed for individual system integration projects.

The user application providing the best accessibility for customers is web browser. On the other hand, the web browser is not allowed to get full access to the computer where it is running. Plug-ins like Java script engine and Adobe Flash player are a compromise between the full access rights on the local computer and the need to download and run an application. The latest plug-in technology versions normally have the most advanced feature sets and include many functions, which can speed up the development phase, but the support for them may not be available on all common computing platforms.

Management of user profiles gives the possibility for service personalization, but they also create a difficult situation for the service provider. The service provider has knowledge of the copyright violation of the user, and access to the user account which can link to the real personality of the user. In many jurisdictions police may force the service provider to reveal such information to copyright authorities. In order to avoid such procedures it may be preferable for the service provider not to have user accounts even if the absence of them decreases the possibility for service personalization and customer retention.

When considering the partner selection, the added value of the service provider is related to the contribution it makes for the value network. In one extreme the rights holder could run the post-payment copyright service bundled with its own online music shop. In the early phase it might be useful to have a number of partners, which are specialized in certain parts of the value chain, at least in order to learn how those parts of the value chain typically operate. Having partners enables the service provider to concentrate on the novel parts of the system where it most likely can add significant value.

Concerning network openness, network governance and network complexity, a balance between the network growth and control of the network has to be maintained. The post-payment copyright value network has generally better possibilities to grow uncontrolled, but for the post-payment system operator and for the early players, the uncontrolled growth may lead to lost opportunities and lost market share. A realistic and attractive business case could be to specialize in one part of the system when the value network has potential to grow. The specialization could be providing the post-payment system as a back-end service for existing online music shops, delivering catalogue matching system or user application. Also licensing, consulting and system integration services for the entrants can be considered.

Pricing is probably the most important factor for any product. In the post-payment copyright system, the reference price point is the price of a piece of music in an online music shop. As the system does not need to distribute copies of a file, a lower price point could be justified. On the other hand, the system provides a substitute product for the online music shops and it would not be logical to allow very different price points for substituting product formats. Special pricing according to the quantities should at least be considered so that the system would encourage the users to legalize as many files as possible.

The division of investments for the system includes the development of the system and marketing efforts. Our assumption is that these costs are shared by the rights holder, the online music shop providing the contracts and the back-end system, and the post-payment copyright system provider. The development costs are most naturally carried by the post-payment copyright system provider, because the service is its own initiative. The marketing costs should be shared more evenly.

The post-payment copyright business contracts define the division of costs and earnings. The post-payment system operator may not be able to include all its development costs into new contracts, but at least the amount it would cost for a new player to develop the same system can be taken into account. Basically the same applies for the contribution of the other partners as well.

In the contract negotiations between the partners probably the most important issue is how the valuation of contributions and benefits is carried out. A joint venture can be created where the partners are investors, or more typically each link in the value chain forms a customer – service provider relationship. Each link can be negotiated as a fixed fee, transaction based revenue sharing, or a combination of them.

3) *Critical Success Factors*

Several Critical Success Factors are not positive by default in the service. The compelling value proposition to the customer depends on the viewpoint. On the other hand, no other way to legalize illegal downloads exists in most markets. But as the consumer already has the music file and does not get any concrete value by paying for it after obtaining it, the value proposition is not strong.

The clearly defined target customer group consists of users who have downloaded and copied music illegally in the past, and of the parents of children who have illegal copies of music files. The target groups are rather well defined, although convincing them to use the service is very challenging.

While a compelling value proposition is not strongly present, the value analysis of the service design provides additional insight to the case. The intended value for the end-user customer is the possibility to legalize illegal copies of music files. This gives a covenant not to sue protection to the customer. The delivered value depends on the contracts between the service provider and the rights holders. We can expect that the contracts are professionally made and the jurisdiction has the concept of covenant not to sue, or the freedom of the contract prevails, so that the delivered value matches well to the intended value. The expected value is a more challenging aspect. In most services, the user gets something when he pays money for the service. In the case of a post-payment service, the user gets a receipt. The receipt may not be tangible enough to drive the user to make a purchase decision. Additional material like CD covers, track lyrics, or other material about the artist could improve the perceived value for the customer. On the other hand, the music file to be legalized is known by the consumer. He knows the content, how much he listens to the file, what is the coding quality is, and in which devices the file can be played. Hence, the perceived value of the content equals to the delivered value in the post-payment copyright system.

Unobtrusive customer retention is a challenging aspect. The core offering is to give a unique opportunity to legalize illegal downloads. Furthermore, the user is encouraged to use legal music shops instead of illegal means. From this perspective, customer retention is realized only when the user legalizes just a part of the illegal files in possession when the service is used for the first time. Another possibility for customer retention is that the service is bundled with an online music shop, and customers accessing the music shop are considered as a part of the overall customer retention.

The acceptable quality of service is guaranteed in the web front-end and the payment services, as they follow industry standards. The specific areas to develop the quality of service are illegal vs. legal file recognition and music catalogue matching. Illegal file classification is a recent area of forensics, and major improvements can still be expected. The implementation of the catalogue matching is a trade-off between accuracy, number of methods in use, and resources. The accuracy can be improved by adding more methods for matching. For example, fingerprint recognition can be used in addition to metadata analysis. The accuracy of a method can be increased by adding execution cycles, i.e., increasing the number of times the method is applied. Additional methods require increased development resources. Running methods in parallel and increasing execution cycles require processing resources.

The acceptable profitability of the post-payment copyright service is quantitatively analyzed in Section 5.2.

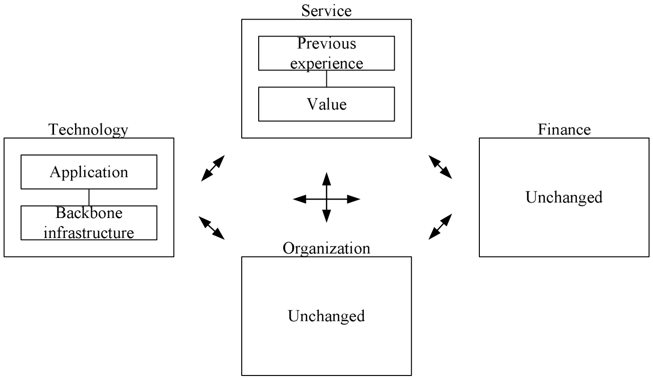

Figure 7. Differences in post-payment system and online music shop STOF models

The acceptable risks are gained by re-using the existing technology assets of the partners. The main investments in the beginning are related to client development, catalogue matching server development, and marketing. In this analysis, we expect that the development risk is taken by the post-payment system operator, and the marketing risk is shared between the participating organizations.

The sustainable network strategy has a good basis, because for all others except for the post-payment system operator, the service is an extension in their current business operations. For most of the participating organizations in the value chain adding the new service does not require new technical development and could be described as “business as usual”.

The acceptable division of roles is achieved by having the same roles as in the online music shop value chain. The roles follow industry standards, and the same applies for the profitability and risk. Post-payment system providers have potential to negotiate better contract terms than online music shop providers due to the advantages of the post-payment copyright system, including the opportunity to increase consumers’ moral regarding copyright.

4) *Differences in post-payment and online shop STOF models*

As part of the STOF analysis, we compare the Service, Technology, Organization, and Finance domain descriptive models of the post-payment copyright system and the online music shop. For both of them, the Organization and Finance domains are similar according to our analysis. The differences are visible in the Service and Technology domains, see Fig 7.

In the Service domain, the customer most likely has previous experience of online music. For the post-payment system only the payment experience exists. The post-payment copyright experience is new for the customer. The customer does not know how long scanning, or catalogue matching takes. Also, the accuracy of matching and illegal vs. legal classification is without earlier references. The intended value of the online music shop is that the user is able to listen to the purchased music file. The perceived value of the DRM protected content can be lower, if the customer would like to play the files in a device without the DRM client of the online music shop. In the post-payment system, the content itself is well know by the customer, as it is already in her possession, but due to that the delivered value of the system is abstract rather than practical.

In the Technology domain the payment and customer data platforms are similar in both online shop and post-payment systems. The main differences are in the client and in the backbone infrastructure. The online music shop client has a download feature, and often it also has its own music player with the DRM client installed. The post-payment system client includes the scanning and illegal vs. legal classification but no download or player features. The main difference in the network components is the catalogue matching service existing only in the post-payment copyright system.

B. Quantitative Techno-Economic Modeling

With the base case parameters, the scenario A produces total revenue of €1.49 million and the scenarios B and C €1.43 million. Therefore, the scenarios are at a comparable revenue level. The online shop scenario (A) has a linear revenue curve, whereas the post-payment scenarios (B and C) have a peak curve.

Table 7 depicts the results of break-even analysis in the base cases. The break-even point is reached when NPV is zero. The break-even market penetration rate $r^{MP}_{B\text{-}E}$ in the table is defined as the number of users in the break-even situation. It is calculated as the number of users n_U multiplied by a break-even multiplier $r_{B\text{-}E}$, which is set so that NPV is zero divided by the number of potential users, i.e., the number of users n_U divided by market penetration rate r_{MP}:

$$r^{MP}_{B-E} = \frac{r_{B-E} n_U}{n_U / r_{MP}} = r_{B-E} r_{MP} \,. \tag{7}$$

The post-payment scenario (C) reaches the lowest break-even market penetration rates, followed by the post-payment download scenario (B). Thus, post-payment scenarios require less market penetration among potential users than the online shop scenario (A) to reach a break-even situation in the base case.

The results of the NPV analysis are depicted in Fig. 8. The first bars illustrate the mean values, whereas their error bars display the minimum and maximum values. The second bars are base values. The mean, minimum, and maximum values are calculated based on the risk analysis, whereas base values represent the results without risk analysis. The results clearly indicate that the post-payment scenario (C) is the most profitable and has mid-level risk, whereas the post-payment download scenario (B) is the least profitable and has the most risk.

According to our sensitivity analysis, the usage parameters have the largest effect on the outcome in all the scenarios. Because we did not perform extensive sensitivity analysis eliminating the effect of potential cross-correlations of variables, we do not present the results in detail.

Fig. 9 depicts the results of the cost analysis. Mean values and error bars are displayed. Reimbursement to copyright holders is the most significant cost item in all the scenarios. The other items are notably less substantial. The differences in scenario definitions are clearly visible in the cost structure of each scenario.

TABLE VII. BREAK-EVEN MARKET PENETRATION RATES $R^{MP}_{B\text{-}E}$ (%) IN THE BASE CASE SCENARIOS

Scenario	2009	2010	2011	2012	2013
A	0.0	4.4	6.6	11.0	13.3
B	0.0	4.2	6.6	9.4	11.3
C	0.0	3.9	6.1	8.7	10.4

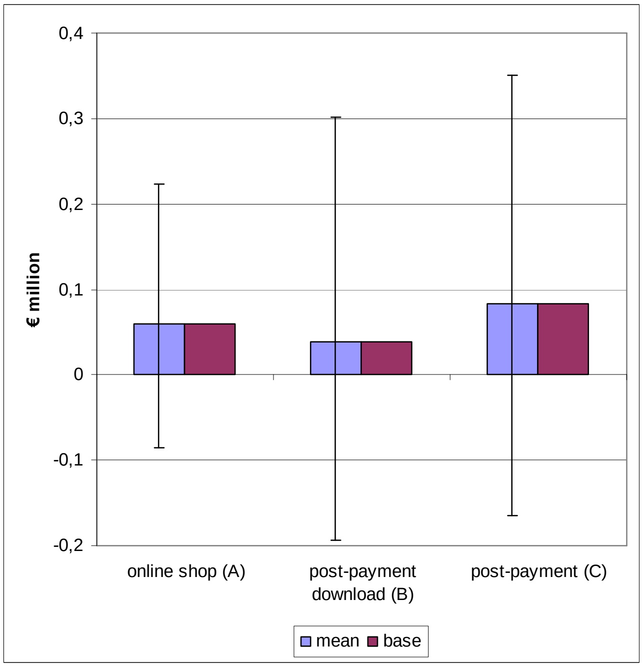

Figure 8. Results of NPV analysis

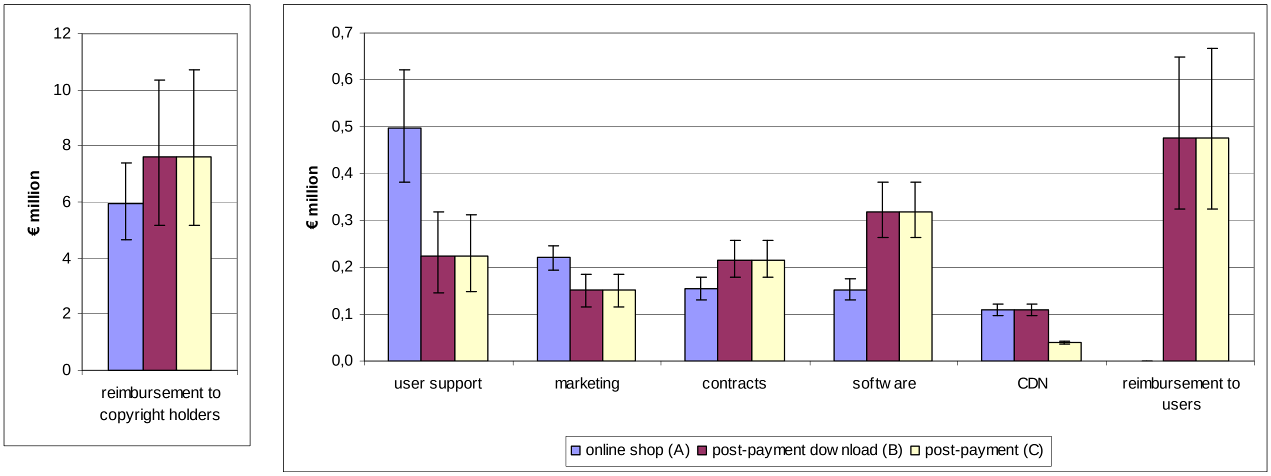

Figure 9. Results of cost analysis

C. Privacy Threat Analysis

In this section, we present the results of the attack tree method -based privacy threat analysis, see Fig. 4. We describe how the system provider can try to assure the user that private information is not compromised. For the success of the post-payment copyright system, it is particularly important that the users of the system can be confident that the user identity in combination with the list of illegal content in the user's possession does not leak out of the system. The goal of the privacy protection measures is to limit the privacy exposure of the users.

In our analysis, the threat class 1 *combining user records*, relates to the improper re-identification of the user and linking of data records between system components. The most critical re-identification risk is related to the requests to the catalogue matching server. If the requester is identified and the requests tracked, one can obtain an extensive list of potentially illegal content on the requester's device. That can obviously be incriminating evidence against the user. While the request protocol as such is based on anonymous operation, the source IP address of the requests still remains traceable. In some cases, the IP address may be linkable to a specific device. That can potentially reveal the requester's identity, described as *user IP address tracking*, threat class 1.1.

Even if the IP address cannot be traced back to a specific device or person, the IP address provides a potential key, based on which information between the system components could be linked. If the front-end and the catalogue matching server colluded by comparing the IP addresses of requests they serve, it would be possible to link the shopping cart information with the actual list of illegal content on the user's device. For a comparison of privacy risks arising from collusion of individual system components, see Table 8.

TABLE VIII. COLLUSION RISKS AGAINST USER PRIVACY

Collusion risks	**Worst-case privacy exposure**	**Colluding components**		
		Catalogue matching server	***Front-end and back-end***	***Payment system***
Linking of catalogue matching requests to purchase sessions based on IP address	User contact information + list of content to purchase licence for + list of illegal content in user's possession	X	X	
Linking of shopping cart information to payment information leading to full user identification	User identity + User contact information + list of content to purchase licence for		X	X
Linking of catalogue matching request to payment transactions based on IP addresses	User identity + list of illegal content in user's possession	X		X
Linking of catalogue matching requests to shopping carts and payment information leading to full privacy exposure	User identity + User contact information + list of content to purchase licence for + list of illegal content in user's possession	X	X	X

Even when there is no malicious intent against the users in the system itself, there are external privacy threats. They are related to the user information that external attackers can get by eavesdropping. The external communication threats are threat class 2 *external eavesdropping* of unprotected user communications, and threat class 3 *external component intrusion*. Note that also law enforcement officials using a search warrant can be regarded as such external attackers against the users' privacy. Once an intrusion happens, the intruder can of course learn user information, which is hosted on the system component. Increase in privacy exposure by combining this information to other data is much more challenging, as can be seen in Table 9.

From the privacy point of view, threats in class 2 related to eavesdropping are as problematic as the collusion threats in class 1 *combining user records*. Unlimited eavesdropping on the system communications would enable an external attacker to know the same information as the system components. However, as all communications between the user’s device and the system are protected by using encryption, we estimate that the probability of successful eavesdropping attacks against the user is very low. The eavesdropping will not impact users’ privacy perceptions so much that it would have a negative impact on the adoption of the post-payment copyright system.

After analyzing the threats, we present solutions for the recognized privacy threats of the post-payment copyright system. We also go through the tradeoffs of the selected solutions, see Table 10.

Distributing the user information in the system decreases the impact and risk of the threat class 1 *combining user records*. Storing payment information and receipt information is regulated by the legislation. The information is distributed in the system: backend provides clearing the payments for the rights holders; payment system operator handles the payment; and the service front-end operator works with the shopping basket. The distribution may decrease the consumer privacy concerns, as no one in the system has information about the user files, real identity, and credit card information. All these transactions can be collected and linked together for example in a copyright infringement claim investigation. If the user loses the receipt and likes to get another copy of the receipt, the distribution of the data makes the task more challenging.

Academic research is a valid reason to collect private and sensitive information in copyright legislation. At this state of the work, the post-payment copyright system is a research project. The research part is clearly separated from the commercial service, it has its own privacy statements, and the difference is clearly communicated to the user.

TABLE IX. PRIVACY EXPOSURE IN EXTERNAL INTRUSION THREATS

Linking scenarios	Privacy exposure
Linking of catalogue matching requests to purchase sessions	Linking cannot be done, since catalogue matching requests are anonymous and IP addresses are not tracked
Linking of shopping cart information to payment information leading to full user identification	Back-end cannot identify user, since payment system provides only information about the success of the transaction not about payment information
Linking of catalogue matching request to payment transactions	Linking is not possible since there is no linking key. IP addresses are not tracked.

TABLE X. PRIVACY SOLUTIONS, TRADEOFFS AND BENEFITS

Solution	Threat	Tradeoff	Benefit
Distributed architecture	1	More privacy statements, service agreements, and other legal documents. More complicated management of the system.	All information related to the user is not available at one point
Research data separated	1	More complicated data storage system. More complicated data structures in the research analysis.	Less private information stored long periods
No user accounts	1	Less possibilty for personalization of the service	Less information can be linked to a user
Anonymizing proxy	1.1	Service cannot use any information gained during the previous session. Research of data gets more difficult.	Extremely difficult to link any service use to the user
Encrypted communication	2	Difficult for user to verify the data sent to the network	No eavesdropping at intermediaries
Illegal vs. legal analysis at user device	1	The accuracy of analysis is decreased	The most sensitive information is not transmitted in the Internet or stored on the servers
Catalogue matching only for items which user considers paying	1	The only a coarse price of the music available in the client for all user files	Minimized personal data transfers from the device to the network
User data not stored	1.1	Tedious tracking of all purchase data afterwards at the service provider. No possibility for service personalization.	As little as possible personal data is stored in the system
Rights holders clearly visible	Adds trust	May raise worries about hidden agenda of the rights holders	Increases trust for the validity of the service

Storing information about the users' past illegal activities is naturally a very sensitive matter. It should be handled with similar care as the patient registers in health care. Collection of such information would be an attractive target for internal and external attacks, and it could potentially be interesting for authorities. From a user point of view, this would represent threats that could deter users from using the service in the first place. Therefore, we decided not to store any of the information that links a specific user to the illegal past actions. The result of with this decision is that we don’t have any user accounts on the web frontend. The user accounts could be used to help the user during the consecutive usage sessions and to provide a possibility for service personalization.

A commonly used method to protect against the threat class 1.1 *user IP tracking*, is that the service is used through an anonymizing proxy. If all system components maliciously collude against the user of the system, user privacy is compromised leading in the worst case to full exposure of the user's private information. This is clearly unacceptable for the users of the system. From the user point of view, the best improvement here would be that the users would apply an anonymizing proxy or an anonymizing network in all interactions with the system.

As a solution for the threat class 2 *external eavesdropping*, we apply encryption in all communication in the service. We use Secure Socket Layer (SSL) to decrease the concerns about potential eavesdropping or network monitoring by authorities. Also here, the selection of the encrypted communication is a privacy concern tradeoff. The positive impact is that the users need not to be so worried about their sensitive information being transmitted in clear text through the Internet. The negative side is that for people like civil liberties and web activists, who would really like to check what is communicated between the application and the servers, it is challenging to verify that the service provider promises about the communicated content match with reality.

The exposure to the threat class 1 *combining user records* is decreased by carrying out the illegal vs. legal analysis in the user device only. As a tradeoff of the client based analysis we lose the centralized analysis help in researching the accuracy of the analysis. The centralized analysis would also allow faster deployment of the improvements to the users. But as that information is the most sensitive in the system, the user privacy was selected as the dominating factor in the implementation.

An opposite tradeoff was accepted with the catalogue matching functionality. It is implemented on the network server. In this case, we therefore trade the privacy concern for a small application download size and for a more reliable catalogue matching in the system. The impact of the threat 1 combining user records with the selected architecture is decreased by carrying out the catalogue matching only for the items, which user considers paying, and by clearing all private data like IP addresses in the logs of the catalogue matching server. The threat class 2 *external eavesdropping* is made very difficult by encrypting all communication with the catalogue matching server. It is however to be noted that encryption alone cannot hide the fact that a specific source IP address has been in interaction with the catalogue matching server. Even this information might be considered incriminating. The alternative of the adopted solution would have been to download the entire catalog of available content to the user device and to perform the catalogue matching locally, thus minimizing the exposure of the user.

In addition to protecting the user against the negative privacy threats, we try to use a positive approach to improve the user trust in the post-payment system. The privacy concerns of the users are greatly diminished if they can consider the post-payment copyright service as a trusted third party that does not forward sensitive data to the rights holders. The challenge of the post-payment copyright service is to act as a reliable trusted third party between the users and the rights holders. The trusted third party should be credible in the users' perception and make the users willing to use the service.

Communication about the system plays a very important role. We build the system architecture and operating process to minimize privacy concerns. The consumers become aware of these solutions through communication. With successful communication about the selected solutions we can build trust in the consumers and lower their privacy concerns. Peer-to-peer is a very sensitive issue from the communication point of view. In the communication, it might be wise not to mention peer-to-peer as a source of illegal copies in order to avoid the wave of emotional bursts in the peer-to-peer user groups, leading to a decreased trust within other post-payment users.

Showing clearly which rights holders are behind the post-payment system builds trust in the consumer. It convinces the users that the service really delivers what it promises. At the same time, quite a few consumers may wonder if the rights holders have a hidden agenda in the service. The users might get increased privacy concerns about what data is really collected and to whom it is given.

VI. Discussion

Our quantitative study shows that a post-payment copyright system is potentially a more profitable business than an online music shop. However, the study is limited by the definition of the inputs to the model and the simplifications used in the model. In reality, the outcome may differ significantly from our results.

In our study, the models are separated, whereas in commercial systems the post-payment system will be linked to other models. We have assumed that the users of a post-payment system receive electronic vouchers to online shops as reimbursements of their transactions. The vouchers encourage post-payment users to buy their digital music in online shops.

The largest source of inaccuracy is the number of people using the service. The popularity of the service is very difficult to estimate due to the following factors: the development of P2P networks, broadband connections, digital rights management, upcoming legal implications on P2P networks, popularity of digital media, the perceived usability of the service, and the benefit from the service.

Comparing the scenarios, CDN cost for file storage and delivery is very deterministic, because the post-payment without download scenario benefits significantly from the absence of media retention and transfer. There are ways to the cost: limiting the market area geographically, replacing CDN with own servers, locating servers close to an Internet exchange point, having point of presence in the Internet exchange point, and leasing own fibers.

Our research is a continuation to the trend of studies suggesting P2P networks as a part of a viable business model for media distribution [15]-[18]. We also demonstrate the usefulness of techno-economic modeling and associated risk analysis when making decisions regarding the development and deployment of a new online service. Our model could be generalized for the analysis of different types of media, for instance the online distribution of movies, and potentially extended with real options analysis [46].

The qualitative analysis with STOF helps to form a working business model and to identify the relevant partners. The main benefits of using STOF instead of other potential analysis frameworks are its holistic and systematic approach and its fit to novel online services. With the help of STOF analysis, we were able to create a more solid business model for post-payment copyright. The post-payment system architecture (Fig. 1) and the post-payment process (Fig. 2) support directly the new business model.

The Critical Success Factor evaluation reveals that the service design and enrollment of the service may have a great impact on the revenue generated by the service. The main challenges in the post-payment copyright system are low value for customers and low customer retention rate. Service bundling with an online music shop offering and careful consideration of marketing message are suggested as solutions for value perception and customer retention.

Our analysis does not concentrate on the Roll-out and Market phases of the STOF framework. In the actual deployment of the service, a current and detailed analysis of the market situation and the relevant competing services should be made. De Reuver et al. [47] demonstrated that addressing Critical Design Issues in sufficient detail leads to better scores in Critical Success Factors, i.e., a viable service design improves the chances for actual success. Furthermore, according to de Reuver et al. [48], having a balanced business model internally is not sufficient for success. The business model also has to be continually balanced to changing market, regulation, and technology conditions in different phases of the service lifetime.

Based on our threat analysis, it seems that trustworthiness of the system is a key factor for users to be willing to use the post-payment copyright system. The users need to be able to trust the system. It must not maliciously act against the user in any way, and it has to protect the user against external threats. If we presume that the post-payment copyright system implements the suggested privacy solutions, we can conclude that it provides quite sufficient protection for the user's privacy even against external threats.

Our study does not confirm that a post-payment copyright system will be the winning model, but the study shows that in favorable conditions post-payment copyright is a very competent model compared to the online shop model. The privacy challenges play in an important role in the user adoption of the service, and solutions for the most important challenges are available. Our recommendation is to do further evaluation among industry experts and end-users and finally to test the validity of our results with a live post-payment service.

ACKNOWLEDGMENT

An earlier version of this work was presented at the ICDS 09 conference, see [1]. We would like to thank our colleagues, especially Mark de Reuver, Asta Kärkkäinen, Sakari Luukkainen, Ben Mellin and Jukka K. Nurminen, the reviewers of this journal, and the reviewers and participants of the ICDS 09 conference for their feedback on previous versions of this work.

The research was partially conducted in the DECICOM project funded by the Finnish Funding Agency for Technology and Innovation (Tekes), Nokia, Ericsson, and NetHawk and partially within the Econ@Tel (COST605) network.

REFERENCES

[1] M. V. J. Heikkinen and H. Kokkinen, “Techno-Economic Modeling of Post-Payment Copyrights,” Proc. Intl. Conf. on Digital Society (ICDS 09), IEEE Press, Feb. 2009, pp. 217-222, doi:10.1109/ICDS.2009.12.

[2] H. Bouwman, H. De Vos, and T. Haaker, Eds., Mobile Service Innovation and Business Models, Springer, May 2008, doi:10.1007/978-3-540-79238-3.

[3] H. Bouwman, E. Faber, T. Haaker, B. Kijl, and M. De Reuver, “Conceptualizing the STOF Model,” in Mobile Service Innovation and Business Models, H. Bouwman, H. De Vos, and T. Haaker, Eds. Springer, May 2008, pp. 31-70, doi:10.1007/978-3-540-79238-3_2.

[4] H. Bouwman, E. Faber, E. Fielt, T. Haaker, and M. De Reuver, “STOF Model: Critical Design Issues and Critical Success Factors,” in Mobile Service Innovation and Business Models, H. Bouwman, H. De Vos, and T. Haaker, Eds. Springer, May 2008, pp. 71-88, doi:10.1007/978-3-540-79238-3_3.

[5] H. De Vos and T. Haaker, “The STOF Method,” in Mobile Service Innovation and Business Models, H. Bouwman, H. De Vos, and T. Haaker, Eds. Springer, May 2008, pp. 115-136, doi:10.1007/978-3-540-79238-3_5.

[6] P. Timmers, “Business Models for Electronic Markets,” Electronic Markets, vol. 8, Apr. 1998, pp. 3-8, doi:10.1080/10196789800000016

[7] R. Amit and C. Zott, “Value Creation in E-Business,” Strategic Management J., vol. 22, June 2001, pp. 493-520, doi: 10.1002/smj.187.

[8] H. Chesbrough and R. S. Rosenbloom, “The Role of the Business Model in Capturing Value from Innovation: Evidence from Xerox Corporation’s Technology Spin-Off Companies,” Industrial and Corporate Change, vol. 11, pp. 529-555, 2002.

[9] R. Alt and H.-D. Zimmerman, “Introduction to Special Section: Business Models,” Electronic Markets, vol. 11, Jan. 2001, pp. 3-9, doi:10.1080/713765630.

[10] A. Osterwalder, Y. Pigneur, and C. L. Tucci, “Clarifying Business Models: Origins, Present, and Future of the Concept,” Communications of the Association for Information Systems, vol. 16, pp. 1-25, 2005.

[11] S. M. Shafer, H. J. Smith, and J. C. Linder, “The Power of Business Models,” Business Horizons, vol. 48, 2005, pp. 199-207, doi:10.1016/j.bushor.2004.10.014.

[12] H. Kokkinen, J. E. Ekberg, and J. Noyranen, “Post-Payment System for Peer-to-Peer Filesharing,” Proc. Consumer Communications and Networking Conf. (CCNC 08), IEEE Press, Jan. 2008, pp. 134-135, doi:10.1109/ccnc08.2007.37.

[13] H. Hietanen, A. Huttunen, and H. Kokkinen, “Laila: File Sharing Indulgence Service,” NIR Nordic Intellectual Property Law Review, vol. 78, pp. 175-180, 2009.

[14] H. Kokkinen and J. Nöyränen, “Forensics for Detecting P2P Network Originated MP3 Files on the User Device,” in Forensics in Telecommunications, Information and Multimedia, LNICST 8, M. Sorell, Ed. Springer, May 2009, pp. 10-18, doi: 10.1007/978-3-642-02312-5_2.

[15] H. Hietanen, A. Huttunen, and H. Kokkinen, “Criminal Friends of Entertainment: Analysing Results from Recent Peer-to-Peer Surveys,” SCRIPTed, vol. 5, 2008, pp. 31-49, doi:10.2966/scrip.050108.31.

[16] D. Y. Cohn and V. L. Vaccaro, “A Study of Neutralization Theory’s Application to Global Consumer Ethics: P2P File-Trading of Musical Intellectual Property on the Internet,” Intl. J. Internet Marketing and Advertising, vol. 3, pp. 68-88, 2006.

[17] M. Peitz and P. Waelbroeck, “An Economist’s Guide to Digital Music,” CESifo Economic Studies, vol. 51, pp. 359-428, 2005.

[18] S. Bhattacharjee, R. D. Gopal, K. Lertwachara, and J. R. Marsden, “Economic of Online Music,” Proc. Intl. Conf. on Electronic Commerce, ACM Intl. Conf. Proc. Series, vol. 50, 2003, pp. 300-309, doi:10.1145/948005.948045.

[19] L. A. Ims, Ed., Broadband Access Networks: Introduction Strategies and Techno-Economic Evaluation, London: Chapman & Hall, 1998.

[20] N. K. Elnegaard and K. Stordahl, “Analysing the Impact of Forecast Uncertainties in Broadband Access Rollouts by the Use of Risk Analysis,” Teletronikk, vol. 4, pp. 157-167, 2004.

[21] T. Monath, N. Kristian, P. Cadro, D. Katsianis, and D. Varoutas, “Economics of Fixed Broadband Access Network Strategies,” IEEE Communications Magazine, vol. 41, Sept. 2003, pp. 132-139, doi:10.1109/MCOM.2003.1232248.

[22] B. Jerman-Blažič, “Techno-Economic Analysis and Empirical Study of Network Broadband Investment: The Case of Backbone Upgrading,” Information Systems Frontiers, vol. 10, 2008, pp. 103-110, doi:10.1007/s10796-007-9059-y.

[23] K. R. R. Kumar and V. Y. H. Kueh, “Techno-Economic Analysis of International Mobile Roaming,” IEEE Wireless Communications, vol. 15, June 2008, pp. 73-80, doi:10.1109/MWC.2008.4547526.

[24] T. Smura, A. Kiiski, and H. Hämmäinen, “Virtual Operators in the Mobile Industry: A Techno-Economic Analysis,” Netnomics, vol. 8, Oct. 2007, pp. 25-48, doi:10.1007/s11066-008-9012-3.

[25] E. Kivisaari, T. Autio, T. Smura, and H. Hämmäinen, “Operator Roles in Mobile Broadcast,” Nordic and Baltic J. of Information and Communication Technologies, vol. 2, pp. 48-60, 2008.

[26] T. Rokkas, D. Varoutas, D. Katsianis, T. Smura, R. Kumar, M. Heikkinen, J. Harno, M. Kind, D. Von Hugo, and T. Monath, “On the Economics of Fixed-Mobile Convergence,” Info, vol. 11, 2009, pp. 75-86, doi:10.1108/14636690910954999.

[27] M. V. J. Heikkinen and S. Luukkainen, “Value Analysis of Technology Evolution: Case Mobile Peer-to-Peer Communications,” Proc. Wireless Telecommunications Symposium (WTS 2009), IEEE Press, in press.

[28] J. Schäfer, K. Malinka, and P. Hanáček, “Peer-to-Peer Networks: Security Analysis,” Intl. J. on Advances in Security, vol. 2, pp. 53-61, 2009.

[29] J. Suomalainen, A. Pehrsson, and J. K. Nurminen, “A Secure P2P Incentive Mechanism for Mobile Devices,” Intl. J. on Advances in Security, vol. 2, pp. 42-52, 2009.

[30] P. Merz, F. Kolter, and M. Priebe, “A Distributed Reputation System for Super-Peer Desktop Grids,” Intl. J. on Advances in Security, vol. 2, pp. 30-41, 2009.

[31] H. Koshutanski, M. Ion, and L. Telesca, “Towards User-Centric Identity Interoperability for Digital Ecosystems,” Intl. J. on Advances in Security, vol. 1, pp. 26-38, 2008.

[32] T. Buchanan, C. Paine, A. N. Joinson, and U-D. Reips, ”Development of Measures of Online Privacy Concern and Protection for Use on the Internet,” J. of the American Society for Information Science and Technology, vol. 58, Nov. 2006, pp. 157-165, doi: 10.1002/asi.20459.

[33] H. Wang, M. K. O. Lee, and C. Wang, “Consumer Privacy Concerns about Internet Marketing,” Commun. ACM, vol. 41, Mar. 1998, pp. 63-70, doi:10.1145/272287.272299.

[34] A. Kobsa, “Privacy-Enhanced Personalization,” Commun. ACM, vol. 50, Aug. 2007, pp. 24-33, doi:10.1145/1278201.1278202.

[35] Y. Lu, W. Wang, B. Bhargava, and D. Xu, “Trust-Based Privacy Preservation for Peer-to-Peer Data Sharing,” IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, vol. 36, May 2006, pp. 498-502, doi:10.1109/TSMCA.2006.871795.

[36] D. L. Hoffman, T. P. Novak, and M. Peralta, “Building Consumer Trust Online,” Commun. ACM, vol. 42, Apr. 1999, pp. 80-85, doi:10.1145/299157.299175.

[37] J. W. Palmer, J. P. Bailey, and S. Faraj, “The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements,” J. of Computer-Mediated Communication, vol. 5, Jun. 2006, doi:10.1111/j.1083-6101.2000.tb00342.x.

[38] I. Clarke, S. G. Miller, T. W. Hong, O. Sandberg, and B. Wiley, “Protecting Free Expression Online with Freenet,” IEEE Internet Computing, vol. 6, Jan 2002, pp. 40-49, doi:10.1109/4236.978368.

[39] S. Lipner, “The Trustworthy Computing Security Development Lifecycle,” Proc. 20th Annual Computer Security Applications Conf. (ACSAC 04), IEEE Press, Dec. 2004, pp. 2-13, doi:10.1109/CSAC.2004.41.

[40] B. Schneier, “Attack trees,” Dr. Dobb’s J., Dec. 1999.

[41] Statistics Finland, “Population Projection,” May 2007.

[42] Ministry of Transport and Communications Finland, “National Broadband Strategy: Final Report,” Jan. 2007.

[43] IFPI, “Digital Music Report,” Jan. 2008.

[44] Jupiter Research, “US Digital Music Forecast,” Jan. 2007.

[45] W. B. Norton, “Video Internet: The Next Wave of Massive Disruption to the U.S. Peering Ecosystem (v1.5),” Apr. 2007.

[46] J. Alleman, G. Madden, and H. Kim, “Real Options Methodology Applied to the ICT Sector: A Survey,” Communications & Strategies, no. 70, pp. 27-44, 2008.

[47] M. de Reuver, H. Bouwman, and T. Haaker, “Mobile Business Models: Organizational and Financial Design Issues that Matter,” Electronic Markets, vol. 19, Mar. 2009, pp. 3-13, doi:10.1007/s12525-009-0004-4.

[48] M. de Reuver, H. Bouwman, and I. MacInnes, “Business Models Dynamics for Start-Ups and Innovating E-Businesses,” Intl. J. Electronic Business, vol. 7, pp. 269-286, 2009.