EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

Research on Online Business Models Infringing Intellectual Property Rights

Phase 1

Establishing an overview of online business models infringing intellectual property rights

July 2016

www.euipo.europa.eu

Research on Online Business Models Infringing Intellectual Property Rights

Report commissioned to Deloitte Spain by the European Union Intellectual Property Office (EUIPO)

Content

Foreword

Over the past few decades the ingenuity of infringers of intellectual property rights (IPRs) appears to have kept track with and even to some extent outpaced the development of the legitimate business models designed to facilitate online commerce.

The very success of the legal online business models, often relying on advanced technology, has acted as a spur to those seeking to profit from illegal activity.

This report is one of the first steps by the EUIPO, through the Observatory, to look specifically at the variety of online business models infringing IPR, but will certainly not be the last. This crucial area will continue to have a high priority in the work of the Observatory.

The report sheds light on the numerous illicit examples of marketing through Business-to-Business (B2B) and Business-to-Consumer (B2C) websites, online marketplaces and social media.

This shadow landscape thrives on the misuse of IPR belonging to others and is often built on the use of domain names and other digital identifiers.

It more and more relies on new encrypted technologies like the TOR browser and the bitcoin virtual currency, which are employed by infringers of IPR to generate income and hide the proceeds of crime from the authorities.

The new business models created to take advantage of IPR infringements include, for example, the systematic misuse of the domain name system to direct internet traffic to webshops completely unrelated to the brand names suggested by the domain name and other marketing.

IPR is also being used to disseminate malware, carry out illegal phishing and simple fraud to the detriment of society, businesses and the ordinary user of the internet.

The current report is part of an effort to develop a complete map of the business models used, the different supply chains and the roles of intermediaries, facilitators and enablers.

Since e-commerce is an increasingly strong force in modern business, representing 17% of all EU business turnover in 2014, this report must act as an alarm call for both the private and public sectors.

Ultimately, the goal must be to identify, analyse, and come up with effective strategies to combat IPR infringements in the online environment in the interest of protecting citizens, right holders, legitimate businesses and the economy as a whole.

António Campinos,
Executive Director, EUIPO

Executive summary

Background

In 2015, the European Union Intellectual Property Office (EUIPO), through the European Observatory on Infringements of Intellectual Property Rights, commissioned a research study on business models used to infringe intellectual property rights (IPRs). The initiative is envisioned as an independent data-driven study that will assess and analyse specific techniques used to facilitate online IPR infringements on a commercial scale. The aim of this independent research is to provide an overview of different infringing business models, assessing how they function, how they are financed, how they generate profits for their operators, what kinds of content they disseminate and how large their user bases are.

The study will provide enhanced understanding to policymakers, civil society and private businesses. At the same time, it will help to identify and better understand the range of responses necessary to tackle the challenge of large scale online IPR infringements.

It was foreseen that the study should be divided into two phases with phase 1 being a qualitative study aimed at providing an overview of the different business models used to infringe IPR online and a phase 2 being a more quantitative oriented phase where specific business strategies can be researched in more detail. The present report presents the outcome of phase 1 of the study.

Methodology

During the execution of phase 1 a comprehensive collection of material on businesses activities that have been determined to be infringing IPR or have been considered susceptible of IPR infringement was collected and processed. The material consisted of publicly reported case law i.e. decisions taken by national courts and dispute resolution bodies such as domain name dispute panels as well as, cases that have been referred to in publically available reports and studies. To some extent also examples of 'notice and takedown' actions that are not immediately available to the public at large were collected. As far as activities on Darknet markets and new business models are concerned independent research was made. Due to lack of available case law an assessment of the susceptibility of IPR infringement on the websites was made on the basis of information gathered from the websites themselves.

Based on collected material on business models in general and on online business models in particular an analytical method was developed that makes it possible to identify, dissect, analyse, describe and present any IPR-infringing business model in the online environment. The method is comprised of two main tools. Namely a taxonomic matrix that in a systematic way identifies and presents the main characteristics of possible IPR-infringing business models and a business model canvas describing the specific features of each individual online business model.

The analytical method developed is a dynamic tool that will enable businesses, authorities and other stakeholders to identify, dissect, analyse, describe and present any future IPR-infringing business methods and relate them to the existing business models.

The analytical method has been applied to 25 online business models that have been identified during the execution of the study and the canvasses of these business models are presented as a separate appendix to the report. The template for the canvas looks like this:

CANVAS

Online Intellectual Property Rights Infringing Business Model:
Short Description of the Business Model

Reference: Identification of legal decision (if any)

Date of Decision: Date of Analysis

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Short summary description of the business model with focus on specific features or traits.

Indication of whether the business model is to be considered deceptive or non-deceptive.

In the Matrix, the specific digital platform and infringing activity is indicated with a grey background.

Matrix: Online Digital Platform / IPR Infringing Activity	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

In this part of the canvas it will be indicated whether the platform is on the open Internet or Darknet.

Indication of whether the services are freely accessible or access is restricted.

Products and Services:

Description of what is actually offered on the website, such as non-genuine products or access to copyright protected works, including an indication of the variety, quality and availability as well as the pricing of the goods (if available).

Involved IPR(s):

Identification of which intellectual property right(s) that is affected by the specific activity including trademarks, copyrights and related rights, protected databases, design rights and patents.

Identification of Infringer:

An indication of whether the name of and contact information of the operator of the website is immediately available, including WHOIS information for the involved domain name (if applicable).

Revenue Sources:

A description of the revenue sources, including how revenue is obtained through direct sales, sales commission, subscription fees, pay-per-click, advertising, donations or fraud. Payment options in fiat as well as virtual currencies are identified.

Customer Relations:

Description of elements such as accessibility, login features, delivery and shipment, and return and refund policy. It is indicated whether the business model seems deceptive or non-deceptive towards the immediate user and customers.

Resilience Against Enforcement Action:

An indication of whether the provided service is subject to extra-judicial enforcement, such as notice-and takedown complaints. It is further indicated whether the provider of the service has indicated that steps to counteract possible enforcement actions has been taken.

Marketing Channels and Internet Traffic Features:

Description of how the business activities are marketed such as by the use of a trademark-infringing domain name, by use of legal as well as illegal traffic redirection, participation in advertising networks or affiliate programs, and use of unsolicited marketing such as phishing mails.

Customer Incentives:

An indication of which initiatives – if any – the vendor has in place to retain and increase the user and customer base.

The 25 online business models identified and analysed

During the research 25 distinct business models were identified and analysed:

- 5 business models where IPR is misused in the domain name (or other digital identifier) in marketing practices on the open Internet: cybersquatting, domain name parking, affiliate marketing and marketing of products either related or unrelated to the misused IPR.

- 5 business models where IPR is not misused in the domain name (or other digital identifier) in marketing practices on the open Internet: marketing of pharmaceuticals, applied arts replica and virtual items and marketing on third party commercial platforms or social media.

- 5 business models existing on the hidden part of the Internet, Darknet: trading of user accounts, computer software source code, complete databases, weapons and storage devices as well as an online e-book library.

- 5 business models with the aim of conducting phishing, dissemination of malware or traditional fraud: spoofing, phishing e-mails, ransomware mobile apps, malware dissemination from websites making unauthorised trademark use and fraudulent misuse of the name of a national IP office.

- 5 business models sharing digital content on the open Internet: linking, torrent, streaming and cyberlocker sites and a site contributing to video streaming.

In the examples infringement of trademarks and copyrights are the most common, but there are also infringements of other IPRs. It is often seen that several IPRs are infringed at the same time, sometimes in surprising combinations.

It is apparent from the analyses of the identified business models that the operators that are engaged in IPR-infringing activities in the online world are using a wide variety of business models as the following overview of the analysed business models plotted into the taxonomic matrix illustrates:

Matrix: Online Digital Platform / IPR Infringing Activity		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

It can be observed that a number of the IPR-infringing business models are based on generally applicable online business models, such as Business-To-Business (B2B) or Business-To-Consumer (B2C) websites and marketplaces. The revenue sources of the IPR-infringing business models are to a large extent the same as for non-infringing business models and consist of direct revenue sources such as sales revenue, subscription fees and donations, or indirect revenue sources such as pay-per click or advertisement fees. Payment options often include traditional bank transfer and credit card payment, but increasingly also include payments in virtual currencies (mainly Bitcoins).

However, the IPR-infringing business models differ from the non-infringing business models in the way that they are often deceptive to the customers and it can be observed that certain specific online IPR-infringing business models have been developed to benefit from IPR-infringing activities. Examples of that are misuse of the domain name system through cybersquatting, domain name parking and marketing of goods on websites making unauthorised use of trademarks unrelated to the marketed goods or services.

Deceptive business models are also found on websites marketing goods to consumers constructed in ways that give the consumer the impression that there is a connection to the legitimate brand. Other deceptive business models include those business models that gain their revenue from dissemination of ransomware and other kinds of malware or fraudulent schemes to obtain payments for non-existing goods and services. Other examples include phishing and spoofing scams, where consumers and companies are deceived to reveal access codes to bank accounts or credit card details. It has been observed that the borderline between IPR-infringing activities and traditional cybercriminal activities are blurring and that trademark infringement is a key component in many current cybercriminal business models.

Not all identified business models are deceptive however and especially on Darknet markets it seems that consumers are receiving clear information as to the IPR-infringing nature of the goods for sale.

Advanced misuse of Internet technologies, anonymity possibilities and marketing tools

Irrespective of the concrete online business model and its revenue sources, the operators of IPR-infringing businesses are dependent on users and customers actually visiting their websites or noticing their listings on online marketplaces. These operators therefore apply marketing tools that are generally available for online businesses including search engine optimisation, search engine marketing and advertising on social media platforms. Many of the websites that are used for IPR-infringing activities have also designed apparently well-functioning user interfaces, and some vendors even appear to offer the same customer services and use the same customer incentives as legitimate businesses, such as return policies and discounts. Delivery services for the IPR-infringing websites are often comparable to legitimate businesses and are carried out by means of reputable courier services.

Most of the analysed business models are operated through an Internet site that is controlled by the infringer which means that the infringing entity is the registrant of the domain name and that the content on the website is made available by the infringer. However, operators behind the IPR-infringing activities often either conceal their identities by using privacy shield services for the registration of their domain names or provide inadequate, false or otherwise misleading contact details on the website thus hampering or even precluding enforcement actions.

The study has also found that it seems that an increasing number of providers of IPR-infringing products and services are expanding their businesses to Darknet (primarily the TOR-network) or maybe even moving their businesses to Darknet. Since the providers and possible affiliates are anonymous it is apparent that they cannot be immediately identified. In addition, the 'notice and takedown' procedures, which are provided by the operators of online marketplaces and other Internet service providers on the open part of the Internet, do not appear to be available on Darknet.

In cases where it is possible to take enforcement action against an IPR-infringing business either through a civil lawsuit, by ways of a criminal complaint, through an alternative dispute resolution procedure (like UDRP) or via a 'notice and takedown' request, the study shows that a number of the analysed business models are based on concepts that make it possible for the providers to be able to continue their illegal business even in the event of an enforcement action being initiated. Examples of this are the sale of IPR-infringing goods on third party websites, where the vendor may create a new user profile or a new listing if his initial profile or listing has been closed down, through which he can offer the same goods as before. Another example is where a provider of an IPR infringing business appear to be able to set up a new business under a different domain name but with the exact same design and content as before, immediately after the initial domain name that was used for the business was transferred or deleted as a result of a legal action. In some of the business models the providers openly state to their customers that they have included resilience against enforcement actions in their business models.

Phase 2 of the research into online business models infringing IPRs will look further into some of the advanced misuses of the domain name system, that have been identified in this report. The extent and nature of the apparently widespread affiliation between infringing websites will also be researched.

1. Background and scope: Establishing an overview of different online business models infringing intellectual property rights

The research study on online business models infringing intellectual property rights (IPRs) is one of the initiatives included in the 2015 work program for the European Observatory on Infringements of Intellectual Property Rights (the Observatory). In the work program[1] it is described as an independent data-driven study that will assess and analyse specific techniques used for facilitating online IPR infringements on a commercial scale.[2]

The aim of the independent research is to provide an overview of the different infringing business models, assessing how they function, how they are financed, how they generate profits for their operators, what kinds of content they disseminate and how large their user bases are. The study shall provide enhanced understanding to policymakers, civil society and private businesses. At the same time, it will help to identify and better understand the range of responses necessary to tackle the challenge of commercial scale online IPR infringements.

In the accepted final Terms of Reference for the research study it was foreseen that it should be divided into two phases. It was underlined that the aim of the research study was to provide a practical and structured view and understanding of which business models are used in the attempt to gain direct or indirect economic advantage[3] in the online environment regarding activities susceptible to IPR infringement.

Special focus should be paid to horizontal features crucial for the ability of the online business models to generate income.[4] It was foreseen that the Observatory in cooperation with a consultant (assisted by external experts) in Phase 1 of the research study would produce an initial overview of the different known infringing business models through a review of available literary and case law[5] sources and initial Internet research. Following the creation of the overview, Observatory stakeholders would be asked for their feedback to prepare Phase 2 of the research study.

This report is the result of Phase 1 of the research study and will be followed up during 2016 by Phase 2.

The aim of Phase 1 of the project was to make an overview of the different existing online business models infringing IPRs. In order to make this overview the project team developed an analytical method that made it possible to identify, dissect, analyse, describe and present the existing business models in a systematic and structured way. However this analytical method is a generally applicable method that will also facilitate the analyses of any future online business models that may be identified.

The initial overview of the existing business models was presented for and discussed with the Observatory Working Group on IP in the Digital World and the Observatory Working Group on Enforcement at their meetings in Brussels in September 2015.

A draft report including the developed analytical method was sent to the members of the working groups and comments and the feedback from the working group meetings in March 2016 have been taken into consideration in order to produce this final report.

[1] European Observatory on Infringements of Intellectual Property Rights. Work Programme 2015, p. 12.

[2] In the scope of the study 'commercial scale' is defined in accordance with recital 14 of the preamble to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004): 'Acts carried out on the commercial scale are those carried out for direct and indirect economic commercial advantage; this would normally exclude acts carried out by the end consumers acting in good faith'.

[3] Direct or indirect economic advantage includes payments in fiat currencies, including subscriptions and donations, payments in digital, virtual and encrypted currencies, exchange of items of economic value, including physical and virtual items, revenue from advertisement and pay-per-click service, misdirection as well as redirection of Internet traffic, installation of illegal malware, ransomware and adware, illegitimate harvesting of access codes and emails, phishing and other cybercriminal activity.

[4] These secondary features could be e.g.
- Types of infringing websites (galaxy to which a website belongs)
- Deceptive/non-deceptive business practices
- Level of combination of legal and illegal marketing
- Exploitation of territorial and jurisdictional boundaries, and diverse level of IP protection
- Website accessibility, external promotion, solicited or un-solicited marketing, traffic redirection efforts and use of trademark in domain name
- Affiliation between websites
- Product/content variety, quality and availability
- Layout, e.g. user/customer service/information and customer review, satisfaction, complaint and advocacy features
- Interactivity between marketing platforms and technology/programming, including cybercrime synergies
- Pricing, subscription, discount, reward and VAT policy in regards to direct sale/subscription
- Reliance on revenue from advertisement, donations or other alternative lines of income
- Availability of payment options and level of transactions costs
- Shipment service and return/refund policy
- Misuse of intermediaries (including facilitators of shipments, advertising, payments, hosting and domain names) and other essential infrastructure
- Financing and profitability issues
- Location of infringing business (including servers a.o.) and anonymity features
- Reaction to disruptions of business through enforcement action

[5] Case law will in the scope of this study cover e.g. court rulings, arbitration decisions, alternative dispute resolution decisions and administrative decisions.

2. Methodology

The scope of the research study Phase 1 is, as stated above, to provide a practical and structured overview of the different online business models infringing IPRs in order to better understand which business models these operators use in the attempt to gain a direct or indirect economic advantage.

It is outside the scope of this research study to determine whether an online activity is in fact infringing one or more IPRs since such a determination can only be made in a judicial procedure. Accordingly the project team of Phase 1[6] has, first of all, collected material on suspected online business models based on case law from national courts or decisions from dispute resolution bodies such as UDRP Panels, but also case law that has been referred to in various reports made by public authorities, international organisations or other reliable and publicly available sources.

It should be emphasised that the aforementioned legal decisions or determinations only address the issue of whether the specific activity, that was the subject of the dispute, was infringing on one or more IPRs or not. The decisions do not focus on whether the specific activity can also serve as an illustration of a business model, i.e. an activity that is or may be used by other entities than the alleged infringer. When a decision is mentioned in this report it is therefore the assessment of the project team that the particular case concerns an activity that can serve to illustrate a business model as such.

As it will appear from the below descriptions of online business models, in some cases the descriptions are based on deletion actions that are not publicly available since they have been taken by the provider of the relevant digital platform through a 'notice and takedown' procedure. Such dispute resolution procedures are integrated parts of the user terms on most trading platforms and social media platforms and they allow a third party, such as a holder of an IPR, to file a complaint against a specific posting or a specific user profile of the platform with a request to the service provider to take down the posting or to suspend the user profile. The decisions that the service providers make in these cases are not publicly available.[7] The Phase 1 team has however been granted access to a number of such decisions and has been allowed to use them as a basis for the study on the condition that the content of specific cases is not made publicly available. The team has accepted these conditions, since we have determined that they will not affect the description of the online business model as such.

In addition, as far as online business models on Darknet or other new business models are concerned, and where no relevant case law has been reported, the team has conducted its own independent research and made its own immediate assessments[8] on whether the online activities are susceptible of infringing the IPRs of a third party.

These initial bottom up descriptions were then analysed from a theoretical point of view based on available literature on business models in general and on available literature and reports focusing on online business models in particular.

This led to the development of a generally applicable analytical method that made it possible to categorise and describe not only the existing IPR-infringing business but also future IPR-infringing business models in the online environment. The method and its components will be explained further the below in chapter 6.

[6] In accordance with the framework contract between the EUIPO and Deloitte Advisory S.L. Spain the task of performing Phase 1 was awarded to Deloitte Advisory S.L. Spain in cooperation with Danish IT forensic investigation expert Michael Lund, DBI, and Danish attorney-at-law, PhD. Knud Wallberg.

[7] Information on the use of such procedures is available at https://www.chillingeffects.org/ which is a project of the Berkman Center for Internet & Society at Harvard University. Access to the content of the concrete cases may be given upon request.

[8] The assessment is based on the description of the business model made by the provider himself on the website, including whether it is stated that intellectual property is infringed, information about price and delivery and any other available information. In carrying out the assessment the team has made analogous use of criteria to determine infringement from known case law and dispute resolution practice.

3. Definitions of the terms used

The following paragraphs contain explanations of some of the terms that are used throughout the report and which cannot be expected to be known by all readers.

BitTorrent

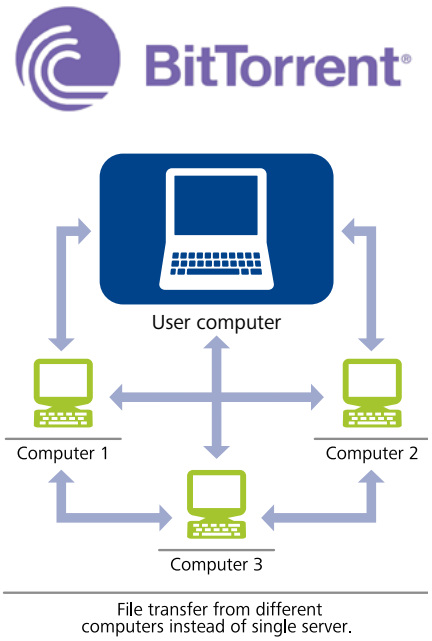
BitTorrent[9] is a file transfer protocol designed in 2001. The BitTorrent protocol makes use of peer-to-peer connectivity, which means that files can be shared directly between computers that use the protocol without the need of a central server, and the protocol is optimised for file sharing of large amounts of data over the Internet. As such the Bittorent protocol is the base of a decentralised file sharing network commonly called the BitTorrent network. This network is currently the prevalent file sharing network and accounts for the majority of file sharing taking place today. Numerous clients are available to use to connect to the network and they generally consist of similar features and user interfaces.

A torrent file (.torrent) contains information (metadata) about a shared file - called X. When users of the BitTorrent Network want to download X, they can download the related torrent file. Once downloaded the torrent file can be opened in a BitTorrent client, which then uses the contained information in the torrent file to establish direct connections with other users who share X. Through these connections X is then downloaded and potentially simultaneously uploaded to other users. The torrent file does not contain any file data from X.

Magnet links are predominantly used to facilitate file sharing through the BitTorrent Network. Magnet links contains a range of parameters for a shared file X. By activating or opening a magnet link in a BitTorrent client, users are able to directly connect to other users who share X. Once the connections are made the download of X commences. As opposed to torrent files users don't have to first download a torrent file to begin downloading.

Popcorn Time is the name of a software project founded by a group of Argentinian developers. The project is basically a BitTorrent client and a video player integrated in one user friendly client. In terms of functionality this client allows users to browse a very large number of video files and watch them on demand by streaming (in reality downloading temporarily) the video files. As part of this process the user shares parts of the files to other users watching the same video file. The original Popcorn Time project was shut down in early 2014. The software was subsequently made open source, which prompted several new projects to arise. The main functionality of these is identical to the original project, but developers are differentiating the projects by adding new features such as built-in VPN functionality for secure usage and applying different content quality levels. These new features also mean that the projects are potentially incorporating new business models whereas the original project didn't focus on this.

Fig. 1: BitTorrent



[9] More information on BitTorrent can be found at http://help.bittorrent.com/customer/en/portal/articles/178790-the-basics-of-bittorrent?b_id=3884, http://techterms.com/definition/bittorrent, and several other sources.

Bitcoin

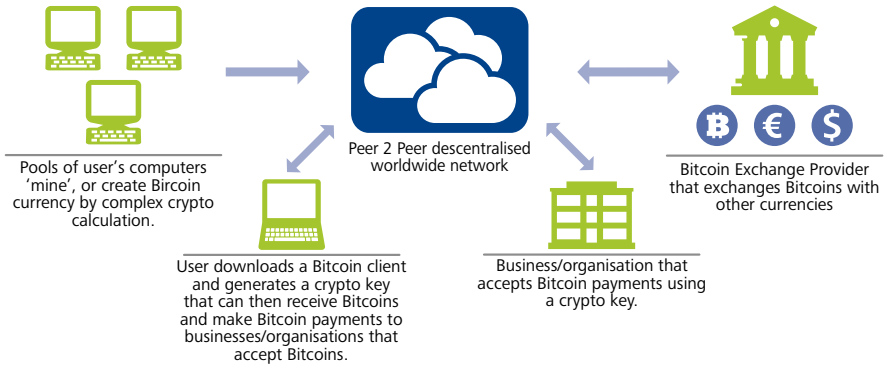
Bitcoin[10] is a cryptocurrency launched in 2009. It is the largest and most well-known of several cryptocurrencies.

The Bitcoin system uses encryption and advanced algorithms to generate the bitcoins and to validate and finalise transactions. These essential processes are carried out by bitcoin miners which are run by individuals, groups or enterprises.

Bitcoin transactions are publically visible as they become part of the so-called Bitcoin blockchain that is a distributed database or ledger that holds every single transaction since the launch of the currency. This distributed nature is a vital security feature as it acts to avoid regulation or malicious manipulation. The Bitcoin blockchain contains all transactions ever completed in its lifespan and is publically available. Online services even provide a real time view of transactions entering the blockchain. The blockchain functionality is implemented in several other cryptocurrencies beside the Bitcoin currency. Bitcoin transactions consist of a number of technical details, of which the common ones are the wallet IDs of the sender and receiver, as well as the amount transferred.

There are no public records connecting Bitcoin wallet IDs with personal information of individuals. Because of these Bitcoin transactions are considered semi-anonymous.

Fig. 2: Bitcoin



[10] More information on Bitcoins can be found in: Virtual Currency Schemes, European Central Bank, October 2012, a number of recent publications like Nicolas Wenker: Bitcoin Pandemonium, 2014, the ECJ decision in Hedqvist, C-264/14 and on the website of the Bitcoin Project, https://Bitcoin.org.

Cryptocurrencies

Cryptocurrencies11 are digital currencies in which encryption techniques and technologies are used to enhance security and stability. The same features are used to generate the currency units and as part of transaction verifications. Cryptocurrencies are stored in semi-anonymous digital wallets. They can be used as payment for a wide variety of purchases across the internet and in the offline world. In general cryptocurrencies are characterised by being regulated only by supply and demand with no central authority or industry regulation.

Darknet

Darknet[12] is a term describing a certain part of the Internet. Darknet is part of the 'deep web' which is the un-indexed part of the internet consisting of data that cannot be indexed by traditional search engines and is therefore not directly searchable. In popular terms darknet is specifically designed to secure the anonymity of those who disseminate information or who carry out other activities by making use of specific technologies and network configurations. As a result, specific software and/or configurations are needed to access darknet websites.

The most popular Darknet makes use of the TOR network (see below).

Darknet Markets are websites on Darknets that provide a market platform which facilitates trade of goods and/or services between vendors and customers. By utilising Darknet network topology Darknet Markets are able to provide high levels of security and anonymity to their users.

The Darknet Markets generally offer users full featured markets with listings, vendor pages, vendor and product review sections as well as customer support and dispute mitigation processes. Darknet Markets primarily make use of cryptocurrencies for payment transactions. Bitcoins are the predominant method of payment but other cryptocurrencies are also widely accepted.

The first successful darknet market was called Silk Road and was started in 2011 and becoming very popular before being shut down by authorities in 2013. The vast majority of Silk Road successors run as hidden service websites on the Tor darknet. It is estimated that 50—60 darknet markets are currently active on this darknet.[13]

Domain Name System

The domain name system (DNS)[14] serves the essential and central function of facilitating the Internet users' ability to navigate the Internet. A domain name is the user friendly address of a specific computer´s underlying numeric IP address: The domain name euipo.europa.eu is thus tied to the computer with the numeric IP address 109.232.208.230, which means that instead of remembering and typing in '109.232.208.230' in the internet browser an internet user can type in 'euipo.europa.eu' to be connected to the EUIPO website.[15]

Technically, the DNS works through a network of distributed databases that are operated by the various domain name registries. These databases contain the lists of domain names and their corresponding IP numeric addresses and perform the function of mapping the domain names to their IP- numeric addresses for the purpose of directing requests to connect computers on the Internet.

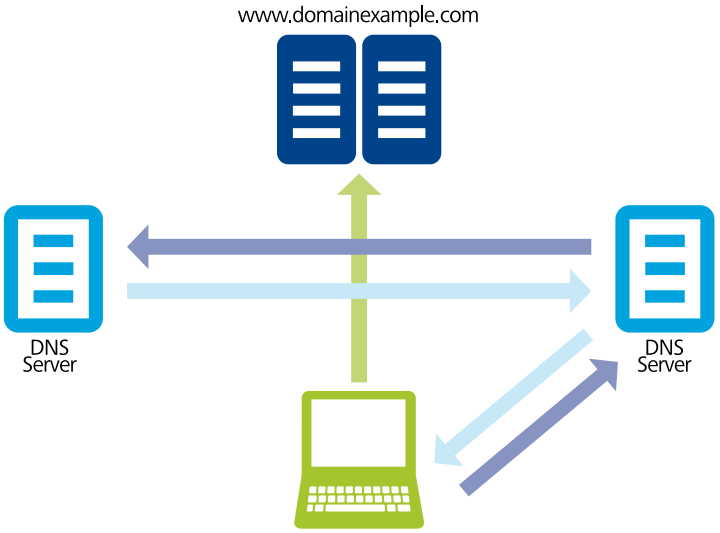
[11] More information on cryptocurrencies can be found in Virtual Currency Schemes, European Central Bank, October, 2012.
[12] A comprehensive description of Darknet can be found in Jamie Bartlett: The Dark Net , William Heinemann, London, 2014.
[13] More information on the Darknet can be found at https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/
[14] More information on the Domain Name System can be found at https://www.icann.org/resources/files/domain-names-beginners-guide-2010-12-06-en. See also Torsten Bettinger: Structure and Organization of the Domain Name System in Domain Name Law and Practice, 2nd Ed., Oxford University Press, 2015
[15] Final Report of the First WIPO Internet Domain Name Process, WIPO, 1999, Domain Name Law and Practice. An International Handbook Torsten Bettinger and Allegra Waddel l(ed.), 2nd ed., 2015

It is the Internet Corporation for Assigned Names and Numbers (ICANN) that coordinates the key technical functions of the DNS and defines policies for how the 'names and numbers' of the Internet should run. Domain names have to be registered with the ICANN approved Registry that is responsible for the specific top level domain, and registrations have to be filed through an accredited Registrar. By way of an example, if a company wants to register a .eu domain name the company must contact an accredited .eu Registrar and request the Registrar to file an application to register the domain name on the company´s behalf. If the domain name is vacant and all other formalities are fulfilled the domain name will be registered and entered into the DNS-database.[16]

The Registries do not examine the applications for a new domain name against prior rights of third parties such as trademarks, company names or personal names. Third party rights holders are therefore compelled to enforce their rights after the domain name has been registered if they find that a registered domain name infringes their rights. Infringements can be addressed through ordinary means whether out of -court or in-court proceedings, but in addition, a majority of top level domains have established Alternative Dispute Resolution services (ADR´s), which enables right holders to file complaints against alleged abusive registrations with an appointed dispute resolution body. Such procedures are much faster and less expensive than court proceedings and may result in the transfer or the deletion of the disputed domain name.[17]

All Registries that operate generic top level domains (.com, .net, .biz, .email, .mobile, .attorney etc.) are obliged to apply the Uniform Domain Name Dispute Resolution Policy (UDRP), which is a uniform set of rules laid down by ICANN.[18]

Fig. 3: Domain Name System



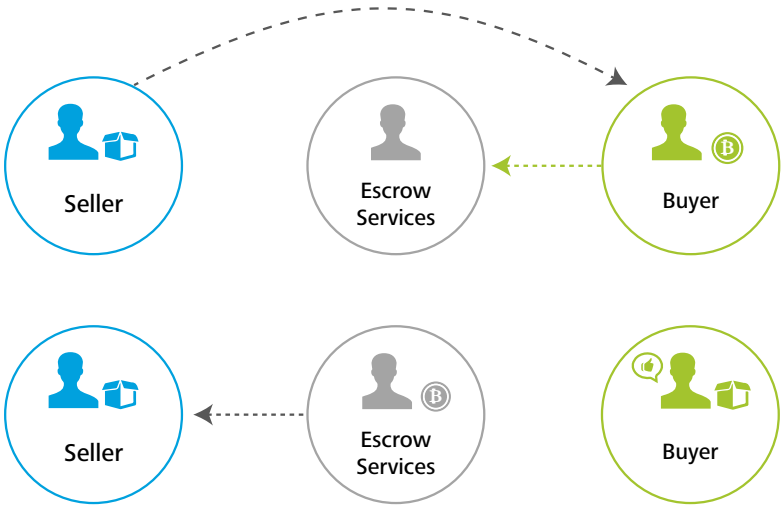
[16] http://eurid.eu/en/get-eu/how-get-started .
[17] The most recent of the many publications dealing with these proceeding is the already mentioned 'Domain Name Law and Practice. An International Handbook', 2nd Edition, 2015, edited by Torsten Bettinger and Allegra Waddell, Oxford University Press. An overview of the more than 70 country code registries that apply variations of the so called UDRP procedure can be found at http://www.wipo.int/amc/en/domains/cctld/.
[18] https://www.icann.org/resources/pages/dndr-2012-02-25-en ; http://www.wipo.int/amc/en/domains/gtld/

Escrow Service

Escrow or Escrow Service is a financial service or instrument where an independent third party becomes part of a transaction between two parties (payer and receiver). The third party holds the transaction funds until specific obligations have been met (i.e. reception of purchased items) at which point the funds are released and the transaction finalised.

Escrow is rapidly becoming a standard feature on Darknet Markets.

Fig. 4: Escrow Service



Intellectual Property Rights

Intellectual property rights (IPRs) for the purpose of this study include trademarks, copyrights and related rights, protected databases, design rights, patents, utility models, geographical indications, topography of semiconductors, plant variety rights, and trade names, in so far as they are protected as exclusive property rights in the national law concerned.[19]

Malware

Malware or 'malicious software' is software that is designed to damage or harm a computer or a computer system. Well known examples of malware are viruses, worms, trojan, and spyware.[20] Ransomware is another type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Cryptolocker is a ransomware variety in which the malware encrypts files or devices and demands payment to decrypt these and make them available to the victim. Currently payment in Bitcoin is preferred but occasionally other means of payment are demanded (PayPal, Wire Transfer).

[19] This report will not contain a detailed explanation of the legal framework covering the said intellectual property rights and the criteria for protection or infringement of these rights.
[20] See http://techterms.com/definition/malware with hyperlinks to the definitions of the listed types of malware

Online

The use of terms online and online environment in this report include any activity on the open or the hidden/ un-indexed internet, including websites, lower level pages, user profiles on social networking websites, online auction and trading platforms, virtual or gaming worlds, darknet activities, newsgroups, weblogs, e-mail and internet connected applications on mobile devices.

Phishing

Phishing describes the malicious attempt of acquiring sensitive information through contact with victims via e-mail or other digital communication forms. This contact will appear to be legitimate and will most often require the victim to click a link leading to a malicious website. At this website the victim will be prompted to reveal the desired information without creating suspicion about the malicious circumstances.[21]

Phishing attacks are often carried out in waves (broad attacks) created with a high level of creativity and concealment, making them difficult to safeguard against. Phishing attacks are generally categorised as a social engineering technique. Spear phishing is a more advanced and focused form of phishing. Spear phishing generally targets specific individuals and requires a larger and more focused effort from the attacker.

By acquiring personal information about the victim the attacker is able to conduct the phishing attack utilising this data and increase the chance of a successful attack.

The Onion Router (TOR)

The Onion Router (TOR) is open source software originally aimed at providing Internet users proxy like functionality when using the Internet. Through the use of TOR, a user's Internet traffic is encrypted and routed in specific ways to achieve security and anonymity. This functionality is valued by a long list of users including journalists, citizens in oppressive countries and users with security interests.

The main way for users to access the internet or associated darknets through TOR is by using the TOR Browser Bundle, which is a modified browser setup that is pre-configured to connect to the network. The browser bundle is released and updated by the group of developers currently running the TOR Project.

TOR supports a so-called TOR Hidden Services Protocol that allows users to run Internet services such as websites and marketplaces, instant messaging services and e-mail services, as part of the TOR network. The hidden service inherits the security and anonymity functionality from the TOR network and as such to some extent is protected against identification and disruption.

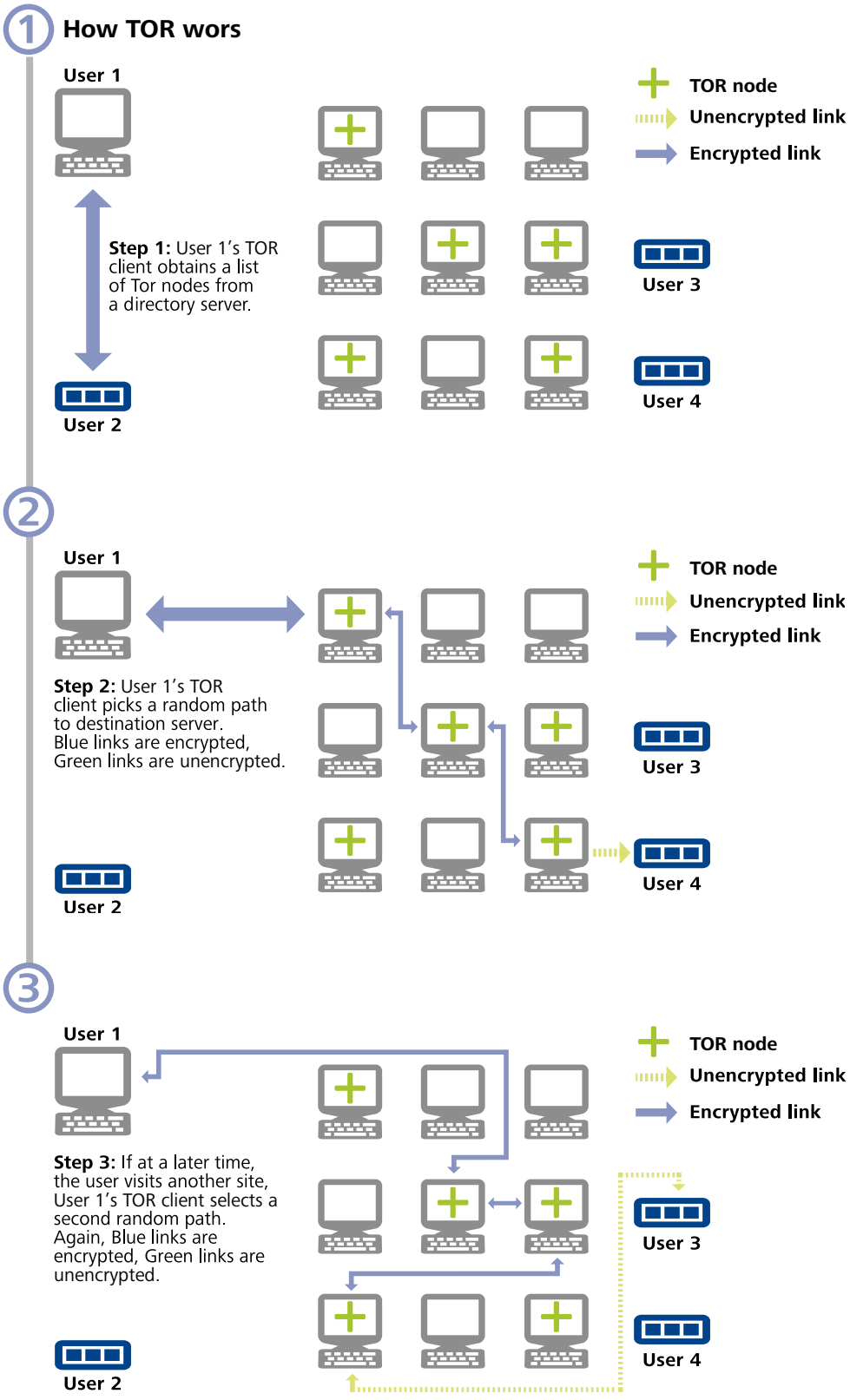
TOR hidden services include websites, marketplaces and online services comparable to those known from the open internet. Each hidden service is allocated a specific .onion IP-address containing 16 digits followed by the .onion designation. A customer who wants to use a hidden service must use the .onion address to establish the contact and get access to the services that are offered by the provider. 22 It must be noted that .onion is not a generic top level domain that is established in accordance with the ICANN DNS Policy.[23]

[21] Phishing will thus most often include the registration and use of a domain name that is similar to the domain name of the company that the sender passes off as representing. See Torsten Bettinger: Uniform Domain Name Dispute Resolution Policy, paragraphs IIIE.376-377,in Domain Name Law and Practice. An international Handbook, 2nd. Ed. 2015.

[22] Information on how to establish and set up a Hidden Service as well as the functioning of the .onion IP-address system is found at https://www.torproject.org/docs/hidden-services.html.en

[23] https://www.icann.org/policy

Fig. 5: The Onion Router



Virtual worlds

Virtual worlds[24] is most frequently used as a term that describes the many different types of multiplayer online games and other multiuser interactive worlds. Usually a virtual world is 'populated' by avatars that are created by the individual users and who simultaneously and independently explore the virtual world and who takes part in its activities. It is also possible for the users to communicate with each other.

[24] TRADEMARKS AND THE INTERNET, WIPO document SCT/24/4, 2010, and http://dictionary.reference.com/browse/virtual-environment

4. The framework for the analyses and the developed tools

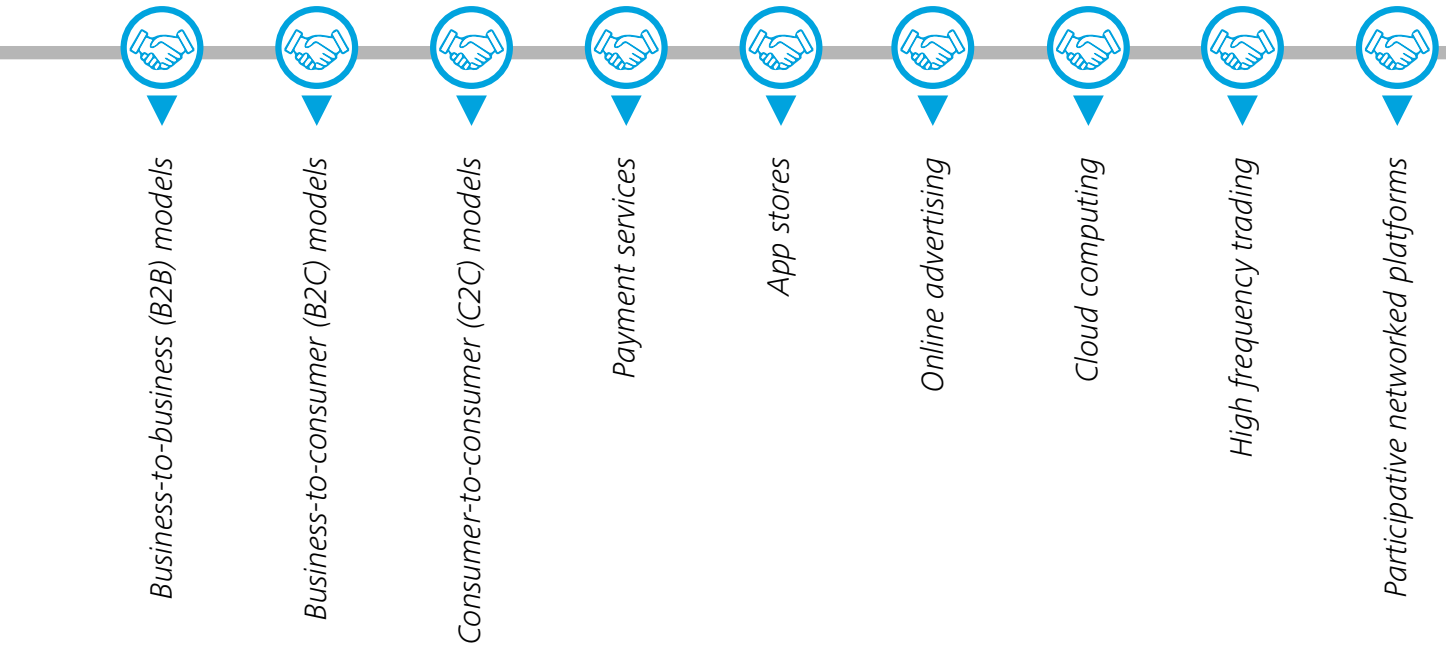
4.1 On business models and online business models in general

A business model is a model that describes the method or the means by which a company strives to create value from its business. A business model will include the various aspects of the company's strategy to generate economic value, including how it produces, distributes and prices its products or services, and ultimately, how the company gains its revenue.[25]

There is a wide variety of general business models such as manufacturer, retailer and distributor, and more specific models such as leasing, franchising and subscriptions. These business models are well-known and have been applied for many years in the offline market.

Although the basic features of a number of these business models are also applied by businesses operating online, they have been adapted to meet the many technical aspects of the digital media and to meet the often profound changes in customer behavior.

In addition, to the adapted versions of well-known business models the emergence and exponential growth in e-commerce has been initiated or increased by a number of new business models. In a recent report the OECD defined and described a number of generally applied online business models.[26]

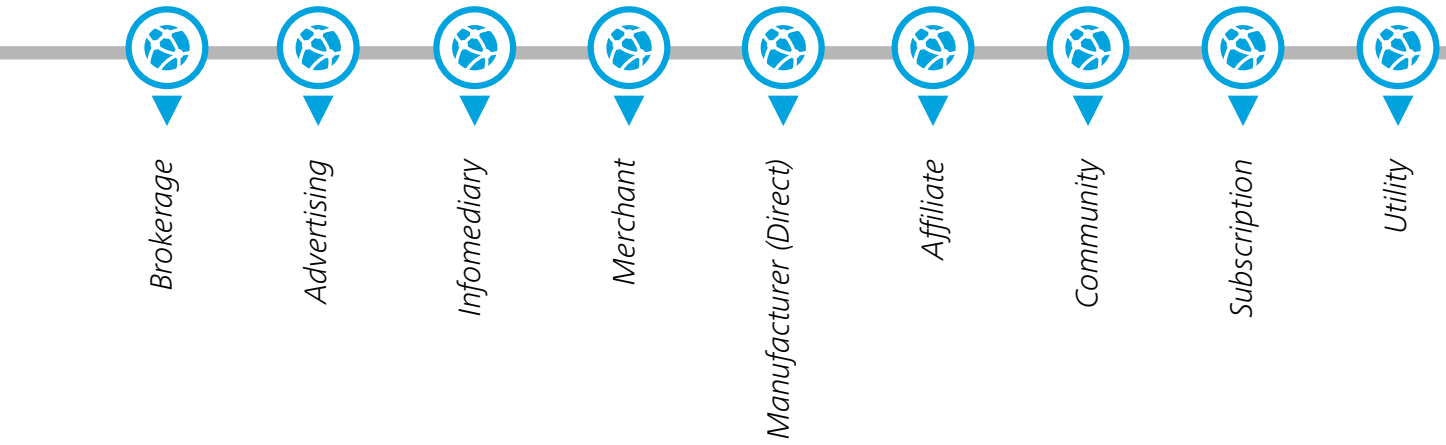


[25] Andrea Ovans: What is a business Model? In Harvard Business Review, 01.23.20015 accessible at https://hbr.org/2015/01/what-is-a-business-model http://lexicon.ft.com/Term?term=business-model.

[26] 'The digital economy, new business models and key features', in OECD, addressing the Tax Challenges of the Digital Economy, OECD Publishing, Paris, 2014: http://dx.doi.org/10.1787/9789264218789-7-en, Appendix I

Other sources adopt a different perspective on the online business models such as Professor Michael Rappa[27] who introduced another taxonomy in 2010,[28] which is often referred to as 'The 9 business Models of the Web': [29]

Such 'merchant models' or 'manufacturer's direct models' are however only some of many variations of online B2B and B2C business models that exist.[31]



B2B (business-to-business) and B2C (business-to-consumer) models are well known business models in the offline world and the basic concept behind both models has been transferred to the online environment.[30] Online B2B models, that according to OECD count for the vast majority of e-commerce transactions, will thus often be online versions of traditional transactions in which a wholesaler purchases consignments of goods online from the manufacturer, but may also consist of providing goods and/or services to support other businesses. Also, online B2C business models are often online versions of traditional transactions, where the company uses its homepage as a storefront and its web-site as a store, through which they sell goods and services to the consumer and where the 'store' takes advantage of the technological possibilities related to e-commerce.

A business model, that also has some parallel in the offline world, but which has been booming in the online environment can be described as the 'brokerage model', a model in which an intermediary brings buyers and sellers ('vendors') together by publishing their information on the website and facilitating the transactions. The latter model is also the basic concept behind the numerous online trading platforms or Internet marketplaces that facilitates C2C (Consumer-to-consumer). Such marketplaces also exist on the Darknet.[32]

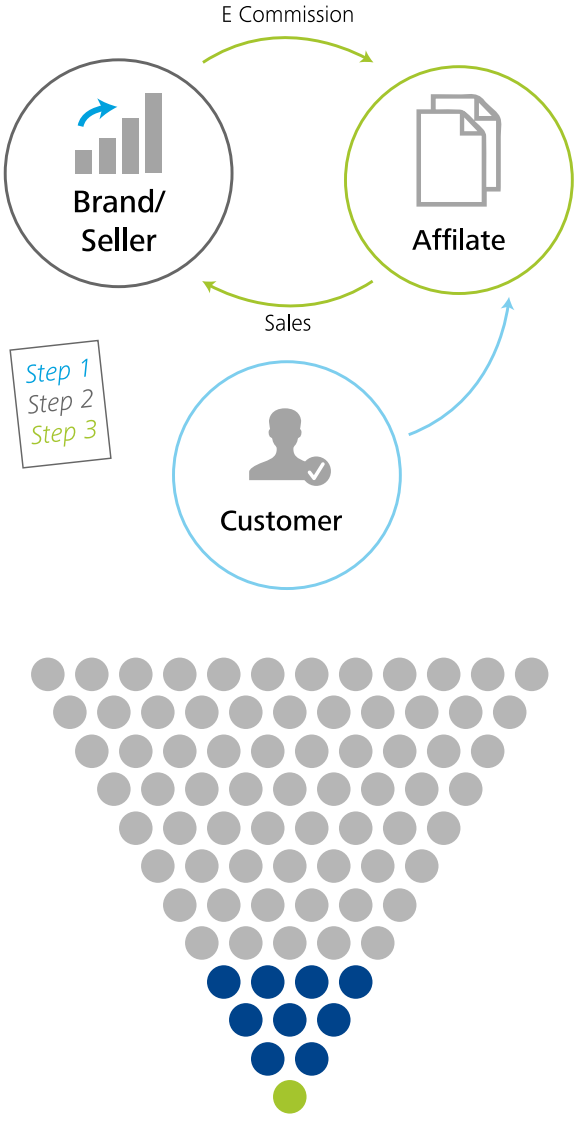
Vendors can and do use these marketplaces to trade IPR-infringing goods either with other businesses or with consumers.[33]

[27] Director of the Institute for Advanced Analytics and a faculty member in the Department of Computer Science at North Carolina State University.
[28] Professor Michael Rappa: Business Models On The Web http://digitalenterprise.org/models/models.html,
[29] See inter alia, 'Internet-Based Business Models Definition' by Victoria Duff, Demand Media, <http://smallbusiness.chron.com/Internet-based-business-models-definition-909.html> and 'The 9 types of online business models; which one do you use?' by Boris Veldhuijzen van Zanten http://thenextweb.com/entrepreneur/2011/05/25/the-9-types-of-online-business-models-which-one-do-you-use/
[30] OECD notes in this context that the vast majority of e-commerce consists of B2B transactions business and that B2C models were among the earliest forms of e-commerce
[31] See 'Internet-Based Business Models Definition' by Victoria Duff, Demand Media, http://smallbusiness.chron.com/Internet-based-business-models-definition-909.html
[32] The intermediary – the trading platform - may or may not charge the users of the platform for these services, depending on their revenue model.
[33] Most if not all marketplaces on the open Internet has instituted procedures whereby holders of intellectual property rights can file complaints against the individual offers for sale of IPR-infringing products and get the specific listing removed from the website, the so called 'notice and takedown'. Some Darknet markets appear to apply a similar procedure, but this has not been verified to work in practice.

Another widely used online business model is the 'affiliate model' where a given website participates in an affiliate program offered by a third party and which implies that products and services of this third party are advertised for sale at the website. The owner of the website receives a fee either for each reference or an actual sale depending on the revenue model.

In a recently applied version of the affiliate model it is the vendor himself that is the holder of the websites that form the affiliate network. This is done by using domain names that have recently expired and that then have been automatically re-registered by the vendor.[34] The domain names are used for websites that on the face of it appear to be independent web shops, but which are in fact redirecting its visitors to the vendors' actual web shop, as illustrated below:

Fig. 6: Affiliate Model



[34] This has been established in research made by EIT/Henrik Bjørner and which is available http://eit.dk/analyse/kina-paa-storindkoeb/. According to the presentation: Rogue Internet Pharmacies: An Update, by LegitScript a similar pattern characterises the online-pharmacy business. Legit Script has thus established that approximately 95% of Internet pharmacy websites are part of an 'affiliate network and that the number of networks are limited to 175 – 225 representing more than 40.000 online pharmacies.

Through this the vendor inherits the possible Google PageRank that the previous website held, they inherit any bookmarks of the previous website and other possible benefits such as access to dissemination of newsletters and e-mail marketing. These are benefits that would not be gained if the vendor registered a new domain name.

A somewhat connected model is the 'online advertising model' or rather the online advertising models. Online advertising is a big and growing business that generates huge revenues 35 for those operators that submit their websites to such advertising and for the various players that participate in the advertising networks,[36] and which of course triggers correspondingly high costs for the advertisers. Those of the operators that will be in focus in this study, are holders of websites that generate such revenue and which are used to infringe IPRs.[37]

As such many of the characteristics of the generally applied online business models are also present in the business models that are the subject of this study.

This is also the case as far as the application of a tool to describe and analyse each individual business model is concerned. In the book 'Business Model Generation' by Alexander Osterwalder & Yves Pigneur, published in 2010, the authors identified a number of key elements in any business model, which were then summarised and illustrated in the following widely used 'Business Model Canvas',[38] and in which the following 9 building blocks were identified as being the most important when establishing a new or analysing an existing business model (See fig. 7):

The initial analyses in this research project of a number of websites and related business models showed that it would be useful to apply an adapted version of the original Business Model Canvas when describing and analysing the business models that are the focus of this study.

Although many of the characteristics of the generally applied online business models are thus also present in the business models that are the subject of this study, it has been found to be useful to develop and apply an analytical method and a set of tools that reflect that the focus of this study is on business models that are used to infringe IPRs online and which makes it possible to categorise and describe any IPR-infringing business model in the online environment.

4.2 The developed tools for analysing online business models infringing intellectual property rights

The developed method is comprised of two main tools namely a taxonomic matrix and a canvas.[39] The purpose of the matrix is to set up a generally applicable systematization of IPR-infringing online business models and the purpose of the canvas is to provide a tool to analyse each individual business in a systematic way.

In addition to being used as the analytical method in this study, the method is meant to be a dynamic and flexible tool that will also enable businesses, authorities and other stakeholders to identify, dissect, analyse, describe and present future IPR-infringing business models and to relate them to the existing business models. The matrix may thus be expanded to include new digital platforms and to include further infringing activities as these may develop.

Fig. 7: Business Model Canvas

<table>
<tr><td rowspan="2">Key Partners</td><td>Key Activities</td><td rowspan="2">Value Propositions</td><td>Customer Relationships</td><td rowspan="2">Customers Segments</td></tr>
<tr><td>Key Resources</td><td>Channels</td></tr>
<tr><td colspan="3">Cost Structure</td><td colspan="2">Revenue Streams</td></tr>
</table>

[35] See: 'Digital Advertising on Suspected Infringing Websites. An Observatory report based on a study conducted by whiteBULLET Solutions Ltd,' 2015.
[36] http://www.adnetworkdirectory.com/
[37] Such online advertising models also apply to mobile advertising See Daniel Rowles: Mobile marketing, Kogan Page 2014, p. 181 ff.
[38] Used in accordance with the terms on http://businessmodelgeneration.com/canvas/bmc
[39] Based on the Business Model Canvas developed by Strategyzer AG available at strategyser.com.

4.2.1 The taxonomic matrix

As far as the digital platform is concerned the following 6 main variations will be applied:

A. Internet Site Controlled by Infringer
B. Third Party Marketplace
C. Social Media or Blog
D. Gaming or Virtual World
E. E-mail, Chatroom or Newsgroup
F. Mobile Devices

As to the IPR-infringing activities, the matrix distinguishes between the following 6 activities:

1. Domain Name or Digital Identifier Misuse of IPR
2. Physical or Virtual Product Marketing
3. Digital Content Sharing
4. Account Access or Codes to Digital Content Sharing
5. Phishing, Malware Dissemination or Fraud
6. Contributing to Infringement

Each combination of 'digital platform' and 'infringing activity' is then identified by a two character designation such as 'C5'. It must be noted that a given business model may qualify for more than one position, depending on the complexity of the model in question.[40]

Fig. 8: Taxonomic Matrix

Matrix: Online Digital Platform / IPR Infringing Activity		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

[40] As the canvasses in the Appendix reveals, this is actually the case for 13 analysed business models.

4.2.2 The adapted Business Model Canvas

The above reproduced Business Model Canvas has been adapted to serve the purposes of this study. In the adapted version of the canvas a set of building blocks that reflect those horizontal secondary features that best serve to describe the IPR-infringing business models has been applied in a comprehensive manner.

After having considered several options the following 9 building blocks or horizontal secondary features were identified as being the most useful: Digital platform, Products and services, Involved IP—right(s), Identification of the infringer, Revenue sources, Customer relations, Resilience against enforcement actions, Marketing channels, Identification of the infringer and Customer incentives.

The canvas of each of the identified business models is based on detailed case studies of one or in a few instances more concrete examples of the business model in question. Applying this method means that the canvas shall be regarded as illustrative of the main features of the business model in question, not as an exhaustive description that covers all aspects of each individual business representing the business model.

The case studies will form part of the background material, but since they may contain confidential or otherwise restricted material they will not form part of the public part of the study.[41]

Based on these parameters the following canvas template will be used to describe and illustrate each identified business model:

1. **Digital platform used:** In this part of the canvas it will be indicated whether the platform is on the open Internet or Darknet and whether the services are freely accessible or access is restricted.
2. **Products and services:** Description of what is actually offered on the website, such as IPR-infringing products or access to copyright protected works, including an indication of the variety, quality and availability as well as the pricing of the goods (if available).
3. **Involved IP-right(s):** Identification of which intellectual property right(s) that is affected by the specific activity.
4. **Identification of the infringer:** An indication of whether the name and contact information of the operator of the website is immediately available, including WHOIS information for the involved domain name (if applicable).
5. **Revenue sources:** A description of the revenue sources, including how revenue is obtained through direct sale/sales commission/subscription/ pay-per-click/advertisement/ donation/fraud. Payment options in fiat as well as virtual currencies are identified.
6. **Customer relations:** Includes elements such as accessibility, login features, delivery and shipment features and the return and refund policy. It is indicated whether the business model seems deceptive or non-deceptive towards the immediate customers.[42]
7. **Resilience against enforcement actions:** An indication of whether the provided service is subject to extra-judicial enforcement, such as notice-and takedown complaints. It is further indicated whether the provider of the service has indicated that they have taken steps to counteract possible enforcement actions.
8. **Marketing channels and Internet traffic features:** Description of how said business activities are marketed such as by the use of a trademark-infringing domain name, by use of legal as well as illegal traffic redirection,[43] participation in advertising networks or affiliate programs, and unsolicited marketing such as phishing mails.
9. **Customer incentives:** An indication of which initiatives – if any – the vendor has in place to retain and increase their customer and user base.

[41] It is also envisaged that further and even more detailed studies will be made in Phase II of this study.

[42] The term 'deceptive' is used to describe whether the business model deceives or is likely to deceive the customer that visits the digital platform on which the specific products or services are offered and which causes or is likely to cause the customer to take a transactional decision that he would not have taken otherwise. The term is thus used in accordance with article 6, 1 of the Unfair Commercial Practices Directive (Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005) according to which 'a commercial practice shall be regarded as misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise'.

[43] Traffic redirection is a term that is used to describe a tool whereby the operator redirect traffic from one website to another for example by 'persuading' a visitor to click on a link on the visited website or obtaining endorsements ('likes') for social media profiles by misusing a well-known brand to attract users to the profile and thus generating increased revenue.

CANVAS	Online Intellectual Property Rights Infringing Business Model: **Short Description of the Business Model**

Reference: Identification of legal decision (if any)

Date of Decision: Date of Analysis | Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Short summary description of the business model with focus on specific features or traits.

Indication of whether the business model is to be considered deceptive or non-deceptive.

In the Matrix, the specific digital platform and infringing activity is indicated with a grey background.

Matrix: Online Digital Platform / IPR Infringing Activity	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

In this part of the canvas it will be indicated whether the platform is on the open Internet or Darknet.

Indication of whether the services are freely accessible or access is restricted.

Products and Services:

Description of what is actually offered on the website, such as non-genuine products or access to copyright protected works, including an indication of the variety, quality and availability as well as the pricing of the goods (if available).

Involved IPR(s):

Identification of which intellectual property right(s) that is affected by the specific activity including trademarks, copyrights and related rights, protected databases, design rights and patents.

Identification of Infringer:

An indication of whether the name of and contact information of the operator of the website is immediately available, including WHOIS information for the involved domain name (if applicable).

Revenue Sources:

A description of the revenue sources, including how revenue is obtained through direct sales, sales commission, subscription fees, pay-per-click, advertising, donations or fraud. Payment options in fiat as well as virtual currencies are identified.

Customer Relations:

Description of elements such as accessibility, login features, delivery and shipment, and return and refund policy. It is indicated whether the business model seems deceptive or non-deceptive towards the immediate user and customers.

Resilience Against Enforcement Action:

An indication of whether the provided service is subject to extra-judicial enforcement, such as notice-and takedown complaints. It is further indicated whether the provider of the service has indicated that steps to counteract possible enforcement actions has been taken.

Marketing Channels and Internet Traffic Features:

Description of how the business activities are marketed such as by the use of a trademark-infringing domain name, by use of legal as well as illegal traffic redirection, participation in advertising networks or affiliate programs, and use of unsolicited marketing such as phishing mails.

Customer Incentives:

An indication of which initiatives – if any – the vendor has in place to retain and increase the user and customer base.

5. Key findings of the analyses of the 25 business models

Based on the above mentioned theoretical framework and the developed tools the study has identified 25 business models. The canvasses of each of the business models are included in the Appendix to this report. In the following paragraphs where the key findings of the study are outlined, references will be made to the canvasses in the text[44] by referring to the designated number of the canvas and a short description of the business model based on the following inventory of the analysed business models.

Open Internet Marketing Misusing IPR in Domain Name or Digital Identifier	
Canvas 1	Cybersquatting
Canvas 2	Domain Name Parking
Canvas 3	Affiliate Marketing Making Unauthorised Trademark Use in the Domain Name
Canvas 4	Marketing of IPR-infringing Products While Misusing the Related Trademark in the Domain Name
Canvas 5	Marketing of Non-Genuine Products on Website Making Use of an Unrelated Trademark in the Domain Name
Open Internet Marketing Without Misusing IPR in Domain Name or Digital Identifier	
Canvas 6	Online Pharmacy Marketing Prescription Medication
Canvas 7	Website Marketing Applied Arts Replica
Canvas 8	Marketing Goods or Digital Content on Third Party Online Wholesale Marketplace (B2B)
Canvas 9	Sale of Non-Genuine Goods through Social Media Networks
Canvas 10	Virtual Product Marketing in a Virtual World
Darknet Hidden Services	
Canvas 11	**A.** Darknet TOR Hidden Service User Account Shop
	B. Darknet TOR Hidden Service User Account Shop Vendor
Canvas 12	Darknet TOR Hidden Service E-book Library
Canvas 13	Darknet TOR Hidden Service Marketing Weapons and Firearms
Canvas 14	**A.** Darknet TOR Hidden Service Marketplace for Goods and Services
	B. Vendor on Darknet TOR Hidden Service Marketplaces Marketing Storage Media Preloaded with Digital Content
Canvas 15	Darknet TOR Hidden Service Marketplace For Protected or Sensitive Information
Phishing, Malware Dissemination and Fraud	
Canvas 16	Spoofing Website Making Unauthorised Use of a Trademark
Canvas 17	Phishing E-mails Making Unauthorised Use of a Trademark
Canvas 18	Android Smartphone Application Making Unauthorised Use of a Trademark, Providing Access to Pornographic Content and Disseminating Malware
Canvas 19	Malware Dissemination from Website Making Unauthorised Use of a Trademark
Canvas 20	Fraudulent use of the Trademark of a Trademark Registration Office
Digital Content Sharing on Open Internet	
Canvas 21	Website with Links to Digital Content
Canvas 22	Website Contributing to Video Streaming
Canvas 23	Torrent Website
Canvas 24	File Sharing Cyberlocker
Canvas 25	Television Streaming

[44] Each reference in the text contains a hyperlink to the specific canvas.

Based on the in-depth analyses of these business models the following points constitute the key findings of the study.

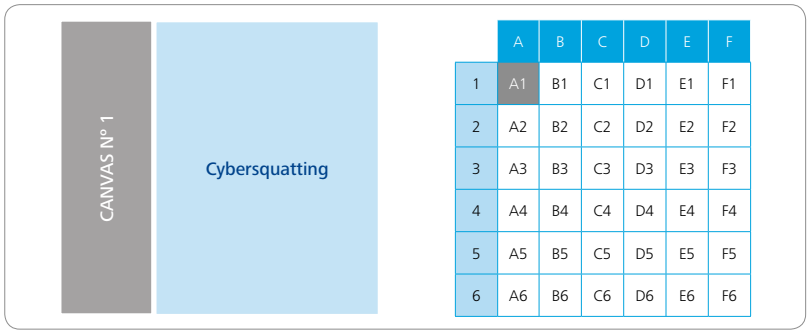
5.1 A variety of business models

It is apparent from the analyses of the identified business models that the operators that are engaged in IPR-infringing business activities are using a wide variety of business models as the following overview of the analysed business models plotted into the taxonomic matrix illustrates:

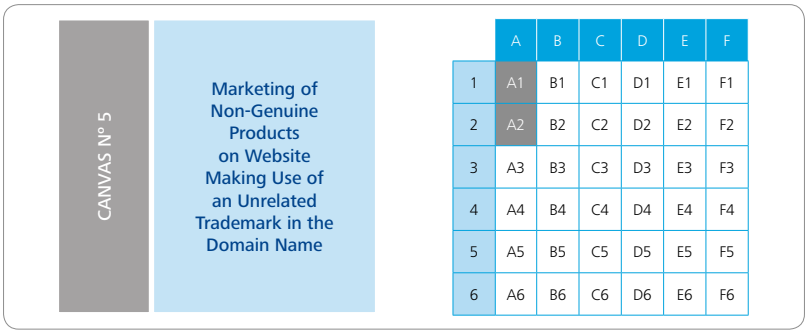
Matrix: Online Digital Platform / IPR Infringing Activity		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

As indicated above in chapter 06 many of these business models are based on generally applicable business models, i.e. business models that can be used and are being used for commercial activities that are entirely legitimate, such as sale of products on B2B or B2C marketplaces and participation in advertising networks and affiliate marketing schemes.

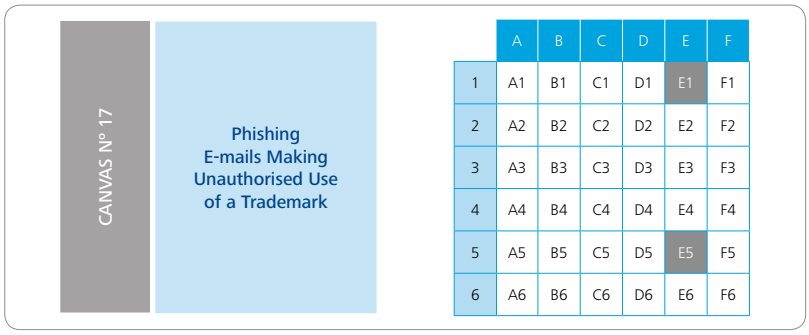
At the same time, it is obvious that some of the business models gain revenue through activities that are meant to -and 'designed' to- take advantage of IPR-infringements such as the following business models which comprise cybersquatting, marketing of IPR-infringing goods and the dissemination of phishing e-mails.



	A	B	C	D	E	F
1	A1	B1	C1	D1	E1	F1
2	A2	B2	C2	D2	E2	F2
3	A3	B3	C3	D3	E3	F3
4	A4	B4	C4	D4	E4	F4
5	A5	B5	C5	D5	E5	F5
6	A6	B6	C6	D6	E6	F6



	A	B	C	D	E	F
1	A1	B1	C1	D1	E1	F1
2	A2	B2	C2	D2	E2	F2
3	A3	B3	C3	D3	E3	F3
4	A4	B4	C4	D4	E4	F4
5	A5	B5	C5	D5	E5	F5
6	A6	B6	C6	D6	E6	F6



	A	B	C	D	E	F
1	A1	B1	C1	D1	E1	F1
2	A2	B2	C2	D2	E2	F2
3	A3	B3	C3	D3	E3	F3
4	A4	B4	C4	D4	E4	F4
5	A5	B5	C5	D5	E5	F5
6	A6	B6	C6	D6	E6	F6

In all three models the operator takes advantage of the often [45] easy and cheap strategy to register domain names that are identical or similar to existing brand names (trademarks).

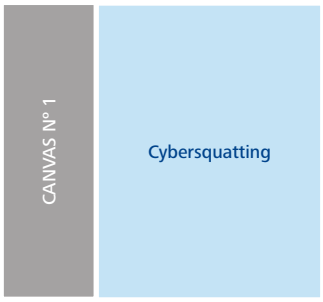
[45] The eligibility criteria as well as the price for registering domain names vary from top-level domain to top-level domain. Information on the various policies and prices are available at several online resources and in Domain Name Law and Practice. An International Handbook, Torsten Bettinger and Allegra Waddell (ed,), 2nd Edition, Oxford University Press, 2015.

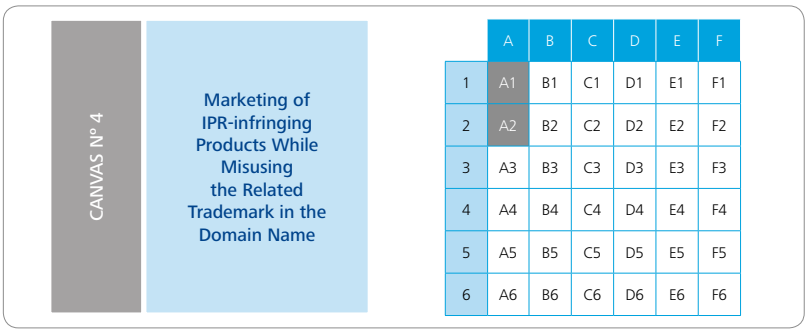
5.2 Affected intellectual property rights

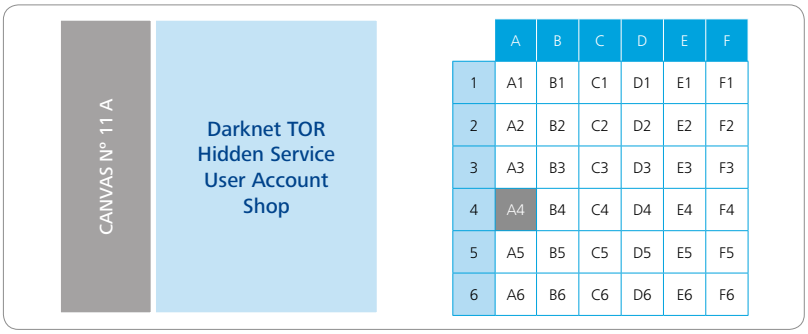
Although it falls outside the scope of this phase of the study to make a determination of which IPRs that are the most infringed in the online environment, the performed case studies primarily include trademarks (18 out of 25) and copyrights (17 out of 25) but there are also examples of activities that involve infringements of design rights and possibly also of patents.[46]

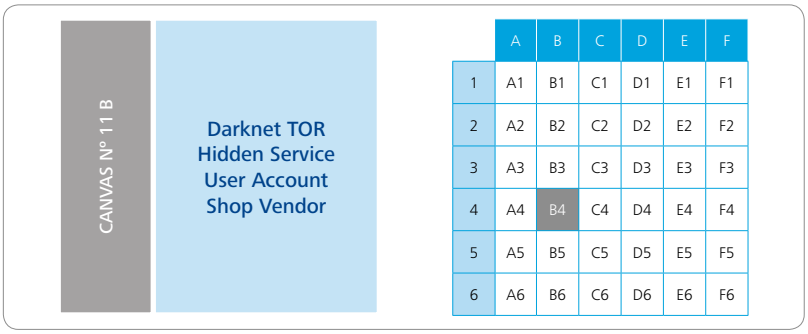
In addition, some of the TOR marketplaces indicate that they offer items that may be infringing on protected databases.[47]

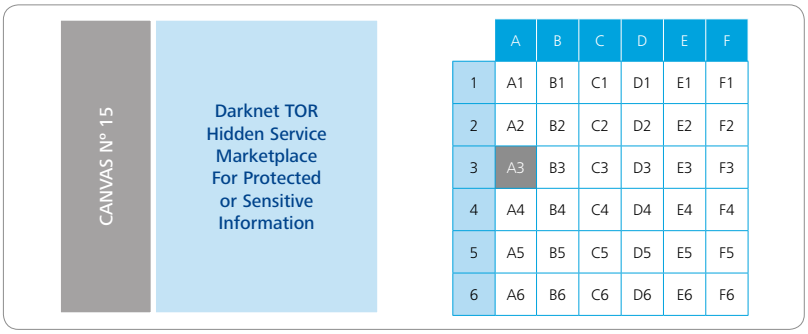
The following canvasses are examples of business models that comprise trademarks, copyright and related rights and database rights:

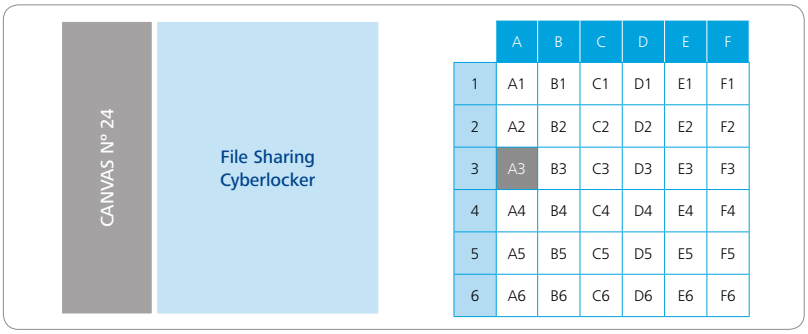






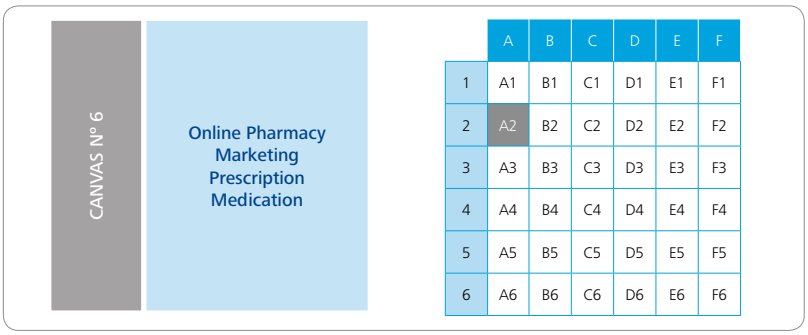


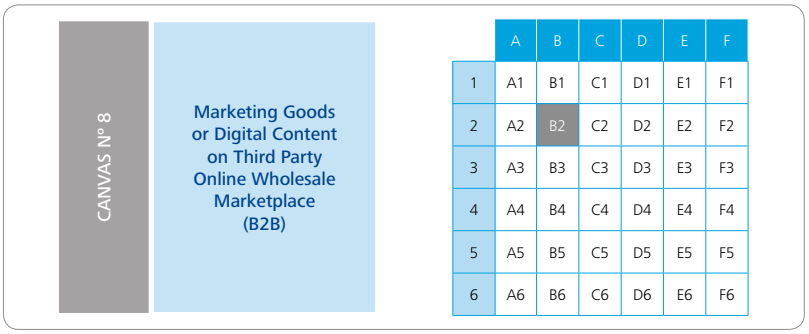


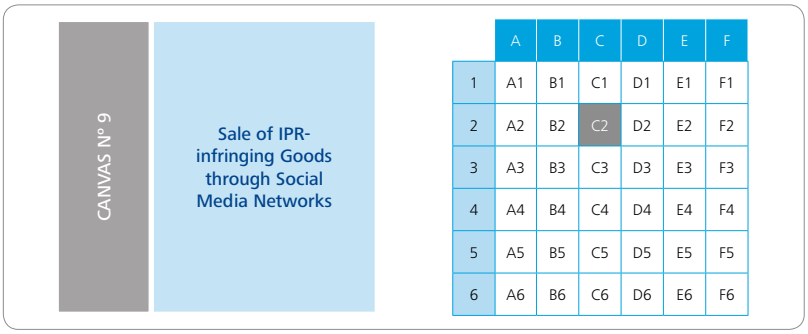


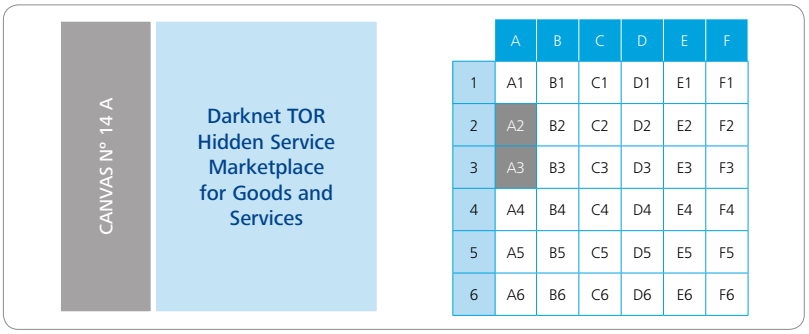
[46] It will require further analyses to determine whether patents are actually infringed – analyses that have not been carried out in this study.
[47] Such items are claimed to be available but the project team has not tested the validity of the claim.

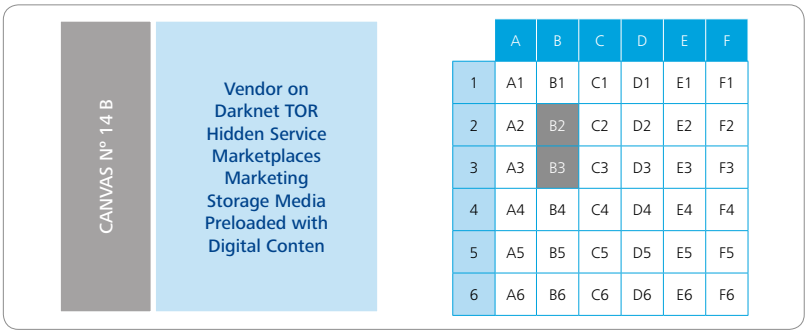
In 12 out of the 25 analysed business models the activities that are exercised are potentially infringing more than one IPR. The following canvasses are all examples of such business models, and they include sale of IPR-infringing products on websites that are controlled by the vendor himself, on third party marketplaces or through social media networks.







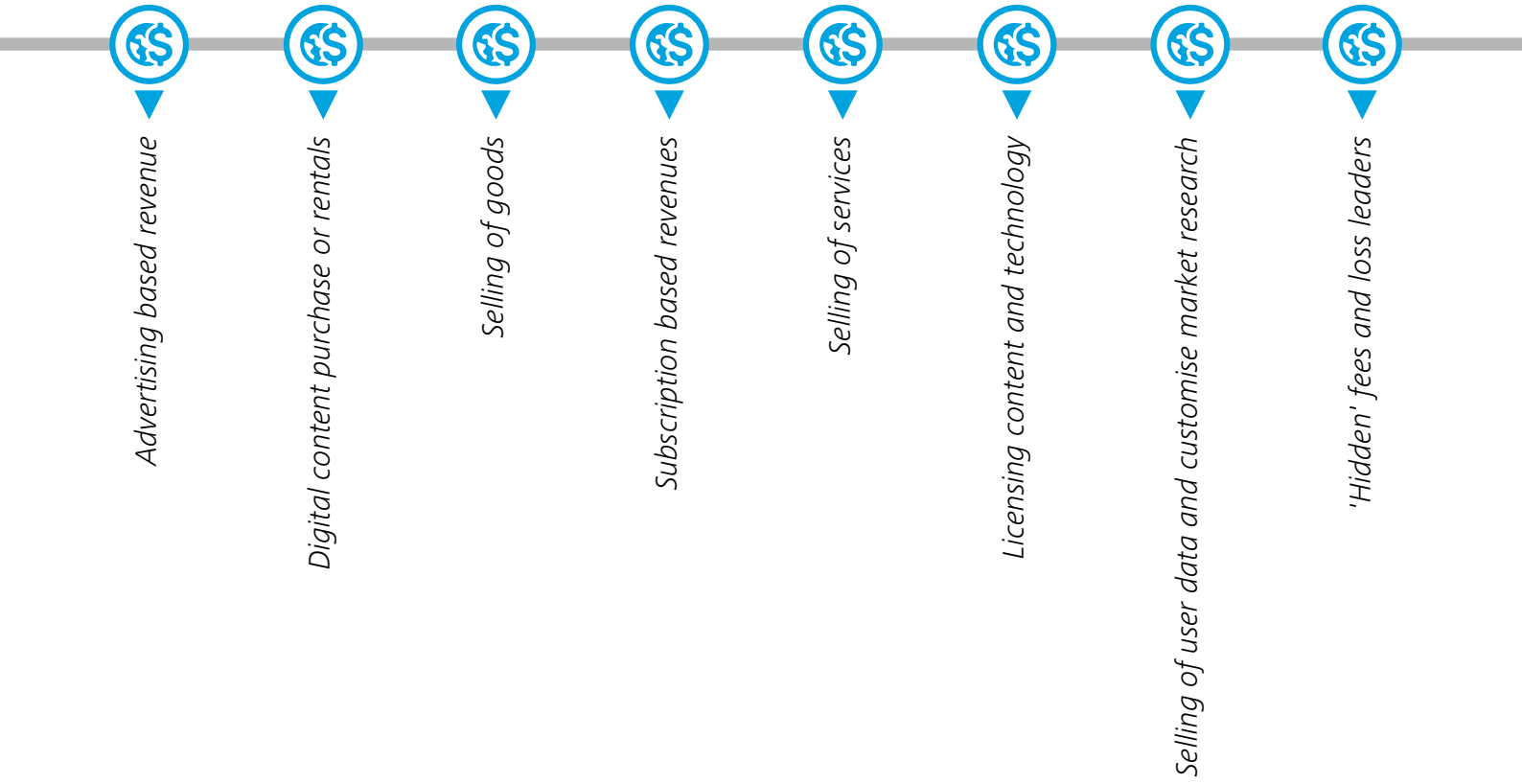




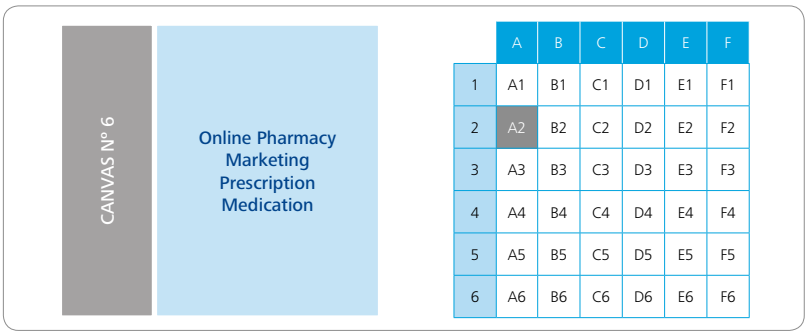
5.3 The revenue sources

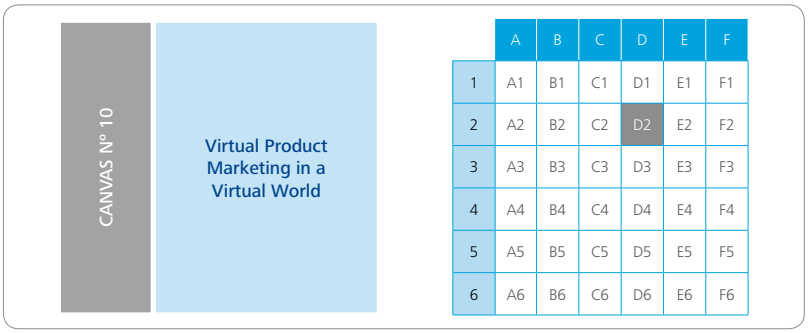
One of the key elements in analysing a business model is to identify the revenue sources. Consequently, it was highlighted in the Terms of Reference that the study should cover this aspect thoroughly and include business models that generate direct as well as indirect income through e.g. payments in fiat currencies, including subscriptions and donations, payments in digital, virtual currencies and revenue from advertisement and pay-per-click services.

The OECD document 'The digital economy, new business models and key features', contains a description of these generally applied revenue models in the digital economy: [48]



[48] OECD, 2014: 'The digital economy, new business models and key features', in OECD, Addressing the Tax Challenges of the Digital Economy, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264218789-7-en. There are other ways of dividing and describing these revenue models. see inter alia http://www.slideshare.net/maryasholevar/chapter-two-e-commerc-business-model



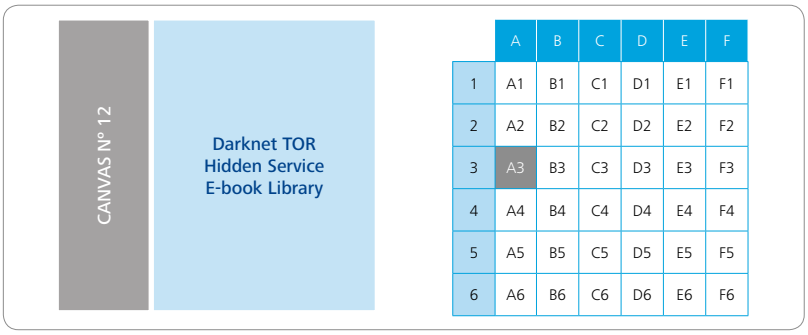


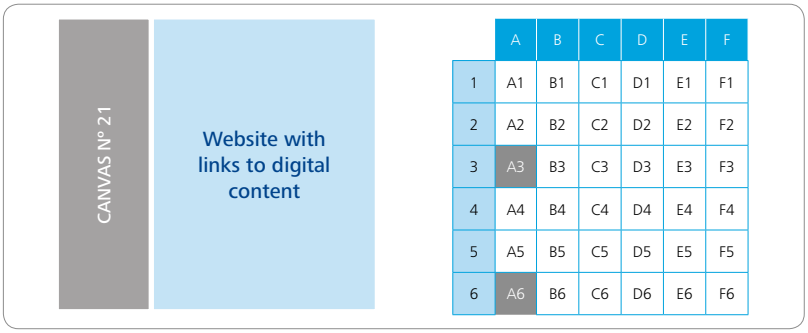
Based on the initial mapping of the 25 business models it was found appropriate to use the following designations and descriptions of the revenue sources of the analysed business models:

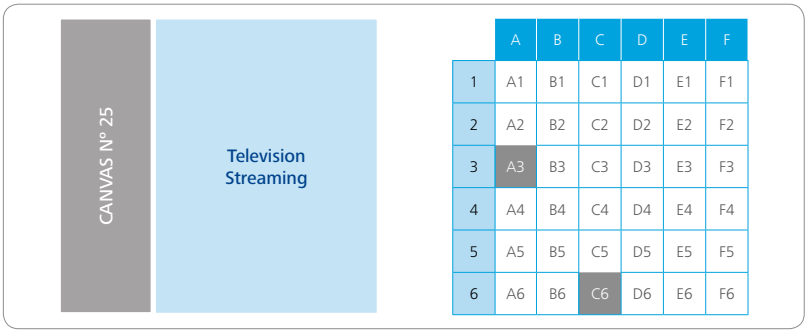
5.3.1 Direct revenue sources

Direct revenue sources are sources where the revenue is paid by the customer to the entity that offers the goods and services that the customer has ordered or subscribed to. Direct revenues include sales revenue, subscription fees and donations. The revenues may be paid directly by credit card or bank transfer, through intermediaries such as payment processors (Liqpay), or through virtual wallets (PayPal, Bitcoin, Linden Dollars et al.).

Around ¾ of the identified business models appear to generate their income wholly or in part from direct revenue sources such as in the following 5 business models.[49]







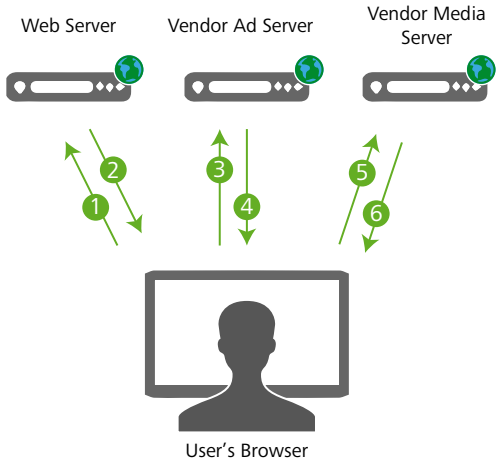
[49] Reference is made to the canvasses in the Appendix

5.3.2 Indirect revenue sources

Indirect revenue sources are sources where the revenue that is or may be generated is paid by other actors than the customer, who visits the website. The emergence of these indirect revenue sources is probably the most significant innovation in revenue generation in recent times,[50] and these revenue sources are widely used also for the IPR-infringing business models such as in the two depicted canvasses.[51]

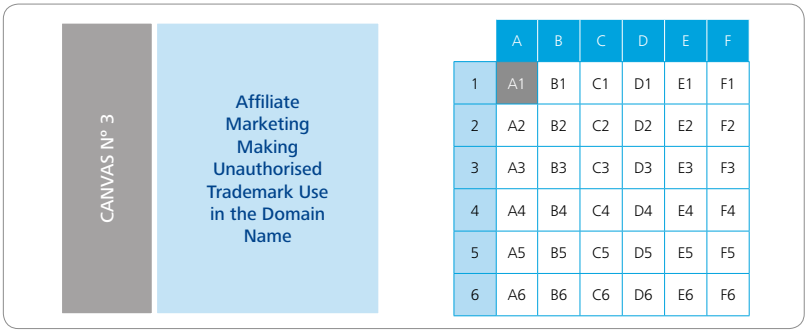
The three most used methods to generate indirect revenues[52] are PPM ('pay per impression') where the revenue is based on page views,[53] PPC ('pay per click') where the revenue is based on the number of clicks[54] and PPA ('pay per action') where the revenue is based on whether the visitor to the website initiates concrete actions on the advertisers landing page.[55] A variation of PPA is 'pay-per-download' and 'pay-per-install' which as the terms indicate trigger a payment if the visitor downloads a file or installs the software.[56]

Fig. 9: Ad Serving Model

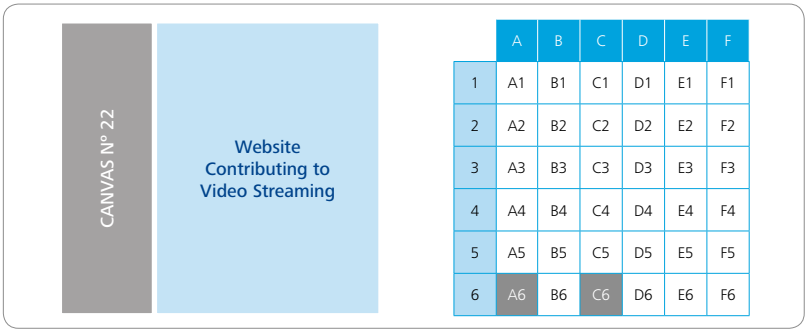


To receive PPM based revenue it is required that banner ads are posted on the website or profile page and that the holder of the website on which the banner ads appear participates in an advertising network running online behavioral advertising ads.

To receive PPC based revenue it is required that banner ads and/or links are posted on the website or profile page and that the holder of the website on which the banner ads appears participates in an advertising network running online behavioral advertising ads.



	A	B	C	D	E	F
1	A1	B1	C1	D1	E1	F1
2	A2	B2	C2	D2	E2	F2
3	A3	B3	C3	D3	E3	F3
4	A4	B4	C4	D4	E4	F4
5	A5	B5	C5	D5	E5	F5
6	A6	B6	C6	D6	E6	F6



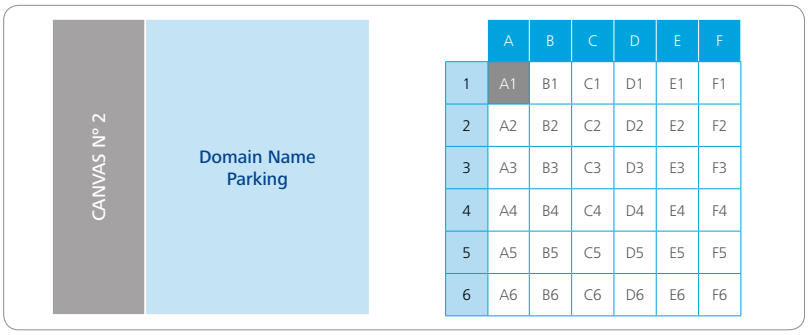
	A	B	C	D	E	F
1	A1	B1	C1	D1	E1	F1
2	A2	B2	C2	D2	E2	F2
3	A3	B3	C3	D3	E3	F3
4	A4	B4	C4	D4	E4	F4
5	A5	B5	C5	D5	E5	F5
6	A6	B6	C6	D6	E6	F6

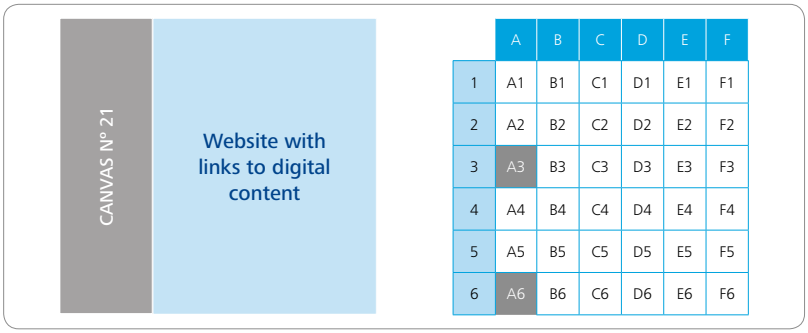
[50] See inter alia Mark Ostrofsky: 'Get Rich CLICK!. The Ultimate Guide to Making Money on the Internet',
[51] See 'Digital Advertising on Suspected Infringing Websites', EUIPO, January 2016..
[52] The three listed types of advertising based revenues, can be diversified further. In 'Get Rich CLICK!', p. 57 ff. has listed 30 different 'pay-per-' actions.
[53] Different calculation methods apply as explained in Annex A in 'Good Money Gone Bad'.
[54] Ibid.
[55] Ibid.
[56] Get Rich CLICK, p 58.

Some domain name registrars and web hosting companies offer standardised webpages for their customers (domain name registrants), that are automatically set up to host PPC- links, so called 'domain name parking.'[57] The technological platform behind parking sites may even be able to target the ad-links that will appear on the website in a way that the ads *'thematically correspond to the domain name will be displayed on your domain.'*[58 59]

To receive PPA based revenue it is required that the holder of the website on which the banner ads appear participates in an advertising network running online behavioral advertising ads. Another option for the holder of the website is to participate in an affiliate marketing scheme, in which the website is set up to promote products or services that are offered by a third party.[60] Many online platformshave developed extensive affiliate network programs in which participation requires that the vendoris 'allowed' to participate in it.

Some types of affiliate marketing require that the provider of the website downloads specific software and installs it on the website in such a way that the ads thematically correspond to the denotation of the domain name.





[57] 'Get Rich CLICK!', p. 115 and ' Domain Name Law and Practice', p. 1374 ff.
[58] https://sedo.com/us/park-domains/park-domains-overview/
[59] See WIPO Case No. D2015-0834
[60] See 'Get Rich CLICK!', p. 89 ff

5.3.3 Illicit revenue sources and fraud

Whereas the revenue sources that are discussed above are also used by completely legitimate companies, some of the IPR-infringing revenue will by the very definition of the nature of the activity be illicit or fraudulent. This is particularly so in the so-called 'phishing scams',[61] where consumers as well as companies are deceived by e-mails requesting the payment of a fee for a specific nonexistent service, to reveal access codes to bank account or credit card details, to reveal trade secrets or to 'update' or 'reactivate' their accounts thereby installing malware.

Fig. 10: Fictitious Phishing E-mails

From: Deri Bank [mailto: business@no-deribank.de]
Sent: 16.jun 2015 14:52
To: mail@hotmail.de
Subject: Business Netbank

Deri Bank

Dear business customer

You have received a notification.
Access your account

From: KreditKard [mailto: kreditkard@kreditkard.de]
Sent: 16.jun 2015 14:52
To: mail@hotmail.de
Subject: KreditKard Password

Verified by KREDITKARD

Protect your credit card

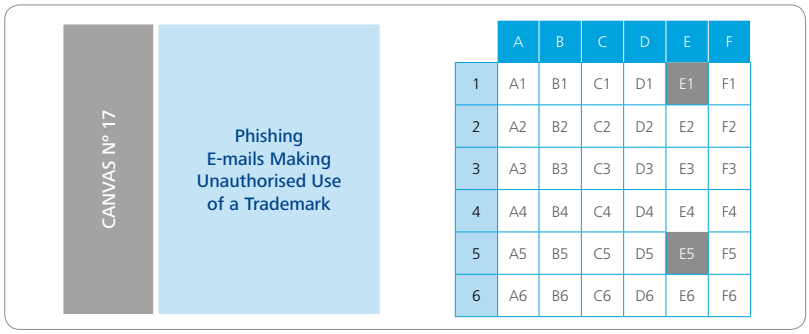
YYour credit card is registered in the program 'Verified by KREDITKARD ' to protect the card against unauthorised used. You must confirm the registration of the card by the filling out the required fields. Press 'Next' and then create a password. When you continue and to act with an Internet business with a logo Verified by KREDITKARD you will be prompted to enter your password authenticate your purchase.

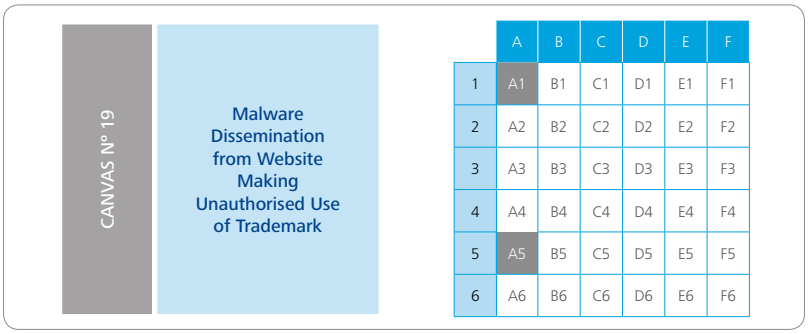
Next

© KreditKard Group 2015.

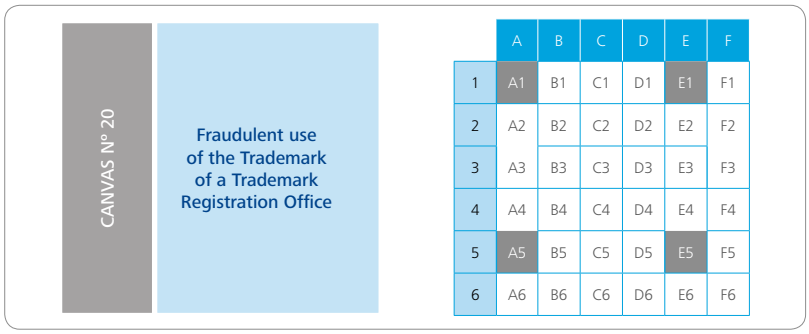
[61] I.e. fraudulent email messages that appear to come from a legitimate business such as a bank or a public authority.

The business models that are described in Canvas No 17 and No 19 are examples of business models that are based on such illicit revenue sources.

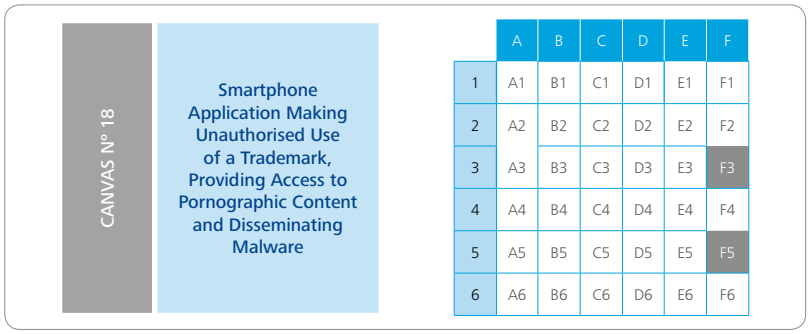




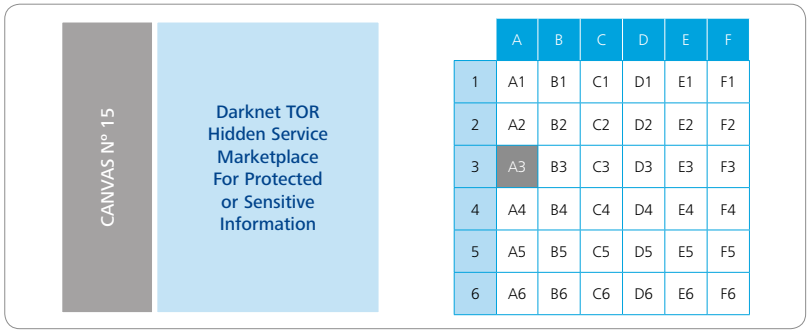
A similar business model is described in Canvas No 20 for a business model where the operator distributes e-mails that due to the fact that the operator uses a name and a logo that is a close imitation of the name and logo of an existing registration authority immediately gives recipients the impression that it is an official renewal reminder.

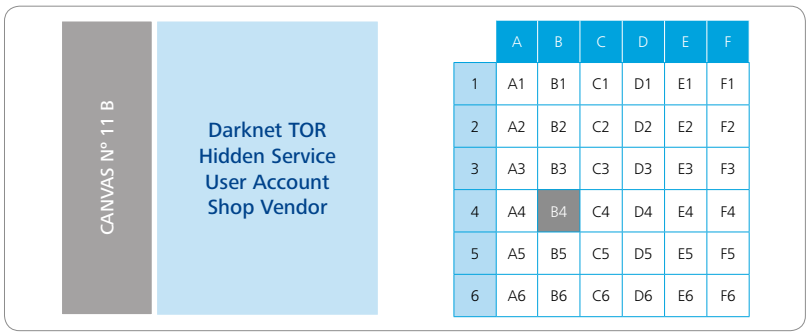


Another example is the distribution of ransomware for smartphones.



Access codes to bank accounts or credit card numbers can be used by the receiver to empty the account or to misuse the credit card but the receiver can also gain revenue through the sale of access codes or credit card numbers on Darknet marketplaces. Some of these marketplaces also appear to offer specific items protected by IPRs such as protected databases.[62] The information can be used by the receiver to blackmail the company or for industrial espionage but the receiver may also gain revenue through the sale of these trade secrets on Darknet marketplaces.





[62] Such items are claimed to be available but the project team has not tested the validity of the claim

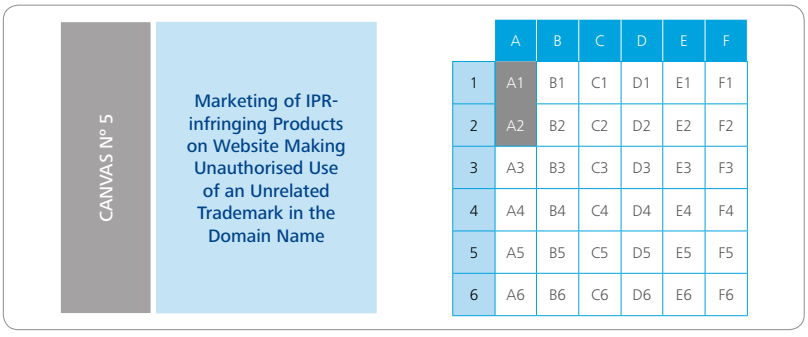
5.4 Marketing channels and tools

Irrespective of the concrete business model and its revenue sources, the operators that provide IP-infringing goods and services online are dependent on the fact that that users and customers actually visit their websites or notice their listings in online marketplaces. It is therefore necessary for these operators to apply the marketing tools that are generally available for legitimate online businesses including search engine optimisation (SEO) and search engine marketing (SEM).

5.4.1 Search engine optimisation

Search engine optimisation (SEO) is a term for the methods that can be used to promote a website's ranking in the generic search results in search engines such as Google, Bing and Yahoo!.[63] Each search engine operator has developed its own unique algorithm that is repeatedly changed. These algorithms are not publicly available, so it is not possible to accurately and comprehensively describe the criteria or 'signals' that are part of the algorithms, let alone their individual weights. However, it is generally assumed that the following signals are included in some algorithm: the 'titles', the 'keywords' and the 'descriptions' that are used in the website source code, the number of external links pointing to the website, the websites timelines, the websites textual content, the pictures on the website, its URL-address and thus the applied domain name, the number and type of referrals on social media ('likes') and most recently the concept of the website's 'authority'[64] which is a combination of different factors related to a website, including some of the above mentioned factors, but also the age and the size of the website.

Since some of the IPR-infringing websites appear high on listings of the generic search results, such as in Canvas No 5, it seems reasonable to assume that these vendors apply SEO techniques.



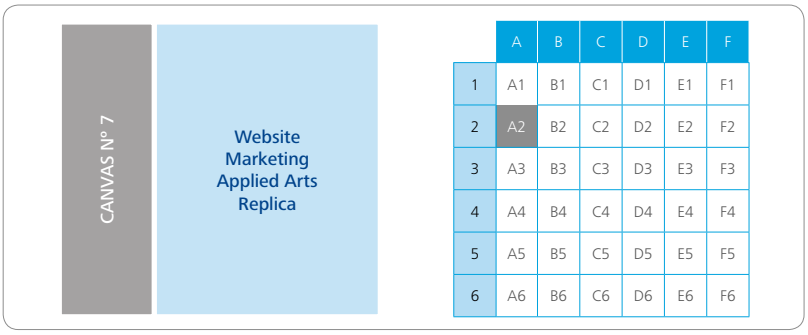
[63] http://www.techterms.com/definition/seo.

[64] Alan Charlesworth: 'Digital marketing. A practical approach', Routledge, 2nd ed. 2014,Caleb Whitmore, Sebastian Tonkin and Justin Cutroni: 'Performance Marketing with Google Analytics. Strategies and Techniques for Maximizing Online ROI', Wiley Publishing, inc., 2010. Several website are dedicated to monitor the constantly changing algorithms of the search engine operators such as http://moz.com/google-algorithm-change.

5.4.2 Search engine marketing

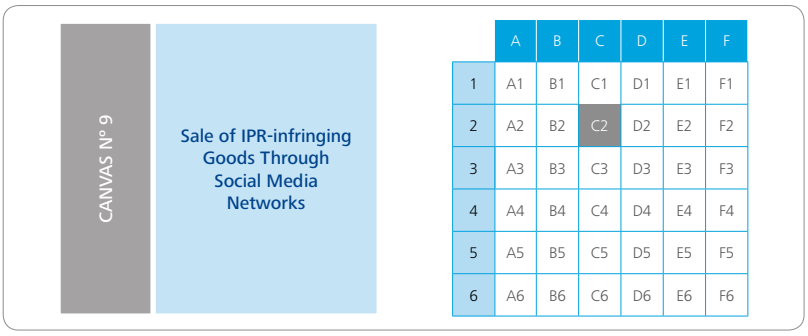
Search engine marketing (SEM) tools are the online marketing tools that consists of the paid links or advertisements on search engine operators' websites that are triggered by the keywords that the user enters. Best known is Google's AdWords advertising program[65], but similar facilities made available to advertisers of the other dominant search engine operators such as Yahoo![66] and Bing.[67] The individual advertiser can buy both generic terms such as 'sporting shoes' and 'anti-depressants' and the trademark of the products that is offered for sale as search terms.[68]

SEM may be used as a marketing tool also by the vendors of IPR-infringing products and services as was the case in Canvas No 7.



5.4.3 Promotion of IPR-infringing products on social media platforms

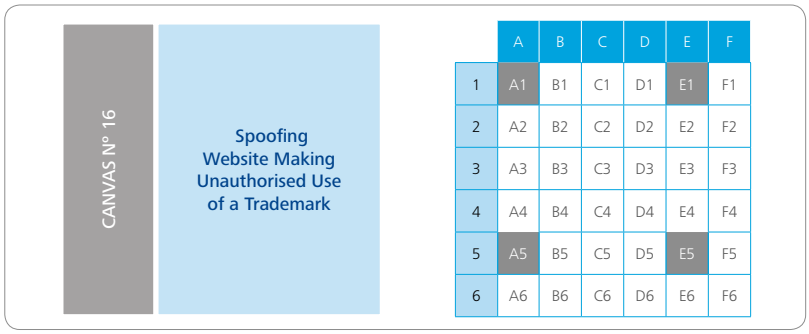
As the various social media platforms have expanded the possibilities for businesses to promote their products or services on the platforms these possibilities have been exploited by vendors of IPR-infringing products as well.



[65] http://www.google.dk/adwords.
[66] https://admanager.yahoo.com.
[67] http://advertise.bingads.microsoft.com/.
[68] The basic features are well explained by the CJEU in paragraphs 22 – 27 of the unified cases C-236-238/08 (Google).

5.4.4 Deceptive marketing

The marketing of IPR-infringing products or services will often be explicitly deceptive meaning that that marketing will cause the customer to take a transactional decision that he would not have taken otherwise.[69] This is particularly prevalent in business models where the provider uses a trademark infringing domain name as a URL or an e-mail address and where the associated website is an exact copy of or a close imitation of the brand owner's website,[70] often referred to as 'web page spoofing'[71] or 'content spoofing'.[72]



Dissemination of malware, phishing attempts and fraudulent activities are always deceptive towards customers, even if the IP-infringing activity as such is non-deceptive. An example will be sharing of copyright protected content that is (also) intentionally infected with malware.

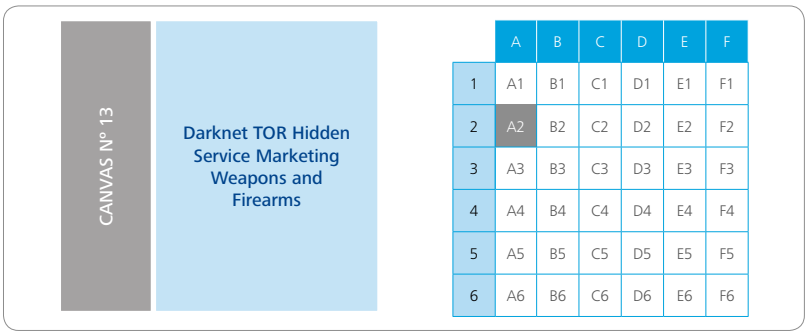
5.5 Customer relations and incentives

The study has also shown that the operators of IPR infringing businesses often act in a professional manner in the sense that the IPR-infringing business models are obviously designed so that they appear to the customers to be legitimate businesses. Many of the websites that are used for IPR-infringing activities do have apparently well-functioning user interfaces, and the operators use up-to-date digital marketing tools such as search engine optimisation, search engine marketing, and affiliate marketing schemes.[73]

[69] Reference is made to the definition of the term deceptive above in paragraph 06.02.02
[70] This has also been pointed out in the '2015 Situation Report on Counterfeiting in the European Union', EUROPOL/OHIM, 2015, p. 32-33
[71] http://idtheft.about.com/od/glossary/g/WebpageSpoofing.htm
[72] https://www.techopedia.com/definition/13594/content-spoofing
[73] On one specific area namely the unauthorised distribution or sharing of copyright protected material in particular of film and music it appears that that the business models that have been developed for these purposes have been the drivers of the development of new business models,

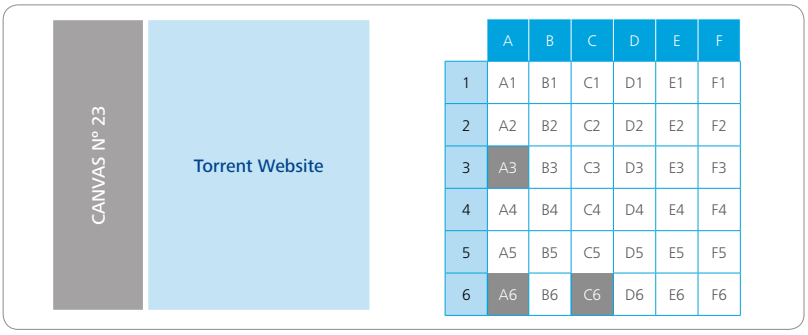
In a number of cases the providers of the IPR-infringing activitiesappear to offer the same customer services and use the same customer incentives as the legitimate businesses, such as return policies and discounts.

An example of this is Canvas No 13 where the provider offers to refund the paid purchase price if an order is lost or confiscated. [74]



5.6 Resilience against enforcement action

Most of the analysed business models use an Internet site that is controlled by the infringer: the infringing entity is the registrant of the domain name and the content on the website is made available by the infringer as in Canvas No 23.

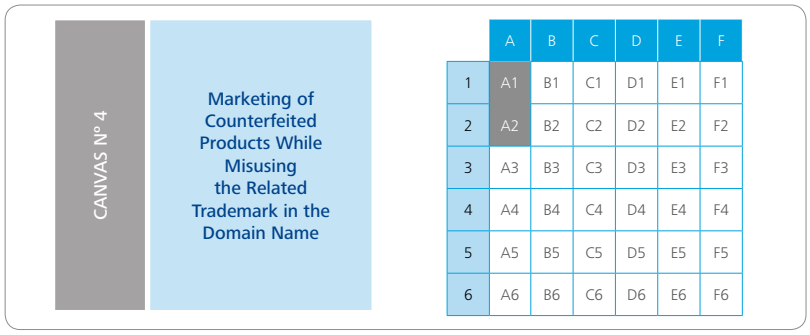


[74] It should however be noted that it has not formed part of this Phase 1 to test, whether those customer services and customer incentives are in fact applied.

The IPR-infringing activities may be confined exclusively to one or they may include various activities that are exercised on other digital platforms but which in the end lead the Internet user to the target site, either through advertisements on social media websites or the dissemination of phishing e-mails.

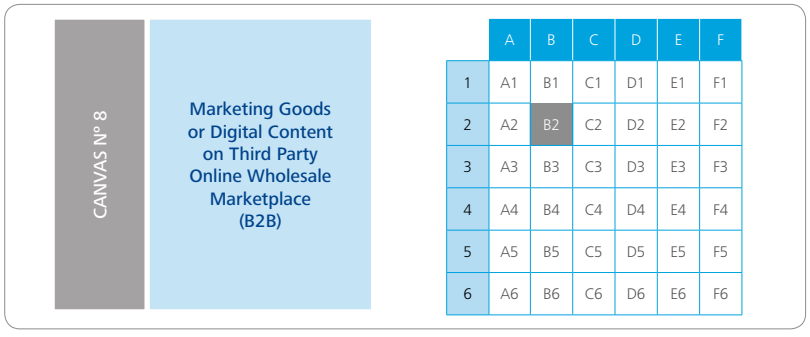
In such cases the right holder may institute civil court actions against the alleged infringer and in some cases the infringing activities may (also) be subject to criminal proceedings and sanctions.

If the domain name that is used for the Internet site is itself infringing on a third party trademark, the trademark owner may, instead of filing a court action, use the extra-judicial enforcement tools that apply to most abusive domain name registrations, either through the UDRP-procedure or through similar alternative dispute resolution procedures.[75]



It should be noted however that the operators of IPR-infringing businesses often either conceal their identities by using privacy shield services for the registration of domain names, or provide false or inaccurate contact details on the website.[76]

If the IPR-infringing activity takes place on a third party website such as a listing of infringing products on an online marketplace, such a listing will be subject to the enforcement scheme that is applied by the provider of the said marketplace, if any. These so called 'notice and takedown' procedures imply that a holder of an IPR, who finds that a listed product is infringing IPRs, can file a complaint ('notice') to the provider and request the listing to be removed ('takedown'). Filing such a notice does not usually require that the true identity of the vendor be known. It suffices that the complainant can refer to the vendors account name and the identification tag of the specific listing.



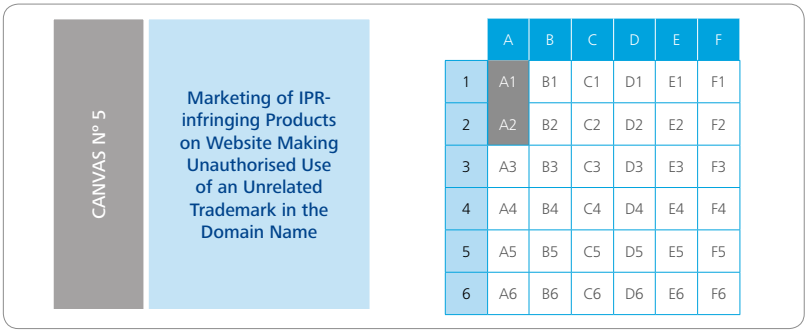
[75] Cf. The most recent of the many publications dealing with these proceeding is 'Domain Name Law and Practice. An International Handbook', 2nd Edition, 2015, edited by Torsten Bettinger and Allegra Waddell, Oxford University Press and the information on domain name disputes on http://www.wipo.int/amc/en/domains/

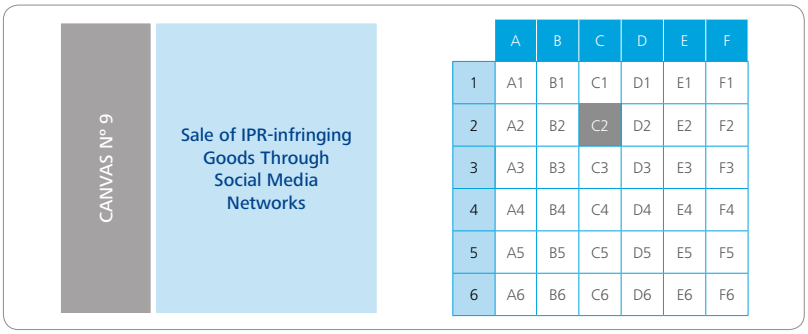
[76] As has been pointed out in the '2015 Situation Report on Counterfeiting in the European Union', EUROPOL/OHIM, 2015, p. 33.

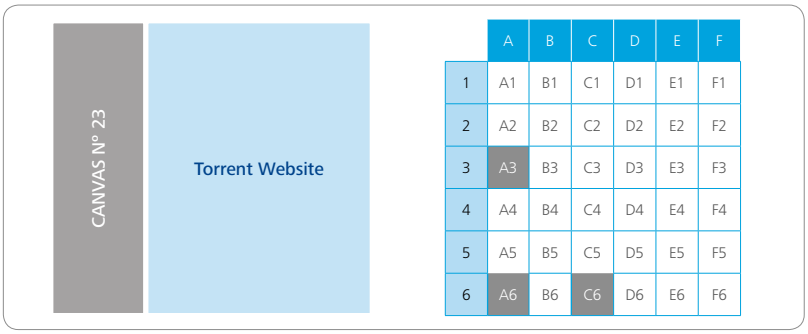
A number of the analysed business models are based on concepts that make it easy for the operators to be able to continue their business even in the event that an enforcement action has been initiated. Examples of this are sale of IPR-infringing goods on third party websites, where the vendor may create a new user profile or a new listing if his initial profile or listing was closed down, through which he can offer the same goods as before. Another example is where providers appear to be able to set up a new web shop under a different domain name but with the exact same design and content as the previous website immediately after the initial domain name that was used for the web shop has was transferred or deleted as a result of a legal action.

In addition, the study has revealed that some vendors openly state on their websites that they have included resilience against enforcement actions in their business model, such as by the simultaneous use of different domain names for the IPR-infringing activities.

The study has also found that it seems that an increasing number of providers of IPR-infringing goods and services are expanding or even moving their businesses to Darknet. Since the providers and possible affiliates are anonymous, they cannot be immediately identified. In addition, the aforementioned 'notice and takedown' procedures,[77] do not appear to be applied to the same extend on the Darknet marketplaces.







[77] And which are envisaged by the European Commission to play an important role in the creation of a Digital Single Market, See paragraph 3.3.2: 'Combatting illegal content on the Internet' in: 'Communication From The Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe', Brussels, 6.5.2015 COM(2015) 192 final.

5.7 The relationship between infringement of intellectual property rights and traditional cybercriminal activities

The last of the key findings of the study is that a number of business models are taking advantage of IPR infringements to carry out traditional cybercriminal activities.

Most e-mail phishing scams make use of well-known trademarks in the sender address and in the e-mail itself, thus deceiving the recipients into believing that the e-mail has been sent by the particular brand owner.

The phishing e-mail may contain ransomware, which is a malware that is used to infect and 'hijack' the recipients' computer, whereby the sender demands a 'ransom' in order to remove the malware from the computer. Recently, apps for mobile devices have also been infected with ransomware in this way.

Phishing e-mails may also include a link to a corresponding website that uses a domain name that includes the third party trademark and which has a user interface that is a close imitation of the particular brand owner's genuine website ('spoofing'). This type of phishing scam is used to deceive the recipient into disclosing access code or passwords to bank accounts or credit card details – information that was previously often obtained through illegal hacking.

It generally seems that some IPR infringements are carried out in technologically advanced combination with traditional cybercriminal activities with the aim of getting access to illicit revenue, personal data or other valuable information.

CANVAS Nº 16

Spoofing Website Making Unauthorised Use of a Trademark

	A	B	C	D	E	F
1	A1	B1	C1	D1	E1	F1
2	A2	B2	C2	D2	E2	F2
3	A3	B3	C3	D3	E3	F3
4	A4	B4	C4	D4	E4	F4
5	A5	B5	C5	D5	E5	F5
6	A6	B6	C6	D6	E6	F6

CANVAS Nº 17

Phishing E-mails Making Unauthorised Use of a Trademark

	A	B	C	D	E	F
1	A1	B1	C1	D1	E1	F1
2	A2	B2	C2	D2	E2	F2
3	A3	B3	C3	D3	E3	F3
4	A4	B4	C4	D4	E4	F4
5	A5	B5	C5	D5	E5	F5
6	A6	B6	C6	D6	E6	F6

CANVAS Nº 18

Smartphone Application Making Unauthorised Use of a Trademark, Providing Access to Pornographic Content and Disseminating Malware

	A	B	C	D	E	F
1	A1	B1	C1	D1	E1	F1
2	A2	B2	C2	D2	E2	F2
3	A3	B3	C3	D3	E3	F3
4	A4	B4	C4	D4	E4	F4
5	A5	B5	C5	D5	E5	F5
6	A6	B6	C6	D6	E6	F6

CANVAS Nº 19

Malware Dissemination from Website Making Unauthorised Use of Trademark

	A	B	C	D	E	F
1	A1	B1	C1	D1	E1	F1
2	A2	B2	C2	D2	E2	F2
3	A3	B3	C3	D3	E3	F3
4	A4	B4	C4	D4	E4	F4
5	A5	B5	C5	D5	E5	F5
6	A6	B6	C6	D6	E6	F6

6. Conclusions and perspectives

The aim of this study was to provide an overview of the different online business models infringing IPRs, assessing how they function, how they are financed, how they generate profits for their operators, what kind of content they disseminate and how large their user bases are with the purpose of providing policymakers, civil society and private businesses an enhanced understanding of these business models.

Based on the above key findings the following conclusions can be made:

- It can be observed that a number of the online business models infringing IPRs are based on generally applicable legal online business models, such as the operation of Business-to-Business (B2B) and Business-to-Consumer (B2C) websites, listings of products on third party marketplaces, streaming services and affiliate marketing. For such business models the revenue sources also appear to be the same whether they are direct sources such as sales revenue or indirect revenue such as pay-per click fees or income from providing advertising space.

- The online business models infringing IPRs differ from non-infringing models in the way that they are often clearly deceptive to the customers, since the operators purport to be legitimate providers of genuine legal goods, while the goods they offer are in fact IPR-infringing. Sometimes the deceptive nature of the business model is connected to distinctively fraudulent activities, phishing and dissemination of malware. In some instances, the infringement of the IPR is carried out completely openly, but the business model is however still deceptive towards the customers due to dissemination of malware.

- It is thus apparent that specific online business models have been developed and intentionally designed to benefit from infringement of IPRs. Such online business models include in particular those models that gain their revenue from phishing e-mails, dissemination of ransomware or other fraudulent activities. But also the widespread registration and use of domain names that contain third party trademarks, and which are used for a variety of purposes including parking sites, that generate pay per click revenue or are used to redirect internet traffic to the registrants own website, can be characterised in this way.

- • If the IPR-infringing activities take place on a website that is controlled by the IPR-infringer it is in principle possible for a rights holder to initiate enforcement actions against the vendor either through court actions, filing of criminal complaints or through extra judicial enforcement mechanisms. However, these vendors often either conceal their identities by using privacy shield services for the registration of their domain names, or they provide false or inaccurate contact details on the website. This hampers and may sometimes preclude any initiative to enforce the infringed IPRs and stop the infringing activities and on this point these operators clearly distinguish themselves from the operators of non-infringing businesses.

- It also seems that an increasing number of providers of IPR-infringing goods and services are expanding or even moving their businesses to the darknet or are offering their services on both the open and the hidden part of the internet. This development will have a serious impact on the possibilities to counter IPR-infringements through the existing means of enforcement, as the providers are more anonymous and cannot be easily identified. In addition, the 'notice and takedown' procedures which are widely used by the operators of marketplaces and other internet service providers on the open part of the internet do not appear to be applied to the same extent on the darknet.

- In cases where it is possible to identify and take enforcement action against a provider of an IPR-infringing activity, the study shows that a number of the analysed business models are based on concepts that make it easy for the providers to be able to continue their businesses even in the event that an enforcement action has been initiated. In some of the business models the providers openly state to their customers that they have included resilience against enforcement actions in their businesses model.

- Finally, it can be observed that the borderline between IPR-infringing activities and traditional cybercriminal activities is becoming blurred. Phishing e-mails may thus contain ransomware, which is malware that is used to infect and 'hijack' the recipient's computer, whereby the sender demands a 'ransom' in order to release malware from the computer, or other malware variations. Spoofing websites and phishing e-mails may also be used deceive the recipients into disclosing private access codes or passwords to bank accounts or credit card details,previously often obtained through illegal hacking.

7. Bibliography and references

Selected references

'2015 Situation Report on Counterfeiting in the European Union', A joint project between Europol and the Office for Harmonization in the Internal Market, Europol/OHIM, 2015

OECD (2014), 'The digital economy, new business models and key features', in OECD, 'Addressing the Tax Challenges of the Digital Economy', OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264218789-7-en

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 'A Digital Single Market Strategy for Europe.' Brussels, 6.5.2015 COM(2015) 192 final

'The Economic Cost of IPR Infringement in the Cosmetics and Personal Care Sector: report of a pilot study, Quantification of Infringement in Manufacture of Perfumes and Toilet Preparations sector ', Office for Harmonization in the Internal Market, 2015

'The economic cost of IPR infringement in the Clothing, Footwear and Accessories Sector', Office for Harmonization in the Internal Market, 2015

'Digital Advertising on Suspected Infringing Websites.' , Office for Harmonization in the Internal Market, 2016

'TRADEMARKS AND THE INTERNET', WIPO Document , SCT/24/4, 2010.

'ENFORCING INTELLECTUAL PROPERTY RIGHTS: AND ECONOMIC PERSPECTIVE', Document prepared by Carsten Fink, WIPO/ACE/5/6, 2009

'The revenue sources for websites making available copyright content without consent in the EU', INCOPRO, 2015

'BEHIND THE CYBERLOCKER DOOR: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions', DigitalCitizensAlliance, 2015

Unicri Report 'Counterfeit medicines sold through the Internet', 2010

'GOOD MONEY GONE BAD. Digital Thieves and the Hijacking of the Online Ad Business', DigitalCitizensAlliance, 2014

Research made by EIT/Henrik Bjørner and which is available http://eit.dk/analyse/kina-paa-storindkoeb/

'2011 Out-of-Cycle Review of Notorious Markets ', The Office of the U.S. Trade Representative (USTR):

'2012 Out-of-Cycle Review of Notorious Markets' , The Office of the U.S. Trade Representative (USTR):

'2013 Out-of-Cycle Review of Notorious Markets' , The Office of the U.S. Trade Representative (USTR):

'2014 Notorious Markets List,' The Office of the U.S. Trade Representative (USTR):

UK Intellectual Property Office IP Crime Report 2014/15: .

Torsten Bettinger, Allegra Wadell (ed): Domain Name Law and Practice. An international Handbook, Oxford University Press, 2nd ed. 2015

Gary S. Becker: Crime and Punishment: An Economic Approach, in Essays in the Economics of Crime and Punishment, 1974

Alan Charlesworth: Digital marketing. A practical approach, Routledge, 2nd ed. 2014

Mark A. Rosso, Bernard J. Jansen: Smart Marketing or Bait & Switch? Competitors´ Brands as Keywords in Online Advertising, WICOW´10, 2010

Daniel Rowles: Mobile marketing, Kogan Page, 2014,

Marc Ostrofsky: Get Rich Click!: The Ultimate Guide to Making Money on the Internet, , Free Press, 2013

Knud Wallberg: Brug af andres varemærker I digitale medier. Et bidrag til afklaring af varemærkerettens indhold og grænseflader, DJØF, 2015

Andrea Ovans: What is a business Model?, Harvard Business Review, 2015

Jurisprudence

England and Wales High Court of Justice, Chancery Division: [2013] EWHC 379 (Ch)

England and Wales High Court of Justice [2014] EWHC 3354 (Ch)

England and Wales High Court of Justice [2015] EWHC 3256 (IPEC)

Criminal Court of Appeal (Castellon, Spain), Resolution No.: 426/2014

United States District Court, Southern District Of Florida, Miami Division, Case No. 11-20427-Civ-Jordan

The Maritime and Commercial Court (Copenhagen, Denmark), cases V-0063-12 + V-0064-12

The Municipal Court of Copenhagen (Denmark), case SS90-15834/2015

The Municipal Court of Aalborg (Denmark), case 12-1319/2015

WIPO Case D2007-1912

WIPO Case D2010-0406

WIPO Case D2010-0966

WIPO Case D2011-1753

WIPO Case D2012-1125

WIPO Case D2014-0268

WIPO Case D2015-0025

WIPO Case D2015-0442

WIPO Case D2015-0834

WIPO Case D2015-1628

Danish Dispute Board for Domain Names, Case 2014-0200

Danish Dispute Board for Domain Names, Case 2015-0093

8. List of figures

9. Appendix. Inventory and listing of canvases

Inventory of the analysed business models

Open Internet Marketing Misusing IPR in Domain Name or Digital Identifier	
Canvas 1	Cybersquatting
Canvas 2	Domain Name Parking
Canvas 3	Affiliate Marketing Making Unauthorised Trademark Use in the Domain Name
Canvas 4	Marketing of IPR-infringing Products While Misusing the Related Trademark in the Domain Name
Canvas 5	Marketing of Non-Genuine Products on Website Making Use of an Unrelated Trademark in the Domain Name
Open Internet Marketing Without Misusing IPR in Domain Name or Digital Identifier	
Canvas 6	Online Pharmacy Marketing Prescription Medication
Canvas 7	Website Marketing Applied Arts Replica
Canvas 8	Marketing Goods or Digital Content on Third Party Online Wholesale Marketplace (B2B)
Canvas 9	Sale of Non-Genuine Goods through Social Media Networks
Canvas 10	Virtual Product Marketing in a Virtual World
Darknet Hidden Services	
Canvas 11	**A.** Darknet TOR Hidden Service User Account Shop
	B. Darknet TOR Hidden Service User Account Shop Vendor
Canvas 12	Darknet TOR Hidden Service E-book Library
Canvas 13	Darknet TOR Hidden Service Marketing Weapons and Firearms
Canvas 14	**A.** Darknet TOR Hidden Service Marketplace for Goods and Services
	B. Vendor on Darknet TOR Hidden Service Marketplaces Marketing Storage Media Preloaded with Digital Content
Canvas 15	Darknet TOR Hidden Service Marketplace For Protected or Sensitive Information
Phishing, Malware Dissemination and Fraud	
Canvas 16	Spoofing Website Making Unauthorised Use of a Trademark
Canvas 17	Phishing E-mails Making Unauthorised Use of a Trademark
Canvas 18	Android Smartphone Application Making Unauthorised Use of a Trademark, Providing Access to Pornographic Content and Disseminating Malware
Canvas 19	Malware Dissemination from Website Making Unauthorised Use of a Trademark
Canvas 20	Fraudulent use of the Trademark of a Trademark Registration Office
Digital Content Sharing on Open Internet	
Canvas 21	Website with Links to Digital Content
Canvas 22	Website Contributing to Video Streaming
Canvas 23	Torrent Website
Canvas 24	File Sharing Cyberlocker
Canvas 25	Television Streaming

CANVAS Nº 1

Online Intellectual Property Rights Infringing Business Model: Cybersquatting

Case study performed by the project team based on the legal decision in WIPO Case D2015-0025

Date of legal decision: March 5 2015. Date of analysis: October 1 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

The registrant of the domain name registers one or more domain names that contain a third party trademark. The domain name leads to a parking website which includes a number of pay-per- click links or advertisements. In addition, it is indicated either directly ('this domain is for sale') or indirectly (by being open to offers) that the domain name is for sale.

Deceptive business model.

Matrix: IPR Infringing Activity / Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet/Darknet:

Open internet platform using the trademark of a third party in the domain names under the generic top level domain .attorney and hosted on undisclosed server.

Freely accessible/restricted access: Freely available website.

Identification of Infringer:

Contact information available on the website, but is likely to be unusable. The identity of the infringer might be able to be established via the WHOIS register of the domain name registry. However WHOIS information is often incorrect for such websites.

Resilience Against Enforcement Action:

N/A.

Products and Services:

Sponsored links to or advertisements for other businesses.

Sale of the domain name itself.

Revenue Sources:

Revenue from direct sale if the domain name is sold and the revenue comes from pay-per- click (PPC) links or advertisements.

Involved IPR(s):

Trademark

Customer Relations:

The business model builds on attracting customers using the trademark of a third party.

Deceptive/non-deceptive business model:

The business model is deceptive due to the use of a trademark of a third party in the domain name.

Marketing Channels and Internet Traffic Features:

Search engine optimisation (SEO) to achieve a high search engine ranking, resulting in increased internet traffic (clicks and views).

Customer Incentives:

N/A.

« » Back to previous page

CANVAS Nº 2

Online Intellectual Property Rights Infringing Business Model: Domain Name Parking

Case study performed by the project team based on the legal decision in WIPO Case D2011-1753

Date of legal decision: December 2, 2011. Date of Analysis: October 1 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A website on the open internet using a domain name that contains the trademark of a third party.

The website contains automatically generated sponsored links to other websites or ads for other websites.

Deceptive business model.

Matrix: IPR Infringing Activity / Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open internet/darknet: Open internet platform using the trademark of a third party in the domain name under the generic top level domain .net and hosted on undisclosed servers.

Freely accessible/restricted access: Freely available website.

Identification of Infringer:

No contact information available on the website. The owner of the website might be identified via the domain name registry WHOIS. However WHOIS information is often incorrect for such websites.

Resilience Against Enforcement Action:

N/A

Products and Services:

Links to other websites that may or may not offer goods or services bearing the trademark that is included in the domain name.

Revenue Sources:

Revenue comes from advertisement, pay-per-click (PPC) links.

Involved IPR(s):

Trademark

Customer Relations:

The business model builds on attracting customers by use of the trademark of a third party.

Deceptive/non-deceptive business model:

The business model is deceptive due to the use of the trademark of a third party in the domain name.

Marketing Channels and Internet Traffic Features:

Search engine optimisation (SEO) to achieve a high search engine ranking, resulting in increased internet traffic (clicks and views).

Customer Incentives:

N/A

« » Back to previous page

CANVAS Nº 3

Online Intellectual Property Rights Infringing Business Model:

Affiliate Marketing Making Unauthorised Trademark Use in the Domain Name

Case study performed by the project team based on the legal decision in WIPO Case D2010-0406

Date of decision: May 5, 2010. Date of analysis: October 1, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A website on the open internet whose domain name making unauthorised use of the trademark of a third party. The website contains automatically generated ads for products sold on other websites. The marketing of these goods may or may not be infringing IPR.

The business model seems deceptive to consumers.

Matrix: Online Digital Platform / IPR Infringing Activity	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open internet/darknet: Open internet platform making unauthorised use of the trademark of a third party in the domain names under the generic top level domain.com and hosted in the USA.

Freely accessible/restricted access: The website is freely available.

Identification of Infringer:

No detailed contact information available on the website. The owner of the website might be identified via the domain name registry WHOIS. However WHOIS information is often incorrect for such websites.

Resilience Against Enforcement Action:

There is no concrete information about the websites resilience against enforcement action, but registrants of affiliate websites often holds a large number of other sites securing continued revenue.

Products and Services:

Ads with links to other websites that may or may not offer goods or services infringing IPR.

Revenue Sources:

Revenue comes from advertisement, pay-per-click (PPC) links.

Involved IPR(s):

Trademark

Customer Relations:

No specific customer relations on the website.

Deceptive/non-deceptive business model:

The business model is deceptive due to the use of the trademark of a third party in the domain name.

Marketing Channels and Internet Traffic Features:

The website uses search engine optimisation through unauthorised trademark use to attract internet traffic.

Customer Incentives:

N/A

« » Back to previous page

CANVAS N° 4

Online Intellectual Property Rights Infringing Business Model:

Marketing of Counterfeited Products While Misusing the Related Trademark in the Domain Name

Case study performed by the project team based on the legal decision in England and Wales UK High Court of Justice [2014] EWHC 3354 (Ch)

Date of decision: October 17, 2014. Date of analysis: March 1, 2016

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A website on the open Internet was selling suspected non-genuine watches of a certain trademark registered highend brand. The website domain name contained the brand name in its entirety and made use of the .com top level domain.

The website had the appearance of a legal and mainstream web shop and made use of both product names and the logo of a manufacturer of high end watches. The website could have appeared authentic to unsuspecting customers.

The website offered a large range of watches at prices around 40-50% of listed retail prices. The website accepted payment with Visa and MasterCard credit cards and through the Western Union money transfer service. The website offered worldwide shipping as well as a returns policy allowing customers to return products.

Deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open internet website using a domain name under the generic top level domain .com containing the trademark of a third party. Website has been hosted in a range of countries including USA, Canada, Germany and Lithuania.

Freely accessible website.

Identification of Infringer:

The website had 'about us' and 'contact us' sections with limited information that likely cannot be used to directly identify infringer. From the domain name registry WHOIS information the domain name is registered in the name of a person residing in Brazil.

WHOIS information, however, is often incorrect for such websites.

Resilience Against Enforcement Action:

There is no information about how the website reacts to enforcement action.

Products and Services:

The website is suspected of selling non-genuine branded watches of a worldwide recognised brand.

The website makes use of the logo and name of a well-known brand as part of the website layout.

Revenue Sources:

Revenue comes from direct sales.

Payment options include Visa and MasterCard credit cards as well as through Western Union.

Involved IPR(s):

Trademark

Possibly design

Possibly copyright

Customer Relations:

The website appears to ship worldwide. Specific delivery time estimates are described on the website. Delivery time estimates are based on customer location. A returns policy is described.

Deceptive/non-deceptive business model

The business model is deceptive due to the use of the trademark of a third party in the domain name.

Marketing Channels and Internet Traffic Features:

The website makes use of a registered trademark as part of the domain name. In combination with the onsite use of numerous original product names it is estimated that the website would appear in search results for watches of the concerned brand.

Customer Incentives:

The website is attractive due to sale of watches bearing a well-known trademark with 50-60% discount.

« » Back to previous page

CANVAS N° 5

Online Intellectual Property Rights Infringing Business Model:

Marketing of Non-Genuine Products on Website Making Use of an Unrelated Trademark in the Domain Name

Case study performed by the project team based on the legal decision in Danish Dispute Board for Domain Names, Case 2015-0093

Date of decision: September 15, 2015. Date of analysis: October 1, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

An online website on the open internet selling suspected

non-genuine branded sunglasses. The website has the appearance of a legal and mainstream web shop and makes use of both product names and the logos of two large worldwide sunglasses brands. The website could appear authentic to unsuspecting customers.

The website domain name, using a country code top level domain (.dk), was previously used (expired) by a Danish company selling shoes inter alia from an Italian shoe brand. The domain name consists of a brand name which is unrelated to the products for sale.

The website offers a large range of sunglasses (lifestyle and sports) at prices around 5-6 % off listed retail prices. The website appears to accept payment with Visa and MasterCard credit cards and offers worldwide shipping.

Deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open internet/darknet: Open internet website using a domain name under the country code top level domain dk containing the text element of a figurative trademark of a third party.

Website is hosted on a server in Panama Freely accessible/restricted access: The website is freely available.

Identification of Infringer:

The website has standard 'about us' and 'contact us' sections with no identification information. The owner of the website might be identified via the domain name registry WHOIS. However WHOIS information is often incorrect for such websites.

Resilience Against Enforcement Action:

There is no information about how the website reacts to enforcement action.

Website is possibly part of systematic and automated domain name acquiring system.

Products and Services:

The website is suspected of selling non-genuine branded sunglasses of two globally recognised brands.

The website makes use of the logos of the two well-known brands as part of the website layout.

Revenue Sources:

Revenue comes from direct sales.

The website displays the Visa and MasterCard logos.

Involved IPR(s):

Trademark
Possibly design
Possibly copyright

Customer Relations:

The website appears to ship worldwide. Specific delivery time estimates are described on the website. Delivery time estimates are based on customer location.

Return and refund functionality is described and available.

Deceptive/non-deceptive business model:

The business model is deceptive due to the use of the trademark of a third party in the domain name.

Marketing Channels and Internet Traffic Features:

The website makes use of an expired domain name of a country specific top level domain (.dk) Through this it inherits a possible Google PageRank and other possible benefits (Newsletter and e-mail marketing).

Customer Incentives:

The website is attractive due to the sale of sunglasses bearing well-known trademarks with prices around 5-6% off the online retail price of original products.

« » Back to previous page

CANVAS Nº 6

Online Intellectual Property Rights Infringing Business Model:
Online Pharmacy Marketing Prescription Medication

Case study performed by the project team based on the Unicri Report: 'Counterfeit medicines sold through the Internet'

Date of analysis: September 29, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

The website sells prescription medicines and other substances targeting primarily bodybuilders but also athletes in a broader sense. Many products appear to be from several international pharmaceutical companies. The website has the appearance and features of a modern web shop. The front page clearly appeals to bodybuilders but also holds descriptions aimed at more regular customers looking for 'health related pharmaceutical items'. The front page also features a live customer support service, customer reviews, links to laboratory tests and featured products. The website front page features a warning for customers in red concerning possible domain name suspension at the registrar level. It states that in such situations the customers will be notified by email with a link to a new domain name indicating that measures are in place to avoid downtime. This illustrates a high resilience level, which is confirmed by several alternative domain names (all with the same online name) that appear to be registered by the website owners. The website supports an active onsite community and rewards returning customers with discounts and a 'bonus cash program'. The website is estimated to have a large user base and receives a lot of attention on related bodybuilding websites, forums, review sites and from social media platforms such as Reddit. Most reviews of the websites are positive. The domain name does not use the trademark of a third party.

Not possible to determine if it is a deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet platform under the generic top level domain .org and hosted in the UK

Freely accessible website.

Identification of Infringer:

No contact information is available on the website. A lower level page called 'terms and conditions' states among other things that the website is run from the Republic of Moldova. Domain name registry WHOIS information and customer discussions likewise point to Moldova as the base for the website. However WHOIS information is often incorrect for such websites. The website itself is hosted in the UK.

Resilience Against Enforcement Action:

Website displays a customer warning in red regarding possible domain name suspension and possible related website down time. Several similar domain names have been registered in what appear to be preparation for potential enforcement actions against the current domain name.

Products and Services:

The website sells a range of prescription medicines such as Human Growth Hormones (HGH) and Insulin from worldwide pharmaceutical brands. Each listed product is described as being genuine with a product picture and price. Website information indicates that products are shipped from both within and outside the EU. It cannot be determined without a testbuy whether the website sells non-genuine products or only engages in illegal parallel trade.

Revenue Sources:

Revenue comes from direct sales.

Payments via bank transfer, Western Union, MoneyGram.

Payments via virtual currencies through Coinstar and Bitcoin (Payments with Bitcoin currently gives a 20% discount).

Involved IPR(s):

Trademark
Design
Possibly Patent

Customer Relations:

Delivery and shipment features are specified on the website. The website uses different regular shipping means (postal services). It offers full refunds if delivery is confiscated

Mainly positive customer reviews displayed onsite and across different review websites.

Deceptive/non-deceptive business model:

It cannot be determined if the website is deceptive as it was not tested whether the products are genuine.

Marketing Channels and Internet Traffic Features:

The website is the center of numerous discussions and reviews coming from a wide range of related websites. Likewise the website offers an affiliate program where users and other websites can use advertising tools to promote the website and through this receive a 10% commission from generated sales.

Customer Incentives:

Bodybuilders and other athletes can purchase steroids and other supplements as well as so-called pharma-grade medicine to enhance their performance. Customers can purchase prescription medicine without having a valid prescription. Discounts offered when using Bitcoins acts as a strong incentive for Bitcoin users to make purchases on the website.

« » Back to previous page

CANVAS Nº 7

Online Intellectual Property Rights Infringing Business Model:

Website Marketing Applied Arts Replica

Case study performed by the project team based on the legal decisions of The Maritime and Commercial Court (Denmark) in cases V-0063-12 + V-0064-12

Date of legal decision: May 20, 2014. Date of analysis: October 1, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Website marketing replica of applied art. The goods are sold and distributed from UK to consumers in continental Europe, as well as the UK.

The business exploits differences in copyright protection, and the marketed goods are thus non–infringing in some countries but infringing in others.

Non-deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet website using a domain name under the generic top level domain .com and hosted on undisclosed servers

Freely accessible website.

Identification of Infringer:

The full contact details of the vendor appears on the website.

The identity of the infringer might be established via the WHOIS register of the domain name registry.

Resilience Against Enforcement Action:

Company does not respond or react to inquiries following foreign court decisions against the enterprise.

Products and Services:

Replica furniture and other applied arts replicas.

Revenue Sources:

Only source of revenue is from direct sales.

Visa and MasterCard and other credit cards accepted.

Involved IPR(s):

Copyright (not protected in country of origin)
Trademark

Customer Relations:

Delivery to most European countries.

Products come with one year warranty.

Goods can be returned up to 7 days after reception.

Customer support offered by e-mail and phone

Deceptive/non-deceptive business model:

The business model is not deceptive towards customers as the marketed products are clearly described as replicas.

Marketing Channels and Internet Traffic Features:

Search Engine Marketing and optimisation.

Enterprises in this industry have used advertising marketing in printed newspapers.

Use of trademarks in the form of product names and descriptions.

Customer Incentives:

The website is attractive to customers, because the replica furniture is sold at considerably lower prices than the prices of the original furniture. The website promotes its Trustpilot rating, which at one point was second highest out of 360 furniture companies.

« » Back to previous page

CANVAS Nº 8

Online Intellectual Property Rights Infringing Business Model:

Marketing Goods or Digital Content on Third Party Online Wholesale Marketplace (B2B)

Case study performed by the project team based on the legal decisions by online marketplaces Indiamart and Alibaba respectively to takedown the listings of the said products

Date of analysis: 2014-2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

The vendor uploads a listing on the wholesale online third party controlled marketplace (B2B) on which they offer the IPR-infringing goods for sale using the trademarks of the genuine manufacturer in the listing, but not in the digital identifier such as the account name.

Deceptive business model

Matrix: IPR Infringing Activity / Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet third party marketplace used to market and sell/buy products

The listings are freely available to users of the marketplace

Products and Services:

Examples of products can be furniture, sporting goods and medicines. Digital services such as software development or modification are also available.

Involved IPR(s):

Trademark

Possibly design

Possibly copyright Possibly patent

Identification of Infringer:

The name and contact details the vendor has provided to the online marketplace are available.

Revenue Sources:

Only revenue source seems to be payments from direct sales.

Payment options depend on both marketplace features as well as vendor specific payment options. Credit cards, PayPal and wire transfer services are mostly used.

Customer Relations:

Delivery and shipment features are specified on the vendor posting. The vendors appears to use regular shipping means such as postal services and small parcel delivery services.

Return/refund options depend on the vendor.

Deceptive/non-deceptive business model:

The business model is deceptive as the products were not listed as non-genuine.

Resilience Against Enforcement Action:

After a notice and takedown the vendor can open another listing or open another account unless the marketplace has made special precautions like banning IP addresses or prohibition measures against certain product listings. Some vendors might offer to replace goods intercepted at customs control.

Marketing Channels and Internet Traffic Features:

The listings on the marketplace can be found by customers through search features on the marketplace and through ordinary search engines.

Customer Incentives:

The listings on wholesale marketplaces are attractive to consumers due to lower prices than online prices for original products. Immediate delivery is also attractive. Marketplaces allow customers to perform vendor reviews, which enable other customers to evaluate those before purchasing goods.

« » Back to previous page

CANVAS Nº 9

Online Intellectual Property Rights Infringing Business Model:
Sale of Non-Genuine Goods through Social Media Networks

Case study performed by the project team based on the UK Intellectual Property Office IP Crime Report 2014/15.

Date of analysis: August 16, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Social media networks are increasingly being used as portals or sales channel for infringing vendors selling a range of suspected counterfeit goods.

These vendors list their products either through specific Facebook profiles or Facebook pages created for that purpose. Vendors often name their profiles and pages with trademark protected names that reflect what products they sell. Likewise vendors will use original marketing material, imagery and product descriptions to elevate their professional appearance. They will often promote limited offers and low prices to attract customers..

Vendors are also known to join Facebook groups intended for private second hand trade. Such groups are often geographically rooted but open for any user to join. In these groups the vendors will list their offers in postings on the group 'wall'.

Vendors generally inform interested customers by communicating through personal/private messages via the Facebook messaging system. This helps them to avoid disclosing contact information publically. It is supposed that customers are serviced either through messages or through a dedicated website the details of which they are given after initial contact with the vendor.

Both deceptive and non-deceptive business model.

Matrix: Online Digital Platform / IPR Infringing Activity		A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1	Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2	Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3	Digital Content Sharing	A3	B3	C3	D3	E3	F3
4	Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5	Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6	Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Vendors use social media websites on the open Internet.

Freely accessible social media websites

Identification of Infringer:

Vendors primarily use pseudonyms when selling through social media networks. Identification of vendors largely depends on cooperation with the social media networks.

Resilience Against Enforcement Action:

Using 'free to use' social media platforms means that when vendors are deleted, they can immediately reconnect and create new profiles or pages with no cost.

Products and Services:

Examples of counterfeit or otherwise infringing goods sold via social media are:
- Prescription medicine
- Clothes
- Handbags

Revenue Sources:

Revenue comes from direct sales.

Involved IPR(s):

Trademarks

Customer Relations

Vendors are immediately available to communicate with customers.

Vendors will communicate directly with customers and guide them through the purchasing process.

Deceptive/non-deceptive business model:

Mostly deceptive business models, but examples of non-deceptive business models are observable if for instance products are openly marketed as copies or replicas.

Marketing Channels and Internet Traffic Features:

By using sales postings on social media networks vendors are able to promote their activities to a large amount of people. Social media networks have built in search features that will present these sales listings when users search for specific brands, product names etc.

Customer Incentives:

Purchasing IPR-infringing goods most often means low prices.

« » Back to previous page

CANVAS N° 10

Online Intellectual Property Rights Infringing Business Model:
Virtual Product Marketing in a Virtual World

Case study performed by the project team based on WIPO Document SCT/24/4, para. 40;

Date of analysis October 1, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Marketing and sale of IPR-infringing virtual items to other users in a virtual world.

Non-deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet virtual world used to market virtual items in virtual shops.

Freely accessible to other participants of the virtual world.

Products and Services:

Virtual consumer goods such as clothing and accessories.

Involved IPR(s):

Trademarks

Design

Possibly copyright

Identification of Infringer:

The infringer will be registered with the virtual world using information provided by the infringer. This information will not normally be available to other users.

Revenue Sources:

Revenue comes from direct virtual sales.

Payment is made in the virtual currency used in the virtual world (e.g. Linden Dollars in secondlife.com, sometimes exchangeable with fiat currencies.

Customer Relations:

Deceptive/non-deceptive business model:

The business model is normally not deceptive for users who are aware that the virtual goods have not been marketed with right holder consent.

Resilience Against Enforcement Action:

N/A

Marketing Channels and Internet Traffic Features:

N/A

Customer Incentives:

N/A

« » Back to previous page

CANVAS
N° 11 A

Online Intellectual Property Rights Infringing Business Model:
Darknet TOR Hidden Service Marketplace with a User Account Shop

Case study performed by the project team without a legal decision.

Date of analysis: August 27, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A TOR darknet marketplace is running a specific account shop where vendors sell user accounts for a wide range of online services and platforms. Accounts for international video and music streaming services, international online marketplaces and airlines are examples of the offers for sale in the shop.

Bank accounts as well as online accounts for payments or wire transfer providers are also sold through the shop. Several of the accounts are described as having valuable 'content' in the form of money deposits (bank accounts) or frequent flyer miles (airline accounts).

The Account Shop makes use of the Darknet Market Escrow feature.

To become a vendor, users must pay a $200 vendor bond (in Bitcoin).

Non-deceptive business model.

Matrix: IPR Infringing Activity / Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Darknet marketplace, TOR hidden service website using the special user domain .onion.

Freely accessible website when access to the TOR network is available.

Identification of Infringer:

The darknet marketplace administrators appear to be from Russia, as this is indicated through the market rules disallowing sale of information/items that may cause harm to Russian people. No direct information on identification of the infringer is available on the market.

Resilience Against Enforcement Action:

Use of the TOR hidden service protocol provides a high level of anonymity and can be considered a resilience action.

Products and Services:

The specific Account Shop facilitates sale of numerous different online accounts for services such as:
- Music streaming
- Movie/TV-series streaming
- Banking
- Airlines
- Gift certificates

Revenue Sources:

Revenue comes from commission and Escrow service/ dispute fees.

A vendor bond of $200 acts as another source of revenue.

All payments are made in Bitcoins.

Involved IPR(s):

Copyright and related rights

Possibly trademark

Customer Relations:

The Darknet market that runs the account Shop offers an escrow service.

The purchase of any account can be disputed within one hour of purchase.

A market forum is provided for user support and general discussions. It has approximately 35.000 members and contains currently 273.000 messages.

Deceptive/non-deceptive business model:

The business model is non-deceptive as the purpose of the shop is clear to both customers and vendors.

Marketing Channels and Internet Traffic Features:

The Darknet Market that runs the Account Shop is currently among the most popular markets. It is widely mentioned and described in related online articles on both the open Internet and Darknet websites.

Customer Incentives:

Users are able to acquire accounts for exploitation without the need to conduct the hacking process that is normally required. Accounts appear to be relatively cheap (i.e. a bank account with a $1000 deposit for $23.99 or airline account with 2500 miles for $8.99). The accounts can be purchased anonymously. Vendors are service minded, active and easy to communicate with. Vendor customer reviews are available.

« » Back to previous page

CANVAS
N° 11 B

Online Intellectual Property Rights Infringing Business Model:
Darknet TOR Hidden Service User Account Shop Vendor

Case study performed by the project team without a legal decision

Date of analysis: March 21, 2016

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A vendor on a TOR Darknet Marketplace running a specific Account Shop offers a wide range of online accounts for sale. The account details are sold either as single accounts or in bundles.

Some accounts are openly listed as hacked, which indicate the means of how the vendor acquired them. Examples of accounts are for banks, airlines, betting websites, sports streaming services, online payment services, web shops with gift certificate services and more.

The vendor has approximately 300 listings and appears to have conducted more than 160 orders since October 2015 until late March 2016 and receives mostly positive feedback by customers.

Non-deceptive business model.

Matrix: IPR Infringing Activity / Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Darknet marketplace, TOR hidden service website using the special user domain .onion.

Freely accessible website when access to the TOR network is available.

Identification of Infringer:

The vendor appears with a user name and can be contacted through a personal message feature through on the Darknet Market platform.

The vendor also lists an ICQ account for possible communication using real time chat.

Most vendors provide their public encryption key for customers to use in connection to e-mail conversations (i.e. during trading or disputes).

Resilience Against Enforcement Action:

Use of the TOR hidden service protocol provides a high level of anonymity and can be considered a resilience action.

Products and Services:

User accounts for a wide range of online services such as banking, payment services, sports streaming, betting and airlines.

Revenue Sources:

Revenue comes from direct sales to customers.

Payment is made in Bitcoins.

Involved IPR(s):

Trademark

Copyright and related rights

Customer Relations:

The Vendor communicates with customers through his Vendor page/ profile on the darknet market account shop.

The Vendor has received mostly positive customer feedback with several comments stating that they offer good customer service.

Deceptive/non-deceptive business model:

The business model is non-deceptive as the purpose of the shop and the products are well described by the vendor.

Marketing Channels and Internet Traffic Features:

The Darknet market that runs the account shop is currently among the most popular markets. It is widely mentioned and described in related online articles on both the open Internet and Darknet websites.

Customer Incentives:

Users are able to acquire accounts for exploitation without the need to conduct the hacking process that is normally required. Accounts appear to be relatively cheap (i.e. a bank account with a $1000 deposit for $23.99 or airline account with 2500 miles for $8.99). The accounts can be purchased anonymously. Vendors are service minded, active and easy to communicate with. Vendor customer reviews are available.

« » Back to previous page

CANVAS Nº 12

Online Intellectual Property Rights Infringing Business Model:
Darknet TOR Hidden Service E-book Library

Case study performed by the project team without a legal decision

Date of analysis: August 13, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A TOR hidden service website is offering approximately 85 000 books in digital format (ebooks) to download for free. The ebooks can also be read on the website and everyone is able to upload new ebooks. The collection of ebooks covers a wide range of genres and the growing collection contain books from both unknown and bestselling writers.

The website does not require membership or other forms of registration for users to be able to use its services. It appears that everyone can download everything and everyone can contribute with new books using an upload feature.

A donation option is possible as the website has an instruction for this along with a Bitcoin wallet key.

The website clearly states disapproval of current copyright legislation and emphasises technology as a way to do away with rules and legislation.

The website and its users inherit the data traffic encryption and anonymization features from the TOR network.

Non-deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Darknet, TOR Hidden Service website using the special use domain .onion.

Freely accessible website when access to the TOR network is available.

Identification of Infringer:

A name and an e-mail address are listed as contact information. These contact details are unlikely to refer to a real identity.

Resilience Against Enforcement Action:

Use of the TOR hidden service protocol provides a high level of anonymity and can be considered a resilience action.

Products and Services:

A large collection of almost 85.000 ebooks available for online reading or download.

Revenue Sources:

Revenue comes from user donations.

Bitcoin donations are accepted.

Involved IPR(s):

Copyright

Customer Relations:

The website 'librarians' validate uploads to make sure they meet a desired level of quality.

Deceptive/non-deceptive business model:

The business model is non-deceptive as the purpose of disregarding the copyright laws is clearly stated on the website.

Marketing Channels and Internet Traffic Features:

Lists of Darknet websites are available on different websites on both the open Internet as well as on Darknet.

This website appears on several lists, but does not appear to be actively promoting itself.

Customer Incentives:

The website offers a large collection of ebooks (almost 85 000) to download or for online reading. Users can download the ebooks anonymously.

« » Back to previous page

CANVAS N° 13

Online Intellectual Property Rights Infringing Business Model:
Darknet TOR Hidden Service Marketing Weapons and Firearms

Case study performed by the project team without a legal decision

Date of analysis: August 14, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A TOR hidden service website selling firearms, ammunition, body armour and other associated products.

The website consists of a web shop with a modern layout, account functionality, checkout features, product categories and more. The website contains multiple explanations and instructions for customers regarding security and anonymity. The website also incorporates ads (torads) in its layout.

The website front page consists of featured and discounted products. In total the website offers products from 28 manufacturers/brands – all from the weapons industry.

The website only accepts payment with cryptocurrencies such as Bitcoin and Litecoin. An escrow service is provided through the website. The website appears to be able to ship the products worldwide. Products appear to be shipped to so-called 're-shippers' located near the customers. To avoid detection rifles and guns will likely be shipped disassembled in separate packages and the re-shipper will assemble the weapon and complete the delivery.

Purchase can be made anonymously as the procedure makes use of cryptocurrency transactions and different means of pick-up or final delivery. An example of this is the use of dead drop delivery where the product is 'dropped' at an agreed location (i.e. a GPS coordinate) to be picked up by the customer.

Non-deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Darknet, TOR Hidden Service website using the special use domain .onion.

Freely accessible website when access to the TOR network is available.

Identification of Infringer:

No contact or general information available on the website to identify the infringer.

Resilience Against Enforcement Action:

Use of the TOR hidden service protocol provides a high level of anonymity and can be considered a resilience action.

Products and Services:

The website sells pistols, revolvers, assault guns and associated items.

Hidden service information indicates that products are shipped from outside the EU. It cannot be determined without a testbuy whether the website sells non-genuine products or only engages in illegal parallel trade.

Revenue Sources:

Main source of revenue is from direct sales, but also revenue comes from advertising.

Payment in virtual currencies, Bitcoin, Litecoin, Anoncoin and possibly others.

Involved IPR(s):

Trademark

Design

Possibly copyright and related rights

Possibly patent

Customer Relations:

Delivery and shipment details are specified on the website.

The website ships to most European countries through reshippers,

pick-ups or dead drop locations. Offers an escrow payment service. Offers refunds if an order is lost or confiscated.

Deceptive/non-deceptive business model:

The business model seems non-deceptive towards customers as the products are well described and illustrated on the website.

Marketing Channels and Internet Traffic Features:

The website is featured on numerous lists of TOR hidden service websites.

Indexing services covering the TOR network such as Grams or Onion.link also feature search results from the website.

Customer Incentives:

Weapon permits are usually required to buy weapons. Permits are not needed to purchase from this hidden service. Assault rifles are not for sale to consumers in the EU. The hidden service offers a convenient and secure way to purchase weapons anonymously.

« » Back to previous page

CANVAS N°14 A

Online Intellectual Property Rights Infringing Business Model: Darknet TOR Hidden Service Marketplace for Goods and Services

Case study performed by the project team without a legal decision

Date of analysis: August 27, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

This Darknet TOR Marketplace is at the time of analysis the largest Darknet Market in terms of number of listings and number of users. It facilitates the sale of various items and services by allowing vendors to list and sell to customers/users of the market. The market is in regards to layout and functionality somewhat equivalent to well-known online market platforms such Amazon, eBay or Alibaba. The market has several listings with what is indicated to be counterfeit products of large international brands.

The market vendors and users inherit the data traffic encryption and anonymization features from the TOR network. The market is built with a high level of customer service, offers an escrow service for Bitcoin payments and has a vendor review system.

Non-deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Darknet marketplace, TOR hidden service website using the special user domain .onion.

Freely accessible website when access to the TOR network is available.

Identification of Infringer:

Profile names of administrators, moderators and vendors are visible, but do not make identification possible. No other contact or general information available on the website to identify either the owner of the marketplace or the individual vendors.

Resilience Against Enforcement Action:

Use of the TOR hidden service protocol provides a high level of anonymity and can be considered a resilience action. There is no information about the hidden marketplace's resilience to enforcement action, but should the marketplace be closed down it would probably be quite easy to open a new similar marketplace.

Products and Services:

The market offers a platform for vendors to sell their items/services.
Examples of vendor listings:
- Counterfeit jewelry and watches
- Prescription medicine
- Digital services
- Online accounts to access copyright material (music, video streaming)

Revenue Sources:

The marketplace takes a 4% commission on sales. Vendors have to pay a bond of 1.5 Bitcoin to the marketplace when registering.

Payment is in Bitcoin with an escrow service available.

Involved IPR(s):

Trademark

Copyright

Design

Customer Relations:

The market moderators can act as mediators in vendor/customer disputes. Customer relations are primarily maintained by the vendors. The market platform provides general customer services, a transaction platform, product/vendor reviews and user forums.

Deceptive/non-deceptive business model:

The business model is non-deceptive as the purpose of the market is clear to both customers and vendors.

Marketing Channels and Internet Traffic Features:

Lists of Darknet Markets are available on different websites on both the open Internet as well as on Darknet. Discussions on social media networks such as Reddit also act as a resource in terms of marketing.

Customer Incentives:

The hidden marketplace is highly attractive to vendors and buyers with the intention of selling and buying IPR-infringing products due to the high level of anonymity. Many of the listings on the marketplace are for products not readily available. Venders are usually service-minded, responsive and easy to get in contact with. In addition, the hidden marketplace provides Bitcoin escrow payments and a dispute mitigation system providing a high level of vendor as well as buyer protection.

« » Back to previous page

CANVAS N°14 B

Online Intellectual Property Rights Infringing Business Model:

Vendor on Darknet TOR Hidden Service Marketplaces Marketing Storage Media Preloaded with Digital Content

Case study performed by the project team without a legal decision

Date of analysis: August 27, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A vendor on several darknet TOR marketplaces on the TOR network offers storage media hardware (hard drives and memory cards) pre-loaded with a high number of music albums, films and TV-series for sale. This content comes at no additional cost as the total price for the hardware items is very close to the retail price.

As a vendor on darknet markets they are able to conduct their business with a high level of anonymity and like most similar vendors offer a high level of customer support in connection with their service. Customers actively review the vendor with mainly positive comments and descriptions.

Non-deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Advertising for or Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Darknet marketplace, TOR hidden service website using the special user domain .onion.

Freely accessible website when access to the TOR network is available.

Identification of Infringer:

The username of the vendor appears on the Darknet Markets, but does is not identify the vendor.

Resilience Against Enforcement Action:

Use of the TOR hidden service protocol provides a high level of anonymity and can be considered a resilience action.

Products and Services:

A vendor sells storage media (hard drives and memory cards) with preloaded copyright protected content.

Example: Hard drive 4 TB (preloaded with 2000+ music albums, 1600+ films, 100+ TV series) price €273.

Revenue Sources:

Revenue comes from direct sales.
Payment is in Bitcoin with escrow service available.

Involved IPR(s):

Copyright and related rights
Trademark

Customer Relations:

Delivery and shipment features are specified on the vendor page. The vendor appears to use regular shipping means (postal services).

Worldwide delivery.

Offers refunds and enhanced security features in the form of optional disk encryption before shipping. Excellent customer reviews.

Deceptive/non-deceptive business model:

The business model is non-deceptive as the products are clearly described by the vendor.

Marketing Channels and Internet Traffic Features:

The vendor has listings on at least three TOR Darknet marketplaces.

Customer Incentives:

Items could appeal to customers interested in either hard drives or copyrighted content. In either case the extra content or hardware could be seen as a benefit or bonus. In addition, the hidden marketplace provides high levels of customer anonymity and secure Bitcoin escrow payments.

« » Back to previous page

CANVAS N° 15

Online Intellectual Property Rights Infringing Business Model:

Darknet TOR Hidden Service Marketplace For Protected or Sensitive Information

Case study performed by the project team without a legal decision

Date of analysis: October 29, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

Two similar services on the TOR network are currently being developed to form new darknet marketplaces or auctions. These services aim to facilitate the trading of a wide range of protected or sensitive information and whilst doing so provide the highest level of anonymity and security for both the vendor and the buyer.

They will make use of encryption and blockchain technology to assure secure and error-free transactions where information can only be sold once.

The services will theoretically provide potential whistleblowers, employees seeking to hurt an employer or company, cyber criminals and other individuals seeking economic profit new opportunities.

Simultaneously the services will in theory provide nations seeking information regarding the security or politics of other nations or states, individuals with the ability to exploit certain information and enterprises/companies seeking information about certain industries or competitors new opportunities for purchasing such information.

Both services have provided long lists of potential information to be sold through the markets, including designs, trade secrets, complete databases and source codes for high-end proprietary software.

Neither of these services is running at the time of analysis. One has made the current developed code publically available (open source). The other service is being developed behind closed doors.

Non-deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Darknet, TOR hidden service website using the special user domain .onion. and open internet promotion website. Website under ccTLD .io hosted on a server in the US.

Freely accessible website when access to the TOR network is available.

Identification of Infringer:

No contact or general information available on the website for identification of either owner of the marketplace or the individual vendors. Some of the software will intentionally be open source and developer identities might be disclosed.

Resilience Against Enforcement Action:

Use of the TOR hidden service protocol, as is the aim of the services, provides a high level of anonymity and can be considered a resilience action. Should the marketplaces be closed down it would probably be quite easy to open new similar marketplaces.

Products and Services:

These services will facilitate unrestricted sale of all kinds of information, including including designs, trade secrets, complete databases and source codes for high-end proprietary software.

Revenue Sources:

Revenue for owner is not identified, but could be advertising, commission and dispute mitigation fee. For vendors the revenue will come from direct sale.

Payments are done in Bitcoin where escrow payment is provided

Involved IPR(s):

Copyright

Database right

Design

Customer Relations:

The services will provide means for dispute mitigation.

All activities and transactions will be encrypted and as such will offer anonymity for both sellers and buyers.

Deceptive/non-deceptive business model:

The business model seems non-deceptive for vendors as well as buyers as the purpose of the marketplace is clearly described on the related websites.

Marketing Channels and Internet Traffic Features:

Dedicated open Internet, freely accessible website promotes one of the services. Vendors will most probably get information about the hidden services through online articles on the open Internet.

Customer Incentives:

The hidden marketplaces are highly attractive to vendors and buyers with the intention of selling and buying protected information due to the high level of anonymity. In addition, the hidden marketplaces provide Bitcoin escrow payments and a dispute mitigation system providing a high level of vendor and buyer protection.

« » Back to previous page

CANVAS Nº 16

Online Intellectual Property Rights Infringing Business Model:
Spoofing Website Making Unauthorised Use of a Trademark

Case study performed by the project team based on legal decision in WIPO Case D2010-0966

Date of legal decision: August 11, 2010. Date of analysis: October 1, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

The operator registers a domain name and creates a website that is similar to that of a legitimate business or organisation, most often a financial institution such as a bank or insurance company, but it may also be a public authority or private enterprise (e.g. hotel chain). The website is set up for the purpose of obtaining the visitors credit card or social security number, user ID, passwords, trade secrets or the like. Access to the websites are usually 'promoted' via use of phishing e-mails.

Deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Use of e-mails that use the trademark of a third party in the domain name. The domain name is registered under the generic top level domain .com and websites were hosted on servers in the UK and US.

Freely accessible website.

Identification of Infringer:

The website contains false information about the owner of the website. The identity of the infringer might be established via the WHOIS register of the domain name registry. However WHOIS information is often incorrect for such websites.

Resilience Against Enforcement Action:

There is no concrete information about the websites resilience against enforcement action, but it will be quite easy to create new spoofing websites when enforcement action is taken.

Products and Services:

The e-mails claim to offer legitimate financial services. They are however not connected to any such service.

Revenue Sources:

Revenue comes from direct fraudulent use or re- sale of access codes to bank accounts. Possible sales in illegal (possibly darknet) marketplaces.

Involved IPR(s):

Trademark

Customer Relations:

The relationship with the consumer is built on the deceptive use of a third party trademark.

Deceptive/non-deceptive business model:

Highly deceptive business model as it clearly has the aim of defrauding unwary clients of legitimate companies.

Marketing Channels and Internet Traffic Features:

The business model relies on dissemination of phishing e-mails, using the domain name, to generate website activity needed to finalise the criminal activity.

Customer Incentives

The website is attractive to consumers, because it appears to be the legitimate company normally used by the consumer.

« » Back to previous page

CANVAS Nº 17

Online Intellectual Property Rights Infringing Business Model:
Phishing E-mails Making Unauthorised Use of a Trademark

Case study performed by the project team based on legal decision in WIPO Case D2015-0442

Date of legal decision: April 4, 2015. Date of analysis: October 1, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

The sender of an email passes themself off as a company or public authority and uses a domain name that is very similar to the genuine company or authority in the e-mail address.

In the mail the receiver may for example be invited to update their account details via an embedded link to a website that is falsely presented as the website of the company.

The receiver may also be asked to 'review' an account statement attached as a file to the email – a file which may contain malware.

Access codes to bank accounts can be used directly to gain access to the content of bankaccounts or can be resold on illegal (possibly Darknet) marketplaces.

Deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	**E1**	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	**E5**	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Use of e-mails that use the trademark of a third party in the domain name. The domain name is registered under the generic top level domain .com and websites are hosted on servers in the US.

Products and Services:

The e-mails claim to offer legitimate financial services. They are however not connected to any such service.

Involved IPR(s):

Trademark

Identification of Infringer:

The true sender of the mail cannot immediately be identified by the recipient. The identity of the sender might be established via the domain name registry WHOIS information register. However WHOIS information is often incorrect for such websites.

Revenue Sources:

Revenue comes from direct fraudulent use or re-sale of access codes to bank accounts. Possible sale on illegal (possibly Darknet) marketplaces.

Customer Relations:

The relationship with the consumer is built on the deceptive use of a third party trademark.

Deceptive/non-deceptive business model:

Highly deceptive business model as it clearly has the aim of defrauding unwary clients of legitimate companies.

Resilience Against Enforcement Action:

N/A.

Marketing Channels and Internet Traffic Features:

The business model relies on use of e-mails with the domain names in question. These e-mails focus on generating traffic on fraudulent financial websites.

Customer Incentives:

The e-mails encourage consumers to respond as they appear to originate from a legitimate company normally used by the consumer.

« » Back to previous page

CANVAS Nº 18

Online Intellectual Property Rights Infringing Business Model:

Android Smartphone Application Making Unauthorised Use of a Trademark, Providing Access to Pornographic Content and Disseminating Malware

Case study performed by the project team without a legal decision

Date of analysis: September 25, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

An android smartphone application (app) which offers to facilitate access to pornographic videos was recently released. The app, however, is malware, categorised as 'Ransomware'.

When the app is executed (launched), it stealthily captures a picture of the user with the built in camera, and locks the user out from accessing the android operating system and subsequently from using the smartphone.

The smartphone owner then receives an accusatory message, with in most cases is an embedded picture of the user and the name and logo of the FBI and a major international IT-security company in the message, aimed at instilling fear and giving credibility to the accusatory message.

The purpose of the message is to force the smartphone owner to pay a 'settlement' amounting to $500 USD after which the smartphone will become unlocked.

The app never resided on the official Google Play store but was available for download via unofficial 'app store' (website).

Deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Application for Android smartphones downloaded from unofficial 'app store' (website) on the open Internet.

The application is freely available.

Products and Services:

The smartphone application offers to facilitate via an app easy access to pornographic content.

Involved IPR(s):

Trademark
Possibly copyright and related rights

Identification of Infringer:

No contact or otherwise infringer identification data was available in the malware or in relation to the used or mentioned websites.

Revenue Sources:

Revenue comes from extortion of victims. Ransom payment is via PayPal.

Customer Relations:

The relationship with the customer is built on attracted them to pornographic content with the aim of deceiving them. In addition the application claims a connection to a IT-security company.

Deceptive/non-deceptive business model:

A highly deceptive business model exploiting trust in a IT-Security Company.

Resilience Against Enforcement Action:

N/A.

Marketing Channels and Internet Traffic Features:

It is not clear how customers are directed to the application, but it is most likely from websites with pornographic content.

Customer Incentives:

The smartphone application offers to facilitate via an app easy access to pornographic content. The application makes a connection to a IT-Security Company making the use of the application seem safe for consumers.

« » Back to previous page

CANVAS N° 19

Online Intellectual Property Rights Infringing Business Model:

Malware Dissemination from Website Making Unauthorised Use of Trademark

Case study performed by the project team based on legal decision in WIPO Case D2015-1628

Date of legal decision: November 10, 2015. Date of analysis October 1, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A website using a registered trademark in the domain name was found to be infecting visitors with malware.

The website generated traffic through an e-mail phishing or spear phishing campaign.

Website visitors would automatically be infected with malware through exploitation of a Java vulnerability if they were running an unpatched system.

The potentially infected and unaware visitors would then automatically be redirected to the official website of the trademark owner and by such the malicious activity would likely not be discovered.

Deceptive business model.

Matrix: Online Digital Platform / IPR Infringing Activity	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet website with domain name under the generic top level domain .org and hosted on undisclosed servers

Freely accessible website

Identification of Infringer:

No information available

Resilience Against Enforcement Action:

N/A.

Products and Services:

N/A

Revenue Sources:

Revenue comes from malware dissemination and related usage of stolen information or other malicious actions.

Involved IPR(s):

Trademark

Customer Relations

Deceptive/non-deceptive business model:

A highly deceptive business model as the installation of malware took place with only a small possibility of the victims noticing it.

Marketing Channels and Internet Traffic Features:

Use of phishing and spear phishing e-mails to generate traffic.

Customer Incentives:

The nature of phishing and spear phishing e-mails is to tempt or trick victims into clicking on links. Victims with genuine interest in the website of the trademark owner would likely be 'easy prey'.

« » Back to previous page

CANVAS Nº 20

Online Intellectual Property Rights Infringing Business Model:

Fraudulent use of the Trademark of a Trademark Registration Office

Case study performed by the project team based on legal decision in England and Wales High Court of Justice [2015] EWHC 3256 (IPEC)

Date of legal decision: September 29, 2015. Date of analysis: September 29, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A company sent letters to proprietors of patents and trademarks and reminded them about the imminent renewal of their rights. The operator successfully claimed renewal fees at up to five times the official fee.

The letter was designed to appear as if the reminder had been sent by an official national trademark registration office and because of this numerous proprietors paid the elevated fee.

Deceptive business model.

Matrix: IPR Infringing Activity / Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet/Darknet: Open Internet website with domain name under the generic top level domain .org and hosted on servers in Sweden

Freely accessible/restricted access: Freely accessible website

Identification of Infringer:

Infringer was identified but the details of how is not publically available.

Resilience Against Enforcement Action:

N/A.

Products and Services:

Patent or trademark renewal service.

Revenue Sources:

Revenue comes from renewal fees paid by right proprietors.

Payment information unavailable.

Involved IPR(s):

Trademark

Customer Relations:

The infringer communicated with right holders (potential customers) via e-mail containing a rights renewal reminder and form.

Deceptive/non-deceptive business model:

A highly deceptive business model as the victims in some cases actually needed to renew their rights.

Marketing Channels and Internet Traffic Features:

Infringer was marketing their service by directly approaching potential customers.

Customer Incentives:

Sending an unsolicited reminder to customers who potentially need to renew their rights represents a high level of service.

« » Back to previous page

CANVAS Nº 21

Online Intellectual Property Rights Infringing Business Model:
Website with links to digital content

Case study performed by the project team based on legal decision in Criminal Court of Appeal (Castellon, Spain), Resolution No.: 426/2014

Date of legal decision: November 12, 2014. Date of analysis March 15, 2016

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A website on the open Internet was facilitating access to copyright protected movies, music, tv-series, computer games and more through links.

The users of the website could browse or search through the website to find links that would allow them access to the mentioned digital content. The links would lead to different filesharing networks through which the content could be downloaded.

The website link sections appeared to be maintained thoroughly and each link verified.

It has not been analysed whether the shared content or the advertising on the website has malware. Therefore It cannot be determined whether the business model is deceptive or not.

Matrix: Online Digital Platform / IPR Infringing Activity	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet website using a domain name under the generic top level domain .com and hosted on a server in the US.

Freely accessible website.

Identification of Infringer:

The identity of the infringer might be established via the WHOIS register of the domain name registry.

Resilience Against Enforcement Action:

N/A.

Products and Services:

Links to copyright protected movies, music, tv-series and computer games.

Revenue Sources:

Revenue comes from advertising and affiliate marketing.

Sale of user information appears to have been another source of revenue.

Involved IPR(s):

Copyright and related rights

Customer Relations:

The website maintained an up-to-date catalogue of links to copyright protected content.

It was possible to contact the webmaster and the website offered a user chat and a section for 'collaboration'.

Deceptive/non-deceptive business model:

The business model is likely to be non-deceptive as the content and means of acquisition was clearly described in connection with the links. Ifthe business model used malware against the website users the business model would be deceptive.

Marketing Channels and Internet Traffic Features:

The website was part of a network of websites. They each promoted and linked to each other.

Customer Incentives:

Free access to copyright protected movies, music, tv-series and computer games.

« » Back to previous page

CANVAS Nº 22

Online Intellectual Property Rights Infringing Business Model:
Website Contributing to Video Streaming

Case study performed by the project team based on legal decision from Municipal Court of Copenhagen, Case SS90-15834/2015

Date of legal decision: June 24, 2015. Date of analysis: September 21, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A website with exclusive focus on online video streaming services, predominantly Popcorn Time, was posting and updating news articles, a Popcorn Time FAQ and troubleshooting section and a set of guides. The website itself was not directly affiliated with the Popcorn Time project and as such did not directly infringe copyrights.

The guides posted on the website mainly contained information such as how to install the Popcorn Time client/player on different platforms (i.e. Window, Mac OS, Linux, iOS and Android). Certain guides gave instructions to users on how to use the Popcorn Time client anonymously by use of VPN services.

The website also featured a download section that links to a range of different Popcorn Time clients.

The website content was predominantly positive, if not enthusiastic, towards the Popcorn Time service. Despite this the website did also post a warning on its front page regarding the fact that Popcorn Time users will have access to copyright protected content. The warning states that the usage of Popcorn Time is at the users own risk.

The website ran ads on its pages – usually one ad per page. The website was using the name Popcorn Time and a country code top level domain as its domain name.

A social media page using the same name as the website's domain name is still active at the time of analysis. The page is actively posting similar content and engaging visitors and reacting to comments. No direct connection between the website and the social media page was confirmed during this study, but is considered to be likely.

Non-deceptive business model

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet website under ccTLD .dk and hosted at an undisclosed location. User profile on Facebook.

Freely accessible website.

Identification of Infringer:

The infringer could be identified through domain name registry WHOIS information.

Resilience Against Enforcement Action:

Use of a social media platform allows the operator to continue to provide similar information as on the dedicated website following a domain name suspension or blocking order.

Products and Services:

The website focus was online video streaming, mainly Popcorn Time. The website content was organised into the following sections: Popcorn Time, News, Versions, Guides, Gadgets, FAQ, Troubleshooting.

The website also provided more general articles such as guides and links to bittorrent clients and VPN services.

Revenue Sources:

The source of revenue was advertising.

Involved IPR(s):

Copyright and related rights

Customer Relations:

The website informed consumers that the use of Popcorn Time client was at their own risk.

Deceptive/non-deceptive business model:

Non-deceptive business model as users are informed that use of Popcorn Time client can infringe copyright.

Marketing Channels and Internet Traffic Features:

An identically named Facebook profile was posting links to the website.

Customer Incentives:

Website visitors were able to read updated and assembled news on Popcorn Time. Users or potential users could use the guides to enhance their use of the Popcorn Time service.

« » Back to previous page

CANVAS Nº 23

Online Intellectual Property Rights Infringing Business Model: Torrent Website

Case study performed by the project team based on legal decision in England and Wales High Court of Justice, Chancery Division: [2013] EWHC 379 (Ch)

Date of legal decision: February 28, 2013. Date of analysis: September 17, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

The largest online 'torrent website' facilitates download of copyright protected content by hosting 'torrent files' and 'magnet links' that enables it's users to participate in peer-to-peer file sharing through the BitTorrent protocol. The site itself does not host the content and claim to have a working procedure for content removal regulation through which copyright holders can interact.

The majority of the website content is related to movies, TV-series, music and computer software. The content in form of 'torrent files' and 'magnet links' are supplied by the users. The website makes use of primarily banner ads for revenue generation. Another revenue source example of affiliate marketing was also observed regarding a recommended vendor of VPN services (to enable anonymous and secure use while file sharing).

The website utilises several different internet domain names to gain resilience against take-down actions and blocking orders. The domain names use different top level domains.

The website contains a very active user community that is indicated on the website to exceed 375 000 active users. The total number of actual users (registered and non-registered) could easily exceed this number.

The website appears to actively use social medial accounts to promote new files and attract users.

It has not been analysed whether the shared content or the advertising on the website is carrying malware. So it is unclear whether the business model is deceptive or not.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet website using different but related domain names under different top level domains. Website is hosted on servers in Canada and possibly other countries.

Use of social media.

Freely accessible website.

Identification of Infringer:

The current main website is registered in the name of what appears to be a physical person residing in Costa Rica.

Resilience Against Enforcement Action:

The website utilises several different domain names to gain resilience against take-down actions and blocking orders. Use of social media allows the website to continue communication with users in the case of take-downs or blocking actions.

Products and Services:

The website hosts 'torrent files' which can be downloaded and used to download digital files from other users of the BitTorrent protocol.

The 'magnet links' on the website has the same overall functionality for the user, but in these instances the website does not host the torrent files.

Revenue Sources:

Revenue sources are advertising and affiliate marketing of VPN services.

Involved IPR(s):

Copyright and related rights

Customer Relations:

Website provides an extensive FAQ for users.

Website has an active community and user forum.

Deceptive/non-deceptive business model:

The business model is likely non-deceptive as the content and means of acquisition is well known by its users. If the business model incorporated malware dissemination against the website users the business model would be deceptive.

Marketing Channels and Internet Traffic Features:

The website has been well established since 2008 and has a high ranking in generic search engine results. The website utilises social media networks to promote itself and engage its users.

Customer Incentives:

The website is user friendly and has a very active community/user base that very often contributes the newest content in many different formats. For each file the user is able to see other user reviews and consequently the best quality material becomes the most popular.

CANVAS N° 24

Online Intellectual Property Rights Infringing Business Model: File Sharing Cyberlocker

Case study performed by the project team based on legal decision in United States District Court, Southern District of Florida, Miami Division, Case No. 11-20427-CIV-JORDAN

Date of legal decision: July 8, 2011. Date of analysis: November 6, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A website on the open internet facilitates easy sharing of video and other forms of digital content. In addition to facilitating easy sharing, the website also incentivises uploaders (affiliates) in the form of a fixed amount of revenue per X amount of visitors they attract. The level of payment appears to be dependent on the uploader's geographical location.

The visitors are likewise incentivised to download large files by offering high speed downloads.

For the website the primary means of revenue generation is ad based. Revenue is also generated from users who sign up for paid premium accounts.

Each visitor is exposed to at least four ads per visit.

The website and its content uploaders generate traffic by advertising on relevant websites, forums and thereby also through search engines.

It has not been analysed whether the shared content or the advertising on the website is carrying malware. So it is unclear whether the business model is deceptive or not.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet website with domain name under the generic top level domain .net and hosted on servers in an undisclosed country.

Freely accessible website

Identification of Infringer:

WHOIS registrant data is unclear. However clear evidence points towards two Egyptian (partners) owners.

No contact information is visible on the website.

Resilience Against Enforcement Action:

Website uses a service to obfuscates hosting details

Products and Services:

The file sharing service facilitates easy sharing of various forms of digital content. Anything from software (incl. sought-after games etc.) to videos of any nature, except illegal pornographic material.

The website offers visitor's the ability to stream video files instead of downloading the file in a traditional sense.

Revenue Sources:

Revenue comes from advertising and direct sales of website premium accounts. revenue

Sales revenue (premium accounts)

Payments are received through PayPal and WebMoney.

Involved IPR(s):

Copyright

Customer Relations:

The website has detailed descriptions of features and affiliate rules.

The website has a more general FAQ.

Users are protected against content with illegal sexual abuse of children as such content is not allowed on the service and removed if detected.

Deceptive/non-deceptive business model:

The business model is likely non-deceptive as the content and means of acquisition is well known by its users. If the business model incorporated malware dissemination against the website users the business model would be deceptive.

Marketing Channels and Internet Traffic Features:

Applicable forums and websites where copyright infringing activities are discussed, such as Reddit.

Customer Incentives:

Customers can be divided into two types, the uploader and the visitor.

The uploader generates revenue for uploading digital content, which in most cases consists of copyright media (games & videos).

The visitor is incentivised by free high-speed downloading of files.

« » Back to previous page

CANVAS Nº 25

Online Intellectual Property Rights Infringing Business Model: Television Streaming

Case study performed by the project team based on legal decision in Danish Municipal Court of Aalborg 12-1319/2015

Date of legal decision: April 22, 2015. Date of analysis: November 1, 2015

Based on the 'Business Model Canvas' by Strategyzer.com

Business Model Summary:

A website offers streaming access to 300+ live TV-channels for €35/month. The wide selection of channels contains several Danish, Swedish and Norwegian channels as well as many channels from the UK and USA. The service can be used on PC's, smartphone and tablets and for TVs.

The website has a modern layout and appears to have a user friendly and simple sign-up process. To become customers, users must sign up with their name and address. Credit cards are required for payment, which after sign-up becomes an automatic process with withdrawal every month.

The website has a live support chat function. Upon request the staff will provide potential customers with a free demo account to test the service.

The website makes use of social media. Particularly it maintains an active Facebook profile/page that currently has 172 Likes. Based on the activity of users it appears the website popularity is rising as the posts are receiving increased amount of likes and comments.

Non-Deceptive business model.

Matrix: IPR Infringing Activity \ Online Digital Platform	A Internet Site Controlled by Infringer	B Third Party Marketplace	C Social Media or Blog	D Gaming or Virtual World	E E-mail, Chatroom or Newsgroup	F Mobile Devices
1 Domain Name or Digital Identifier Misuse of IPR	A1	B1	C1	D1	E1	F1
2 Physical or Virtual Product Marketing	A2	B2	C2	D2	E2	F2
3 Digital Content Sharing	A3	B3	C3	D3	E3	F3
4 Account Access or Codes to Digital Content Sharing	A4	B4	C4	D4	E4	F4
5 Phishing, Malware Dissemination or Fraud	A5	B5	C5	D5	E5	F5
6 Contributing to Infringement	A6	B6	C6	D6	E6	F6

Digital Platform:

Open Internet website with domain name under the generic top level domain .com and hosted on servers in Latvia.

Freely accessible website.

Identification of Infringer:

Founder of the website can be identified through publically available information on social media.

A company name and address in Gibraltar is the only available contact information on the website.

Resilience Against Enforcement Action:

N/A

Products and Services:

The website sells streaming access to more than 300 live TV-channels.

Customers can stream the channels on multiple devices, including smartphones and tablets.

Revenue Sources:

Revenue comes from direct sales.

Payments are made with Credit Cards.

Involved IPR(s):

Copyright

Customer Relations:

The service has no binding period.

The website does not describe any usage restrictions or limitations. Based on this it appears the service is available worldwide.

The website has a live and functioning customer support chat function.

The website offers a free demo profile to potential customers.

Deceptive/non-deceptive business model:

Non-deceptive business model as users are well informed of the website services.

Marketing Channels and Internet Traffic Features:

The website primarily makes use of a Facebook Page to promote the service. The Facebook page is regularly updated with posts about upcoming sport events and other news about the service.

Customer Incentives:

With a price of €35/month for more than 300 TV-channels the service appears to be below 50% of the retail price for known television packages.

Being able to stream live TV-channels on smartphones, tablets might be an advanced feature compared to legal commercial TV-providers.

« » Back to previous page

For more information, please, visit www.deloitte.es

Designed and produced by the Communications, Brand and Business Development department, Madrid.