D9.3

Market analysis

v 1.0 2014-11-14

Apostolos Kousaridas (VELTI), Timotheos Kastrinogiannis (VELTI), Symeon Papadopoulos (CERTH), Adrian Popescu (CEA), Tom Seymoens (iMinds), Marita Holst (LTU), Mireille Hildebrandt (iCIS), George Mourikas (HWC)

This document contains a thorough market analysis on personal data management, presenting the main technology players and providing an overview of the market landscape. An analysis of the envisaged key USEMP outputs is given and the academic or industrial exploitation plans of each USEMP partner are briefly presented, based on the profile of each organization. This deliverable constitutes the basis for subsequent deliverables, where the exploitable foreground to arise from the project will be specified and the detailed plans for exploitation by all the partners will be described.

Project acronym	USEMP
Full title	User Empowerment for Enhanced Online Presence Management
Grant agreement number	611596
Funding scheme	Specific Targeted Research Project (STREP)
Work program topic	Objective ICT-2013.1.7 Future Internet Research Experimentation
Project start date	2013-10-01
Project Duration	36 months

Workpackage	WP9
Deliverable lead org.	VELTI
Deliverable type	Report
Authors	Apostolos Kousaridas (VELTI), Timotheos Kastrinogiannis (VELTI), Symeon Papadopoulos (CERTH), Adrian Popescu (CEA), Tom Seymoens (iMinds), Marita Holst (LTU), Mireille Hildebrandt (iCIS), George Mourikas (HWC).
Reviewers	Tom Seymoens (iMinds), Hervé Le Borgne (CEA)
Version	1.0
Status	Final
Dissemination level	PU: Public
Due date	2014-09-30
Delivery date	2014-11-14

Table of Contents

1.Introduction

In the last few years, the growth of connected devices has exploded, while more and more people are connecting to the Internet and for longer amounts of time. The audience for social networking is also constantly increasing worldwide. Almost two-thirds of overall social media users say they use social media sites at least once a day via their computer, and almost half of smartphone owners visit social networks every day. To this end, in a culture of connectivity there is a growing need for the protection of privacy of individuals online, taking into consideration that in many cases personal data are directly provided by online users or deduced by online web sites.

The USEMP platform aims at providing tools that empower online users to control their data and to understand how they are used by third parties. The proposed approach starts with the study of personal information sharing practices, coupled with a study of the complex legal framework related to this information. It proceeds with the proposal of innovative multimedia information extraction algorithms that infer new knowledge from user data and leverages insights from social and computer science developments to empower the users. As a second goal, USEMP is set to contribute to current debates concerning the way personal data are handled by OSNs and regarding the economic value of personal information and the way it is monetised. To attain its goals, USEMP proposes a multidisciplinary approach that relies on four core domains: (a) empirical user research that combines lab and living lab studies, (b) legal studies that deal with the complex legal framework related to personal data, (c) multimedia information extraction adapted to user empowerment in OSNs, and (d) tools for semiautomatic user assistance in personal data sharing management.

This document contains a thorough market analysis on the personal data management. It constitutes the basis for subsequent exploitation deliverables, where the exploitable foreground to arise from the project will be specified and the plans for exploitation by all the partners will be described in analysed, while specific business models from project assets will be investigated. Specifically, Section 2 gives an overview of the market landscape and elaborates on the main technology players (Privacy aware OSNs, Privacy feedback & awareness, Multimedia Information Extraction, Monetisation of crowd sourced content, Advertisement Filtering and Online advertising). Section 3 provides an analysis of the key USEMP outputs, while Section 4 highlights the academic or industrial exploitation plans of each USEMP partner, based on its profile.

Finally, Section 5 concludes and summarises the most important issues of the Deliverable.

2.Market Overview

There are many types of Online Social Networks (OSN) for business (e.g. Doostang, LinkedIn) and for private purposes (e.g. Facebook, QZone, Google+, MySpace or StudiVZ), where the user-base and purpose of use is very clear[1]. The common denominator for all OSNs is to allow their users to volunteer/share data. For example posting / articulating / linking to opinions, posting / linking to images, creating / joining communities, reveal / accept / maintain / adjust relationships between people and communities etc. All this information is valuable resource to an OSN. The OSN providers use the personal data collected in order to monetise and extract value from users e.g., for more efficiently targeted marketing-campaign[2] or in any case exploit the personal data with purposes that can be undesirable (see interesting experience by TIMES reporter[3]).

The public internet use over the last 5 years (2010- Nov 2014) has increased by approximately one billion users (from ~2 billion to ~3 billion) and the world population increased only by only ~0.3 billion (in the last 5 years from ~6.9 to ~7.2 billion) this reveals that almost 40% of the world population has internet access[4]. From these ~3 billion internet users there are approximately 3.5 billion active social network account (in November 2014 according to Figure 1), this means that multiple subscriptions to OSN accounts are utilised per user. Based on the last population growth percentage (1.14% from 7.162 billion), the associated growth of people with Internet access (7.9% from 2.712 billion) and the current active OSN accounts (sum = 3.54 billion) we can forecast the increase of OSN active accounts in 2017 by approximately 4.45 billion (an increase of 0.91 billion). That means that the personal data information exposed is going to follow the increasing trend with the potential for the social networks to invest more in research and ways to develop new revenue-streams based on the accumulated OSN user-based personal data.

The 4.45 billion OSN-user worldwide forecast by 2017 increases the value of the personal data provided over time to consistent OSN increases at an equivalent rate. To put it in perspective at the moment (June 2014) the average value per user to an OSN is $101.10 (according to top 4 social media sites[5]) this creates a market space of 3.54 billion ‘active OSN users’ * $101.10 = $358 billion market for the OSN this means that accumulating and keeping more users is in their interest. With some simple calculation based on the data above and keeping the ‘average value per user to the OSN’ constant and utilising the forecast trends of the market for the OSN by 2017 could increase by $100 billion.

[1] Von Martin Gneiser, Julia Heidemann, Mathias Klier, Christian Weiß, title *“Valuation of Online Social Networks – An Economic model and its application using the case of XING.com”* http://core.kmi.open.ac.uk/download/pdf/11553958.pdf

[2] Industrial report by Michael A. Stelzner, Title *“2014 SOCIAL MEDIA MARKETING INDUSTRY REPORT. How Marketers Are Using Social Media to Grow Their Businesses”,* May 2014, Author link http://www.socialmediaexaminer.com/SocialMediaMarketingIndustryReport2014.pdf

[3] TIME magazine article *‘Data Mining: How Companies Now Know Everything About You’* By Joel Stein, 10/3/2011 (Link http://content.time.com/time/magazine/article/0,9171,2058205,00.html)

[4] This website includes the internet live stats cited by the World Wide Web consortium W3C http://www.internetlivestats.com/internet-users/

[5] The International Business Times article *“Average Value of Top 4 Social Media Sites is $101 per User”* by Vittorio Hernandez, 26/June/2014, http://au.ibtimes.com/articles/557097/20140626/average-value-top-4-social-media-sites.htm

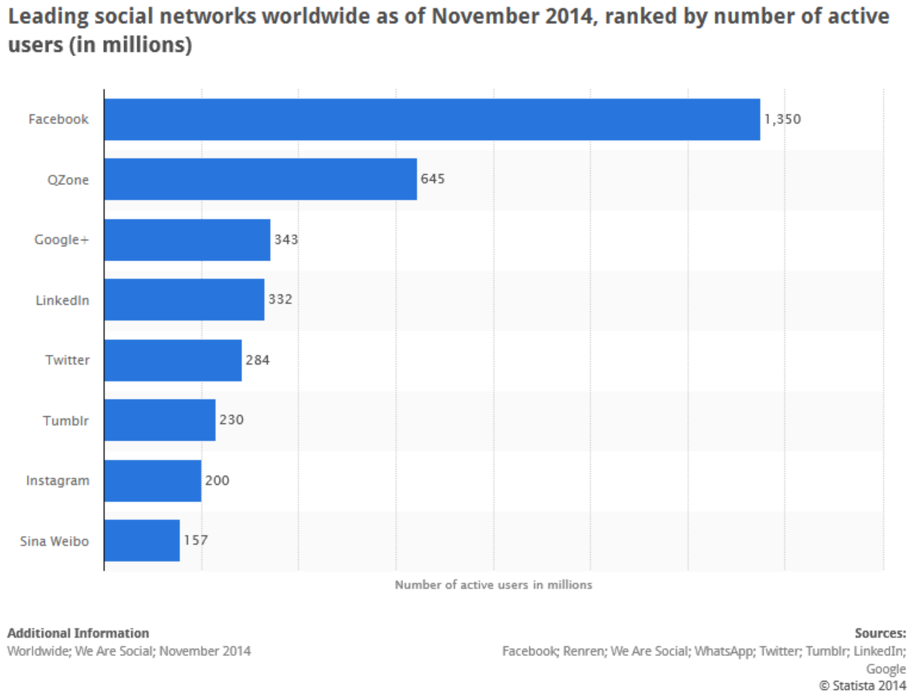

Figure 1. The above chart provides information on the most popular 'OSN worldwide as of November 2014, ranked by number of active accounts (in millions)' [6]

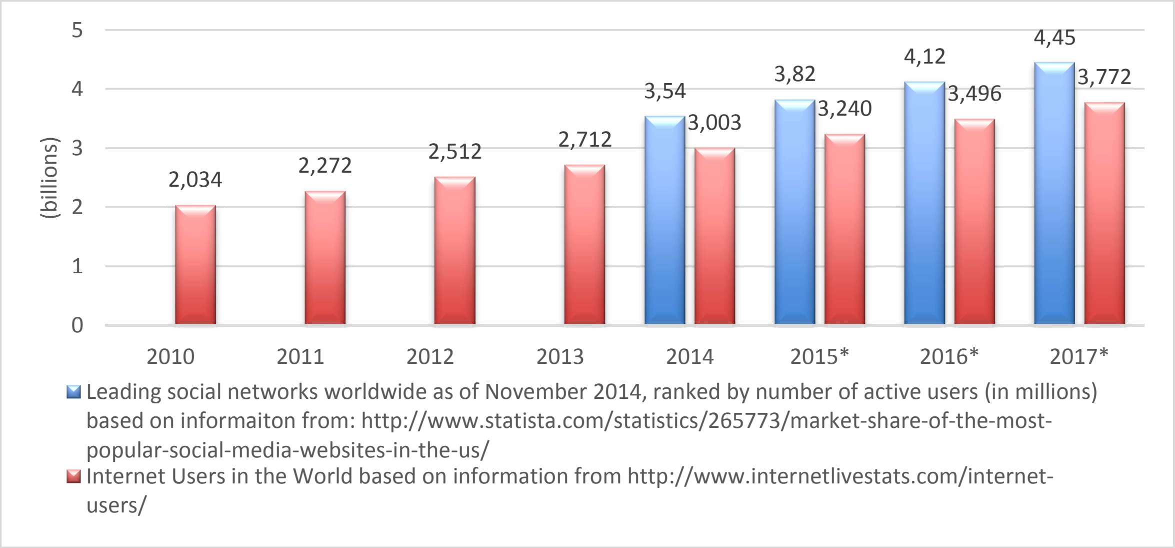

Figure 2. The above is a chart that includes the internet user worldwide (orange lines) the OSN active users from the most popular 'OSN worldwide as of November 2014' (sum of values from Figure 1) and the forecasting based on population increase until 2017

From a market of $358 billion ($449 by 2017) the steady OSN leader in active users (see Figure 1 around 1.35 billion), most visited OSN[7] and marketers favourite is Facebook. In the

[6] Online statistics, title *"Leading social networks worldwide as of November 2014, ranked by number of active users (in millions)"*, http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[7] The graph with the figures on the web link is April 2014 with values from the OSNs visits. Source Dreamgrow.com article, title *"Top 10 Social Networking Sites by Market Share of Visits [June 2013]"*

OSN market Facebook as a business *'has built its $173bn market valuation around profiling its users and showing them targeted adverts. It has refused to allow users to subscribe with money rather than personal data'* [8].

The above short overview of the OSN market landscape shows that it is in the OSNs to exploit their user-base's private data in order to generate revenue streams. The following sections elaborate on the main technology players (solutions, platforms) that are relevant to the USEMP project ecosystem:

- Privacy aware OSNs
- Privacy feedback & awareness
- Multimedia Information Extraction
- Monetisation of crowd sourced content
- Advertisement Filtering and Online advertising.

An analysis of strengths, weaknesses and identified opportunities and risks (SWOT) is provided, while the business model is presented wherever the latter is clear from the available sources. The descriptions below and mainly the content of the SWOT tables are based on the analysis of the USEMP authors' and the information that is available at the official web sites of each solution.

2.1. Privacy aware OSNs

Diaspora: Diaspora markets itself around three key words: decentralization, freedom and privacy. It has no central base, but makes use of servers all over the world (called pods), each containing the data of those users who have chosen to register with it. Their decision can e.g., be based on the privacy policy of the Pod-administrator. This *decentralization* makes it less likely that the private-data of users can be hacked. Another feature of this social platform is that it does not oblige users to identify themselves. Moreover it aims at enhancing the users' privacy online by:

- Promising that diaspora will never use your data for any other purpose besides connecting with others
- Granting the users control over which server can store their data. If they want they can set up and host their own server
- Providing the users with audience management tools

Strengths	**Weaknesses**
• Addressing privacy concerns by installing a decentralized social network. • Independent/Crowd-run initiative. • Possibility to set up your own Pod.	• Doesn't have an aggressive marketing strategy to attract users. • Only 400 000 active users, which is only a fraction of the amount of e.g. Facebook users.

by Priit Kallas, June 2013, http://www.dreamgrow.com/top-10-social-networking-sites-by-market-share-of-visits-june-2013/

[8] The Guardian article *"Could even Facebook become a convert to privacy?"* by Ian Brown, 24/2/2014, http://www.theguardian.com/commentisfree/2014/feb/24/facebook-privacy-convert-personal-data-mining

• Allows posts to be imported from other social network sites	
Opportunities	**Threats**
• Crowd funding. • Growing market for privacy aware social networks. • It is/was one of the most well-known solutions.	• Facebook and other social network sites, fixed some of their privacy issues or incorporated some of Diaspora’s solutions. • Founders handed over the project. • Momentum seems to fade.

Table 1. Diaspora SWOT

Diaspora was launched in 2010, gaining $200 000 by crowd funding. It only generates income from donations. In august 2012 the developers handed the project over to its community. Since that date it has been fully developed and managed by the community members. Estimated amount of active users: 400 000 (2013).

Friendica: Like Diaspora, Friendica counters privacy issues by providing a decentralized architecture with no central authority or ownership. Besides this, it also offers what Diaz & Gürses (2012) describe as privacy as confidentiality as it provides encryption on messages and private conversation groups (as a form of audience management). Furthermore Friendica holds, among others, the following features:

- You can disable people from viewing your profile anonymously
- You can set an expiration date on the content you post, as such it will be deleted automatically everywhere
- Location and other private information embedded in uploaded photos from cell phones is stripped
- One person is allowed to create multiple accounts for different audiences

Strengths	**Weaknesses**
• Addressing privacy concerns by installing a decentralized social network. • Independent, volunteers. • Implements multiple privacy enhancing features. • Access to most other social network contacts, email contacts, RSS feeds, … which also counters the small amount of users.	• Claimed to be not as user-friendly as similar websites (more tech savvy users). • As a result it holds only a fraction of the amount of users of big social network sites. • No real marketing strategy.
Opportunities	**Threats**
• Growing market for privacy aware social networks. • Gathers users from different services in one social network.	• Some of the bigger networks don’t allow access anymore through Friendica. • Many alternatives exist.

Table 2. Friendica SWOT

Friendica is a volunteer-effort, based on the goodwill of its users and enthusiasts to give (monthly) donations. At the moment they are creating a spin-off ‘Red’ that will charge the user for extra features, such as a large number of friends or additional photo space.

WeOurFamily: WeOurFamily presents a different solution to the privacy-concerns. Instead of depending on a decentralized architecture and the effort of volunteers, it has a business model where the user has to pay an annual subscription to create content. In exchange they promise to never sell your personal data or post advertisements to create revenue. Other privacy enhancing features include:

- They use industry-standard SSL-encryption to prevent others outside your intended audience to view your content
- They hold privacy by default setting: initially, all information one posts can only be seen by him. The user can later broaden his audience consciously.

Strengths	Weaknesses
• Addressing privacy concerns by promising never to sell data to 3rd parties in return of a fee • Makes use of encryption. • Greater control over who is in the audience. • Subscription fee generates trust.	• Subscription fee may inhibit widespread use. • User Interface.
Opportunities	**Threats**
• Growing market for privacy aware social networks. • Targets a niche market for people who only want to share within their families/close friends (e.g. baby pictures).	• Facebook recently also changed its default setting when posting to content to ‘friends’ (no longer public). • After 5 years it still sayed to be in Beta-version, slow improvement..

Table 3. WeOurFamily SWOT

Users have to subscribe to a one year contract by paying $21,99, which gives three licenses for using the website. In return, WeOurFamily does not sell personal data to advertisers. Users do not have to pay this as long as they just want to see or comment on what others have posted. Payments are only necessary if they want to create content themselves.

Glassboard: Glassboard is an application where you can create ‘boards’ (groups of people) with whom you can chat and share your location, photos, video, text and other files. It is available for iOS, Android and also has a web-based alternative. You can be part of several boards for different interests, and neither group will know about the other. Only people who are in the same board can see your name and phone number (if you choose to include this information). Other privacy enhancing features include:

- Glassboard has an easy to read privacy agreement
- Glassboard makes use of encryption
- Glassboard will never sell, rent or share personal information to third party companies for marketing purposes.

Strengths	Weaknesses
• Addressing privacy concerns by promising never to sell data to 3rd parties in return of a fee. • Makes use of encryption. • Greater control over who is in	• Positions itself as a solution for businesses, to a lesser extent also for friends, families, scope is unclear. • The free version offers a very

the audience by use of 'boards'. • Available on different platforms.	limited data storage per board. • Premium version might be less attractive.
Opportunities	**Threats**
• Growing market for privacy aware social networks. • Niche market of businesses.	• Many (cost-free) alternatives exist to a certain extent, TMTs for smartphones.

Table 4. Glassboard SWOT

Besides a free version, there also exists a premium version for $5/month or $24,99/year, which has more features such as larger storage to the boards.

Ello: Ello is a social network service that provides an ad-free alternative to the more established social network platforms. With regards to the privacy of its users, it promises the following features:

- Ello will never sell data about its users to third parties
- It's transparent in the sense that it clearly states which information they collect and for which purposes in a easy to read document on their website
- It's not necessary to have an account under your real name

Some privacy enhancing features under construction:

- Private accounts
- Private messaging

One big shortcoming is that all of it profiles are public.

Strengths	**Weaknesses**
• Addressing privacy concerns by promising never to sell data to 3th parties. • Transparency towards collecting information. • Hyped in September 2014 thanks to their 'no real-name' possibility.	• No encryption. • Closed source (no transparency). • Venture capital investment. • No privacy settings: all profiles are public.
Opportunities	**Threats**
• Hype in September. • People are looking for privacy aware / ad free alternatives.	• Still in beta version at the moment, some bugs are reported. • All profiles are public. • Moment might fade.

Table 5. Ello SWOT

To launch the website on a wider scale, $435000 was injected from venture capital investor Fresh Tracks Capital in January 2014. In the future a freemium – model might be introduced according to its founder.

Overview: To sum up, it seems that many privacy aware alternatives are trying to get a piece of the online social networking market. The commotion that can arise with the more famous alternatives (think of the amount of people requesting accounts for diaspora and Ello in their first weeks) shows that a segment of the users are concerned about their privacy online and are interested in alternatives. Nevertheless, until today it seems that their joint biggest weakness lies in reaching a critical amount of users in order to be considered a genuine alternative to Facebook and Twitter. When we look at diaspora, the biggest effort to date, we have to notice that their momentum seems to have faded. Most existing OSNs come in the form of a website (sometimes with an accompanying mobile application), only one of the platforms we studied exists solely as a mobile application, Glassboard. With the exception of WeOurFamily, they all have a free version of the platform. Since they promise not to sell personal data to advertisers, they get money either from funding (from the crowd or venture capitalists) or from their premium version of the social platform. With respect to the USEMP-project it is interesting to see which strategies these websites use to provide more privacy and control over personal data.

2.2. Privacy feedback & awareness

As the Internet and the adoption of online social networking services continue to proliferate, issues surrounding privacy remain a common cause for concern. There is growing anxiety among Internet users of how their online activities are tracked for commercial or other purposes. In light of these increasing concerns, companies and organizations are trying to implement a number of applications for privacy feedback and awareness to be able to capitalize on this trend and to address users' concerns. Here, we briefly describe the most well-known of such privacy feedback and awareness (also known as PFA) tools.

F-Secure Safe Profile: This is a third party Facebook application that helps users to find out how much of their profile information is potentially visible to strangers, and provides suggestions on how to better protect personal information. In other words, the application scans the user's Facebook profile for privacy vulnerabilities and recommends changes. F-Secure Safe Profile is a product from F-Secure, a company with long experience in security and privacy focusing on cloud-based services to protect people's identity, data and devices in the post-PC era and multi-device environment. The app is currently on beta version seeking the users' feedback to identify bugs and provide better services.

Strengths	**Weaknesses**
1. Long experience in security and privacy online 2. Scans the entire Facebook profile of a user to better protect personal information.	1. Available only for Facebook. 2. Still in beta version.
Opportunities	**Threats**
1. Growing variety of connected devices and services. 2. Social media and mobile devices are making users' security and privacy more vulnerable. 3. Facebook users have become much more conscious about the need for security.	1. The market landscape for security software technology will change. 2. Privacy settings on Facebook constantly change. 3. Gathering of user data.

Table 6. F-Secure Safe Profile SWOT

F-Secure Safe Profile is currently on beta version, free for users to install and use. Generally the company allows a period of free trial for their products and then urges companies and consumers to purchase the product. The company focuses primarily on small and medium-sized businesses and consumers by leveraging its current channels and could potentially use Safe Profile as a vehicle to access new markets and stakeholders to create awareness. F-Secure has a strong relationship and solid track record of doing business with over 200 operator partners that serve hundreds of millions consumers and businesses in over 40 countries. The company also has thousands of resellers providing services to businesses. F-Secure has built direct-to-consumer capabilities to drive revenues, to get customer insight directly from consumers and to build brand awareness globally.

Trend Micro Privacy Scanner: This app scans users' Facebook security and privacy settings, and identifies any risky settings for them. It then recommends the changes required and allows users to make the changes. When Facebook updates the privacy settings from time to time, Trend Micro Privacy scanner will be automatically updated so the user can rescan his Facebook profile to make sure it is safe. When combined with other Trend Micro mobile apps like Trend Micro Mobile Security & Antivirus, it is able to identify other apps that impact privacy as well as any risky Facebook settings. The app is freely available.

Strengths	**Weaknesses**
1. Recommends changes to secure privacy. 2. Automatically updated when Facebook updates privacy settings.	1. Needs combination with other tools to identify apps that impact privacy 2. Available only as a mobile app. 3. Available only for Facebook.
Opportunities	**Threats**
1. Over 600 million users access their Facebook profiles via their smartphones. 2. Over 1/3 of people don't know about the security and privacy settings, don't change them or just allow anybody to see anything.	1. Unclear business model. 2. Gathering of user data.

Table 7. Trend Micro Privacy Scanner SWOT

ESET Social Media Scanner: This is a free app to secure Facebook and Twitter accounts from malicious content. On Facebook, it protects the newsfeed, messages, timeline and the timelines of friends. On Twitter, it protects the user's profile and posts from those that she is following. The ESET Social Media Scanner is completely free and is independent from other ESET security products. The user can also create an account so as to:

- Protect unlimited number of social media profiles - of friends and family
- Access all her profiles from one my.eset.com account
- Scan all social media profiles at once
- Explore other online services such as ESET Anti-Theft.

The application is freely available.

Strengths	**Weaknesses**
1. Secures Facebook and Twitter accounts from malicious content. 2. Protects also friends and family's accounts. 3. Multi account management. 4. Great documentation.	1. A missing feature is the option to evaluate your privacy settings and suggest improvements 2. There is a need to create an ESET account 3. Unclear business model
Opportunities	**Threats**
1. Combine the social scanner to other applications of the company to provide an integrated suite. 2. Increasing number of interested people.	1. The market is saturated. 2. Gathering of user data.

Table 8. ESET Social Media Scanner SWOT

AVG PrivacyFix: This offers a simple way to manage one's online privacy settings through their mobile device. The application provides access to one main dashboard that quickly and easily shows what and with whom the user is sharing stuff on Facebook, Google, Twitter and LinkedIn. Moreover, with one simple click the app takes the user directly to where they can change settings. AVG PrivacyFix was designed to let users manage their privacy settings on their phone, tablet, desktop and laptop. The app is free for individuals, and there are business editions available at a cost.

Facebook users are able to:

- Discover over eight different Facebook privacy settings - including some that are not widely known;
- Manage his crowd.
- Stay up to date
- Protect friends or family members who may not be as careful with their privacy settings. AVG PrivacyFix helps spot when friends are oversharing, so that the user can give them a hand.

Google users can:

- Choose what is saved, viewed or blocked - whether it is allowing personal searches to be saved in their Google account, what happens with YouTube viewing history or blocking collection of data history.

Twitter users can:

- Quickly discover and tune Twitter privacy settings;

LinkedIn users are able to:

- Find out whether they are sharing their network with the world and whether others see when they check their profile.

Strengths	**Weaknesses**
1. Available for multiple social media including Facebook, Twitter, Google and LinkedIn. 2. Clear dashboard points you to privacy settings worth checking. 3. Big community of users. 4. Protects friends.	1. Mostly educational in nature; not a true utility. 2. Only one iOS-specific privacy check included.
Opportunities	**Threats**
1. Social media users who care about privacy settings are increasing. 2. Design the platform to target more social media platforms.	1. Gathering of user data.

Table 9. AVG PrivacyFix SWOT

Disconnect: This plug-in reduces user's exposure to many threats, including malware, identity theft, and tracking of their search and browsing history. This software also makes Internet faster and reduces bandwidth consumption, by blocking tracking requests. It is actually a shareware browser plug-in that slaps a green D next to the search bar and shows the number of requests being made on that site for your personal data–and blocks them, speeding up surfing noticeably.

Strengths	**Weaknesses**
1. A large user base. 2. Makes Internet faster not only more secure. 3. Easy to use.	1. Requires custom configuration to block non-consensual trackers. 2. It is not clear if it actually works. 3. It is only available as a browser plugin (not for mobile).
Opportunities	**Threats**
1. Create a mobile app that is able to secure privacy and security for users. 2. Provide an integrated solution to allow privacy management in social media. 3. It is one of the most well-known solutions and has an increasing user base.	1. Potentially unsustainable business model. 2. Increasing competition.

Table 10. Disconnect SWOT

Disconnect is a consumer software company that relies on payments from users for revenue. Their pricing model is "pay what you want" because they believe privacy protection should be available to everybody, irrespective of the ability to pay. Payments help sustain their work and also support non-profits that share their corporate values. Users are also encouraged to try the software before making a decision to pay. In short, a freemium, antivirus-like model is the business model for this enterprise. Disconnect have also come up with Disconnect recommends. According to their website: "The idea behind Disconnect recommends is we'll occasionally show you a recommendation for software similar to Disconnect and Collusion we, the Disconnect team, like and use ourselves. In exchange, we get a referral fee from the developer if you try their software. If you're not interested in a particular recommendation, you can press the close button and we won't show you the recommendation again".

Secure.me: This is a division of AVAST dedicated to making the use of social networks and apps a safe experience. Secure.me is a cloud service connected to Facebook, the center of most social online lives. Sophisticated algorithms analyze and draw attention to actions on Facebook that could hurt one's privacy, security and reputation. Secure.me's Privacy Control monitors personal and sensitive data to protect users' privacy, while providing simple and easy actions for users to secure themselves. App Security uses cutting-edge technology to analyze activities and data access of applications connected to one's Facebook profile. The app identifies untrustworthy actions and data abuse. Its Reputation Guard uses biometric face and semantic language recognition technology to prevent users from over-sharing and damaging their reputation. Secure.me is a free service currently provided by AVAST.

Strengths	**Weaknesses**
1. Uses cutting-edge technology to analyze activities and data access of the applications that users have connected to Facebook. 2. Identifies untrustworthy actions and data abuse. 3. Uses biometric face and semantic language recognition technology to prevent users from over-sharing and damaging reputation. 4. Parents do not have to be registered with Facebook to take full advantage of the	1. Daily and immediate notifications not yet available. 2. Granular control of notifications not yet available. 3. Does not check child profiles for dangerous friends. 4. Secure.me can only get the most recent seven days from Facebook, but in case one turns on automatic monitoring it can capture new activity in real time and retain it for up to 90 days.

secure.me features.	
Opportunities	**Threats**
1. Today, in more than 100 countries and 10 different languages users of all ages. 2. The need for parents to monitor and ensure their children's safety on the Internet and social network sites has risen substantially.	1. Data privacy and security policies. 2. Increasing threat of new entrants in the market.

Table 11. Secure.me SWOT

Lightbeam: This is a Firefox add-on that enables users to see the first and third party sites they interact with on the Web. Using interactive visualizations, Lightbeam demonstrates the relationships between these third parties and the sites that the user visits. During browsing, Lightbeam reveals the full depth of the Web, including parts that are not transparent to the average user. Using three distinct interactive graphic representations - Graph, Clock and List - Lightbeam enables users to examine individual third parties over time and space, and to identify where they connect to one's online activity.

Strengths	**Weaknesses**
1. Informative graphs. 2. Idea that appeals to users. 3. Good ratings. 4. Allows the user to see which advertisers or other third parties are connected to which cookies.	1. Buttons do not work according to a few user reviews. 2. Not useful implementation according to a number of user reviews.
Opportunities	**Threats**
1. An opportunity for Mozzilla to capitalise on growing awareness among internet users of how their online activities are tracked for commercial purposes.	1. What happens to the data collected by Lightbeam is not clear. 2. Need to identify the actual usefulness of the product.

Table 12. Lightbeam for Firefox SWOT

Lightbeam is aimed at a mainstream audience, producing a real-time visualisation charting every site a user visits, and every third-party that operates on those sites that could be collecting and sharing user data. Lightbeam is an open-source tool that is available to view on Github and download directly from Mozilla.

Facebook Privacy Watcher: This is an add-on for Mozilla Firefox and Google Chrome that has been developed at the Center for Advanced Security Research Darmstadt (CASED) in association with TU Darmstadt. It provides a new and simple interface to manage privacy settings on Facebook. The idea of Facebook Privacy Watcher is, to colorize every single item depending on its visibility to one's friends and strangers. So it takes seconds to recognize and change the privacy settings. No clear business model could be inferred from the available sources.

Strengths	**Weaknesses**
1. Takes seconds to recognize and change the privacy settings. 2. After the extension is installed, no further steps are necessary 3. Facebook Privacy Watcher is designed to	1. Manages privacy settings only on Facebook. 2. Extension only for chrome and Firefox. 3. It does not prevent monitoring or

adapt to user needs.	tracking from advertisers.
Opportunities	**Threats**
1. Increasing number of Facebook users interested in protecting their privacy.	1. This add-on is not yet available in the official Mozilla add-ons repository.

Table 13. Facebook Privacy Watcher SWOT

Privacy Badger: This is a browser add-on that stops advertisers and other third-party trackers from secretly tracking what pages one visits. If an advertiser seems to be tracking the user across multiple websites without their permission, Privacy Badger automatically blocks that advertiser from loading any more content in their browser. Privacy Badger is primarily a privacy tool, not an ad blocker. Its aim is not to block ads, but to prevent non-consensual invasions of people's privacy.

Strengths	**Weaknesses**
1. Functions well without any settings, knowledge or configuration by the user. 2. Uses algorithmic methods to decide what is and what is not tracking. 3. Automatically disallows content from third party trackers. 4. A privacy tool, not an ad blocker.	1. Have not made decisions about which sites to block, but rather about which behavior is objectionable. 2. Does not prevent browser fingerprinting. 3. Privacy Badger's icon sometimes does not show up in Firefox. 4. Supports only Chrome and Firefox.
Opportunities	**Threats**
1. Since its launch more than 150,000 people have installed it. 2. It aims to provide something that works automatically without custom configuration. 3. Privacy Badger’s blacklist is user-generated: instead of blocking sites, Privacy Badger blocks objectionable behaviors. As you browse, if it detects the same third-party domain tracking you across three different sites, it blocks it.	1. It is developed by a non-profit so development might encounter problems related to lack of capital.

Table 14. Privacy Badger SWOT

Individual donations make up about half of EFF's support, which gives the company the freedom to work on user-focused projects. The company seeks individuals’ support for the development of Privacy Badger and other projects like it so as to help build a more secure Internet ecosystem.

Bitdefender Safego: This is a free Facebook app that protects users and their friends from malware threats. Safego keeps users safe from all sorts of e-trouble, including scams, spam, malware, and private data by scanning the links the user receives from friends, and monitoring account privacy settings. Moreover, with "Warn friend" option, the user can warn their friends when "fishy" links are posted to their newsfeeds. The application is freely available.

Strengths	**Weaknesses**
1. The BitDefender Safego dashboard shows you at a glance the most recent posts that have been scanned, as well as any that	1. Some users have encountered issues with the app not showing the latest items from their News

have been identified as infected with malware of some sort. 2. The QuickScan button performs an on-demand scan of your PC for any signs of malware.	feed. 2. They have a false positives (items that are clean but are detected as infected) issue with items that contain the full text of a scam. 3. Safego does not allow you to manually check if a link is infected or not.
Opportunities	**Threats**
1. Users spend more time on Facebook than on any other single online destination. 2. With the rise in socially engineered attacks, a tool like BitDefender Safego is attractive.	1. Data privacy policies. 2. It is provided only as a Facebook application.

Table 15. Bitdefender SWOT

Overview: In a nutshell, the market is saturated with a variety of solutions trying to monetize on the increasing needs of Internet and social media users for privacy, security and data gathering from advertisers. Part of the tools is available as web plugins and another part is available as Facebook applications. A few tools are available also for mobile users (as mobile applications for iOS and Android). All tools are provided for free and it seems that in order to be successful in an already crowded and highly competitive marketplace one has to identify a sustainable business model. Such a model should take into account constraints related to attracting a large user base, providing innovative and useful technical functionalities, ensuring transparency about how the app works and how data are exploited and, last but not the least, ensure compatibility with and implementation of the legal framework. USEMP is well placed since these different aspects are covered by the different work packages of the project.

2.3. Multimedia Information Extraction

SimpleWash: This helps users clean up their presence on the Web and become more professional. It is a free Facebook app that searches a user's profile for content that could set off a questionable keyword filter, then it lets the user decide if they want to remove it. SimpleWash looks at the newsfeed, profile wall, photos, even all the links a user has 'liked,' analyzes them and flags anything that can cast the user in a negative light. It then summarizes all the potential social networking flaws in a one-page online report.

Strengths	**Weaknesses**
1. It is a free Facebook app that searches one's profile for content that contains questionable keywords. 2. It summarizes all the potential social networking flaws in a one-page online report. 3. It is easy to use 4. There is a version for twitter as well	1. Not every post SimpleWash picks up will be something that a user will want to remove. 2. Might overwhelm users.
Opportunities	**Threats**
1. Reports say more than 120,000 users have used it to check their profiles 2. Detect visual content in multimedia (photos, videos) posted in a Facebook profile that could be considered unprofessional	1. Data collection privacy policies

Table 16. SimpleWash SWOT

Ditto: It is a logo detection engine that offers brands a new way to understand customer behaviour. This state-of-the art technology "reads" photos shared in social media to find logos and the people with them. Ditto's proprietary technologies provide clients a new kind of customer intelligence. Ditto's algorithm identifies products that it has been trained to recognize, as well as indicators of users' feelings towards the brand like a smile or a frown. By picking out the brands or goods said product is paired with in a given image, Ditto builds maps of product affiliations.

With thousands of images already analysed, the CEO and founder of the company supports that it is simple to turn on analytics for any brand that wants to get the intelligence for a monthly fee. The founders also believe that an ideal business model at this point would be a partnership or acquisition by one of the social networks to help boost revenues by selling sponsored links within photos.

Strengths	**Weaknesses**
1. Unique technological value proposition combining both logo detection and sentiment analysis based on visual information. 2. Flexible fee-based model that is accessible to brands.	1. Over-reliance on personal multimedia content. 2. Potential for misleading results due to lack of proper image interpretation.
Opportunities	**Threats**
1. The availability of visual content will increase even more in the future. 2. Analysis of logos and sentiments in videos and short videos (Vine) could offer added value to even more customers.	1. Risk of disruption of business model by changes in privacy regulations and legal framework (in EU and worldwide). 2. Commoditization of image understanding technology.

Table 17. Ditto SWOT

LogoGrab: This is also a logo recognition platform that provides professional logo detection solutions. It is based on a patented technology that allows to scan logos wherever seen using a smartphone. LogoGrab gives consumers direct access to brand generated content (product info, discounts, etc.) plus real opinions and experiences about brands and products generated by other consumers. It scales exponentially sales and marketing channels of brands and gives consumers direct access to all things relevant about brands and products. Moreover, LogoGrab delivers to brands unprecedented real-time data about marketing effectiveness, customer satisfaction and competition. The app is free but LogoGrab technology is applied to professional solutions for detecting logos within large databases of images and videos. They are also providing an analytics platform for brands.

Strengths	**Weaknesses**
1. Very fast detection of logos. 2. Supports logo detection also for videos. 3. Supports scenarios targeted to professional content. 4. Implementation available for mobile phones.	1. No support for sentiment analysis (compared to Ditto). 2. Lack of accompanying web application. 3. Not very well-defined business model.
Opportunities	**Threats**
1. The availability of visual content will increase even more in the future.	1. Commoditization of image understanding technology.

2. Analysis of logos and sentiments in videos and short videos (Vine) may prove to be an important application of this technology.	

Table 18. Logograb SWOT

Tineye: This is an image recognition platform that provides a variety of services namely a mobile image recognition API to connect users with product information via their smart phone, a Multicolor Engine that allows the user to search by colour, a reverse image search API to automate searching for fraudulent or scammer profile photos, image moderation, verification, copyright compliance and image usage auditing as well as an automated image tracking and analytics service to monitor where one's images appear online.

Strengths	**Weaknesses**
1. It works very well and will even locate images that have been rotated, altered or cropped. 2. Many filters to sort image results. 3. The most popular and widely used reverse search engine. 4. It can also be used to track down illegal use of copyrighted images or stolen ones.	1. The maximum image size for an upload is 1MB. 2. The back-end index that TinEye checks against is rather small. It does not even find the majority of images listed on deviantart.
Opportunities	**Threats**
1. Logo recognition for branding. 2. Discover sentiment in images, with limited success.	1. Google offers similar solutions for image recognition.

Table 19. TinEye SWOT

Besides the free reverse image search engine, TinEye charges different fees for different services aimed at corporations. The basic MatchEngine service for companies starts at $200 a month and rises to as high as $1,500 a month. These plans differ greatly from the free version as they are designed for companies with large databases of photos. The most expensive version offers an image collection size of 200,000 and monthly searches of 150,000. Custom system includes up to 500M images can be proposed "on demand".

Image Raider: This is an automated reverse image search machine that checks Google, Bing and Yandex for websites using a user's image. Image Raider is used by SEOs and digital marketers looking for websites using their images to gain image credit and links, photographers and rights' holders looking for websites who have used their work without permission, users checking if their personal photos have been used online, users who want to find the original source of an image.

Image Raider uses a credit model to ensure that all users get fair use of the resources. Free credits are automatically given when users tweet about the company (50 credits per tweet).

Strengths	**Weaknesses**
1. Flexible and intuitive credit-based system for delivering the service on demand. 2. Application domain of increasing interest. 3. Coverage of a variety of sources.	1. No possibility to evaluate for free. 2. Offered functionality and services not very well promoted and demoed.
Opportunities	**Threats**
1. Potential for expansion to new domains (e.g.	1. Competition by Google Image

detect malicious reuse of news content).	Search (free) and TinEye could prove detrimental.

Table 20. Image Raider SWOT

Nametag: This is an app that will allow mobile users and users of Google Glass to capture images from their live video and scan them against photos from social media and dating sites, including more than 450,000 registered sex offenders. Nametag links ones face to a single unified online presence that includes contact information, social media profiles, interests, hobbies and passions and anything else that the user wants to share with the world. Using the NameTag smartphone or Google Glass app, one may simply snap a pic of someone they want to connect with and see their entire public online presence in one place.

Strengths	**Weaknesses**
1. The app lets users match a face to their online and public record. The app scans a face and pulls up social media profiles but can also browse through 450,000 entries in the National Sex Offender Registry. 2. The app has the added benefit of giving users an easy way to learn more about their date, creating an instant connection based on mutual interest or hobbies. 3. People will soon be able to login to www.NameTag.ws and choose whether or not they want their name and information displayed to others.	1. Performance issues with real time facial recognition. 2. Google has announced that facial recognition will not yet be supported for Glass.
Opportunities	**Threats**
1. NameTag will soon be able to scan a face and compare it with dating profiles from OKCupid.com, Match.com and PlentyofFish.com. 2. Some people believe that this will make online dating and offline social interactions much safer and give us a far better understanding of the people around us. 3. No longer will social media be limited to the screens of desktops, tablets and smartphones.	1. Invasion of Privacy. 2. Sex offender lists are publicly accessible but Mccartan cites a study that concludes public sex offender registries do not increase public safety. 3. Questions if NameTag, and future apps of a similar ilk, will harm social relationships. 4. Questions about database maintenance, accuracy and reliability are also a concern for apps like NameTag. 5. It is not sure that Google will support the project for Glass.

Table 21. NameTag SWOT

Clarifai (www.clarifai.com): This is image recognition and retrieval platform which is based on the winning entry of the ImageNet 2013 competition[9]. The recognition process exploits advanced deep convolutional networks and is able to recognize tens of thousands of different objects. In addition, a powerful content based image retrieval which exploits

[9] http://www.image-net.org/challenges/LSVRC/2013/results.php#cls

recognition results is proposed to the users. The main application areas targeted by Clarifai are: e-commerce, ad targeting, consumer photos, stock photos or security images.

Strengths	**Weaknesses**
1. The app provides image annotation and retrieval tools which are powered by state of the art convolutional neural networks (CNN) and results are very interesting. 2. Results are provided in real time thanks to the use of an optimized CNN architecture. 3. They are able to handle large scale image datasets.	1. They propose a generic tool and it is not clear how easy it is to adapt to specific application domains. 2. The quality of automatic annotation is good but most proposed tags are very generic. 3. Their image retrieval tool seems less precise compared to that of AlchemyAPI.
Opportunities	**Threats**
1. If accurate enough, image recognition can bring added value in a large number of applications, including: search engines, advertisement or e-commerce. 2. Users can use an API such the one provided by Clarifai to better organize their photographic collections.	1. Clarifai evolves in very competitive area of computer vision, in which performances evolve very quickly. 2. It is not clear what the copyright status of the dataset used by Clarifai is.

Table 22. Clarifai SWOT

Temis (www.temis.com): This is a NLP software developer whose main objective is to extract structured knowledge from large and unstructured text collections. They focus on the following aspects: domain knowledge discovery, document filtering, trend mining and knowledge browsing. These modules are integrated in a platform called Luxid which is exploited by clients in a variety of application domains: security, publishing and media, life science and reputation management.

Strengths	**Weaknesses**
1. Temis transforms unstructured text data into useful structured content. 2. They propose their services for over 20 languages and can thus address a large market.	1. The models for different languages have variable quality. 2. While well integrated, their technologies seem to be quite standard ones.
Opportunities	**Threats**
1. They propose a well-integrated platform which is easy to adopt by costumers. 2. They have an established B2B customer base, with focus on life sciences players like Merck, Sanofi or Bayer.	1. Their competition includes big names, such as Google or Microsoft but also promising SMEs like AlchemyAPI.

Table 23. *Temis SWOT*

AlchemyAPI (www.alchemyapi.com): This is a multimedia software provider which bases its solutions on deep learning approaches. AlchemyAPI was initially specialized in text mining but they now offer an image recognition solution. The main NLP features include: entity extraction, sentiment analysis, keyword extraction, concept tagging and relation extraction.

The main outputs of their solutions are: prediction of buyer intent, relevant offerings, brand/product intelligence or question answering.

Strengths	**Weaknesses**
1. Alchemy API relies on powerful neural networks and proposes services related to both natural language processing (NLP) and image recognition. 2. Their NLP services include a strong semantic component. 3. They propose image recognition tools for generic purposes but also for face recognition.	1. Similar to Clarifai, their automatic annotations are often generic. 2. Their image annotation tool seems less accurate than that proposed by Clarifai. 3. The image index they are using seems rather limited.
Opportunities	**Threats**
1. They have a working API to which customers can connect and mine their textual or visual content. 2. They make easy for customers to adopt their products. 3. AlchemyAPI exploits different knowledge bases and is able to link information between these resources.	1. AlchemyAPI evolves in a very competitive domain. 2. The intellectual property status of the images used by AlchemyAPI is not clear.

Table 24. *AlchemyAPI SWOT*

Lexalytics (www.lexalytics.com): This is a company specialized in NLP which proposes two flagship products: Salience, a sentiment analysis engine, and Semantria, a tool for more general text analytics. Their main features include: entity extraction, unsupervised text categorization, text summarization, with all or a part of these features available in different languages. Lexalytics also uses deep learning to empower its products. One interesting feature of Semantria is that it links Excel with unstructured data sources, such as OSNs, for visualization.

Strengths	**Weaknesses**
1. They provide an interesting sentiment analysis tool. 2. Their architecture is scalable. 3. They perform sentiment analysis in different languages.	1. Their tools are less comprehensive than those of competitors, such as AlchemyAPI or Temis. 2. As this is the case for most products of this type, the quality of results varies a lot with the languages.
Opportunities	**Threats**
1. They were among the first companies to work on sentiment analysis and have a well established reputation. 2. They integrate their solution with Excel, a tool which is commonly used by businesses to store their data.	1. Their strategy, which consists in putting sentiment analysis functionalities into two different tools (Salience and Semantria) in not very readable. 2. The field is very competitive.

Table 25. Lexalytics SWOT

Overview: Existing multimedia mining solutions are often focused either on text or image processing, or more rarely on both modalities. Given that text processing is easier to automate; dedicated tools are already widespread in application domains such as Web search, business intelligence, technological watch etc. Due to scalability and accuracy problems, image mining solutions were, until recently adopted mostly in specialized applications. However, recent progress in the field opens the way for wider adoption of these solutions. While a number of solutions exist, recent acquisitions of multimedia mining start-up such as that of DNNResearch by Google show that the market is not yet saturated. Multimedia mining solutions are provided either as part of software platforms which need to be installed at the client side or, more and more frequently, as APIs which can be called through Web services. Usually, these services have proposed a dual functioning mode: free access for a limited number of API calls and paying access if a larger volume of calls is needed. As we mentioned, accuracy and speed are two core characteristics of multimedia mining tools but they are often antinomic. Optimizing one of the two characteristics usually results in a loss associated to the other and working solutions usually propose a compromise between the two. USEMP mobilizes research teams which have strong competencies in both text and image processing and can propose innovative solutions for multimedia mining, with close attention paid to the adaptation of these solutions for personal data management.

2.4. Monetisation of crowd sourced content

The term personal data describes “any information relating to an identified or identifiable individual (data subject)”, based on the OECD Privacy Guidelines. Characteristic categories of personal data include user generated content, activity or behavioural data, social data, locational data, demographic data, or data of an official nature, e.g., financial information and account numbers, health information[10].

Personal data can be considered as an asset for those that generate them as well as for those organizations that collect, store, analyse and use them. Similarly to what is done for to every asset in modern societies, the (monetary) valuation of the personal data is necessary to identify which information is the most important and the most valuable. The value extracted from European consumers’ personal data was worth €315bn in 2011 and has the potential to grow to nearly €1tn annually in 2020, according to research conducted by Boston Consulting Group[11].

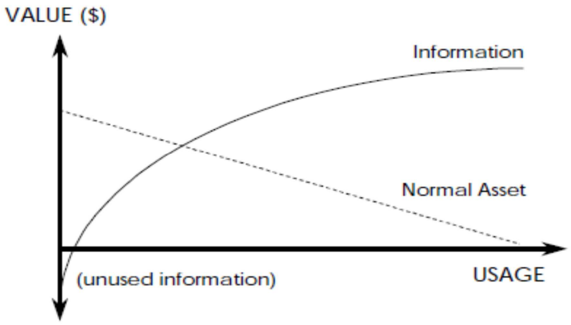

Figure 3: The value of information increases with use

Information actually increases in value the more it is used, while the major cost of information is in its capture, storage and maintenance[12]. An additional major cost that has been added

[10] OECD (2013), “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value”, OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/10.1787/5k486qtxldmq-en

[11] James Fontanella-Khan, “Personal data value could reach €1tn”, Financial Times, 2012

[12] Moody, D.L. and Walsh, P.A. (2002): “Measuring The Value Of Information: An Asset Valuation Approach”, in Guidelines for Implementing Data Resource Management (4th Edition), B. Morgan and C. Nolan, (Eds.), DAMA International Press, Seattle, USA.

the last decade includes the extraction of reliable and valuable information among a big quantity of collected data. The measurement of the value of the personal data is a complex and difficult task. There is no commonly accepted methodology for estimating the value of personal data. Existing approaches rely either a) on market valuations of personal data, or other related market measures or b) on individual perceptions of value of personal data and privacy. For the first approach the market cap/revenues/net income per data record, market prices for data, cost of a data breach, data prices in illegal markets are some the proposed methods to estimate the monetary value of personal data. Alternatively, surveys and economic experiments could be used to estimate the individual valuation of personal data and the individual valuation of privacy. However, this is a complex and very context dependent task.

Datacoup: This is different from the other applications and plugins that are presented in this section. Datacoup helps users to aggregate, package and sell their personal data. Therefore, users can earn money and awareness about their data. The user chooses which data he wants to sell, from social media to his checking account. The more he adds the more he'll make. They also have the option to discover what is interesting about their data through beautiful visualizations and start earning money from it. Privacy is paramount for this platform which is built with choice as the top priority.

Strengths	**Weaknesses**
1. Strong differentiation point. 2. The site layout is simple and intuitive, making it easy to connect and disconnect social accounts. 3. Consumers are encouraged to take educated decision concerning their data 4. Individuals are enabled to benefit from an asset they create each and every day.	1. People deciding whether or not to take the startup's deal must accept that they won't know everything about how their data is used. 2. Measuring privacy trade-offs is exceedingly hard. 3. Until March 2014, no advertiser has bought data.
Opportunities	**Threats**
1. Datacoup collects can be especially useful to advertisers because few data providers can combine traces of a person's online activity with a record of their spending activity.	1. Poor legal framework to deal with such commercial exchanges. 2. Data on consumer behavior is hardly in short supply these days. 3. The idea of people trading their own data has been around for years but has never quite taken off.

Table 26. Datacoup SWOT

On March 2014, Datacoup was running a beta trial in which people get $8 a month in return for access to a combination of their social media accounts, such as Facebook and Twitter, and the feed of transactions from a credit or debit card. The New York City-based startup plans to make money by charging companies for access to trends found in that information, after it has removed personally identifying details.

Overview: The above analysis shows that the first research works for the monetary valuation of users' personal data are based either on market related measures or on individual perceptions of value of personal data. On the other hand, there is the need to design solutions or platforms either embedded to existing applications (e.g., advertising, privacy etc) or provided by external third parties that will offer this type of services to the end uses. To this end, in the context of USEMP, it is necessary to investigate new methodologies by collecting and computing indicators of scores related to the audience in a network (data producers, data consumers), the usage of data and the affinity of users' personal data. The enhanced valuation of personal data will help the end users to increase their awareness about what data-valuation methodologies are utilised to process their personal-data as well as assessment and control of their privacy-level depending on the service-provider data-valuation model.

2.5. Advertisement Filtering and Online advertising

The goals of marketing campaigns are a) product Advertising, b) Brand-Awareness, and c) Direct Response Advertising. Current widely adopted methodologies and techniques in marketing and advertising are highly affected and driven by the rapid evolution of:

- mobile devices technology (i.e., smartphones global penetration with enhanced computational/storage and internet connectivity capabilities),
- wireless access networks (WiFi, 3G/4G) and rich media technologies (e.g., HTML5),
- native application developers evolving communities (mainly driven by three application stores i.e., Google Play (Android), Windows Store and Apple Store (iOS).

The Internet and advertising market and especially mobile advertisement is rapidly growing. There are currently four primary forms of (mobile) advertising:

- Text based (SMS/MMS and text links),
- Search,
- Display (Traditional MMA banners/Rich Media/in-application),
- Experiential – Mobile applications as games and brand advertising.

Display advertising can take many forms:

- Banner advertising, which is the simplest format typically manifested as a small banner displayed within a mobile Internet site or application.
- Rich Media, which add substantial functionality to the advertising experience through expandable banners, web view, embedded video, etc. Typically, this type of advertising is delivered within an application.
- Interstitials, which are full screen takeovers, again typically delivered in an application that can be either Rich Media or static banner.
- Video Pre/Mid/Post Roll, delivered in conjunction with video content prior to, in the middle of, or after the main content ends.
- Offer Walls are a relatively new advertising format and have been historically leveraged in social gaming applications as an alternative to real cash payments for virtual goods.

In some markets[13], this mobile advertising is most commonly seen as a Mobile Web Banner (top of application page) or Mobile Web Poster (bottom of app page banner), while in others, it is dominated by SMS advertising (which has been estimated at over 90% of mobile marketing revenue worldwide). Other forms include MMS advertising, advertising within mobile games and mobile videos, during mobile TV receipt, full-screen interstitials, which appear while a requested item of mobile content or mobile web page is loading up, and audio advertisements that can take the form of a jingle before a voicemail recording, or an audio

[13] http://en.wikipedia.org/wiki/Mobile_advertising

recording played while interacting with a telephone-based service such as movie ticketing or directory assistance.

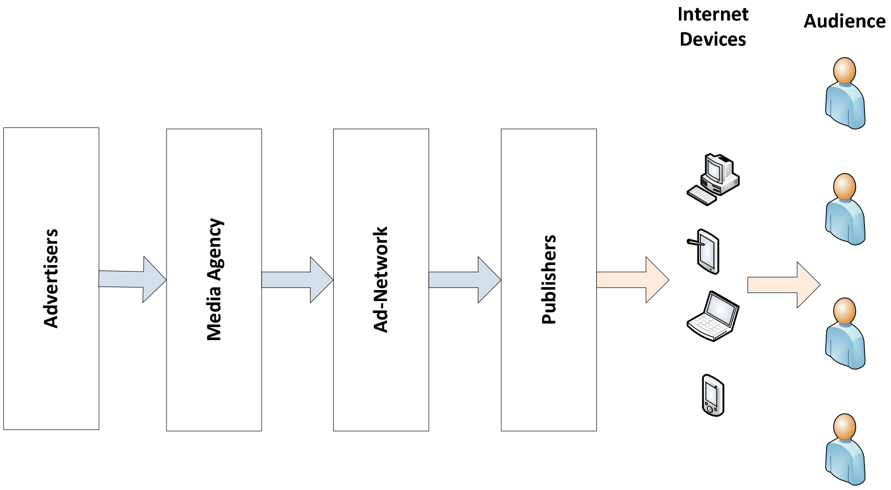

Figure 4: Online advertising value chain

The online and mobile advertising value chain consists of four key elements: on the demand side of the value chain, there are advertisers, and their agencies; and on the supply side, publishers, and ad networks ()[14]. Firstly, *" is being interviewed"* provide the advertisements to be displayed on the publisher's content. *Publisher* is the original source of ad inventory (the owner of a web site, game or mobile portal). By creating a web site or other digital media, and getting people to come and look at it, the publisher creates ad inventory by placing ads alongside the editorial content of their site.

An *ad network* allows an advertiser to deliver their advertisement to a number of individual publisher sites and apps without the advertiser having to negotiate separate deals with each publisher site or app developer. Ad networks exist because there are millions of advertisers and millions of publishers. The *media agency* is an essential intermediary in the advertising value chain, which role includes one of two things: a) ads creation (e.g., animated banner) b) buy the media (i.e. the ad inventory) to display the ads.

The main advantage of mobile advertisement is the fact that it results in more personalized advertisements. In the Q2 2013 "State of Mobile Advertising Report" by Opera Mediaworks, it is reported that mobile advertising is growing globally at a rapid rate. Rich media ads are now averaging a 1.53 percentage click rate among users. In app large banner ads are still the most popular, but they are on the decline. In July 2014 Facebook reported advertising revenue for the June 2014 quarter of $2.68 billion, an increase of 67 per cent over the second quarter of 2013. Of that, mobile advertising revenue accounted for around 62 per cent, an increase of 41 per cent on the previous year[15].

The effectiveness of a media ad campaign can be measured in a variety of ways. The main measurements are impressions (views) and click-through rates. They are also sold to advertisers by views (Cost Per Impression) or by click-through (Cost Per Click). Additional measurements include conversion rates, such as click-to-call rates and other degrees of interactive measurement. One of the popular models in mobile advertising is Cost Per Install

[14] Online Advertising Business, http://www.liesdamnedlies.com/online_advertising_business_101.html

[15] 138pc jump in Facebook Q2 net income to $791 mn". Business Sun. Retrieved 23 July 2014.

(CPI) where the pricing model is based on the user installing an App on their mobile phone. CPI Mobile Advertising Networks work either as incentive or non-incentive. In the incentive model the user is given virtual coins or rewards to install the game or App. On the other, in non-incentive models the users are motivated to download and install an app if the latter is according to their interests.

Google: Google provides two services that support both publishers and advertisers, AdSense and AdWords respectively. Google AdSense[16] is a program that allows bloggers and website owners to make money by displaying Google ads. The revenues are generated based on:

- Impressions: number of pageviews of pages or posts with ads,
- Clicks: number of click on the ads.

The ads are related to what the visitors are looking for to a web site or matched to the characteristics and interests of the visitors the content attracts. Google AdWords[17] is an advertising system in which advertisers bid on certain keywords in order for their clickable ads to appear in Google's search results. Taking into consideration that multiple advertisers may use the same keyword to trigger their ads or want their ads to appear on the same websites. Google uses Ad Rank to determine whose ads will appear, and in what order. Ad Rank is based on the following parameters:

- Your bid, which is how much you're willing to spend,
- The quality of your ads and website,
- Expected impact from your ad extensions and other ad formats.

Keywords can trigger ads to appear next to search results on Google and other search web sites. In addition, keywords can also trigger ads to show on other web sites across the Internet: Google-owned properties e.g., YouTube, Google's partner sites e.g., NYTimes.com or web sites that belong to the Google’s (display) network.

Strengths	**Weaknesses**
1. Service provision in many different groups of people. 2. Easy creation and edit of ads. 3. Support both publishers and advertisers worlds. 4. Quality and customer experience are the primary objects. 5. Effective search engine technology. 6. Large number of users of Google solutions and solutions.	1. Too dependent on advertising revenue. 2. The effectiveness of advertising in many cases is based on cookies technologies.
Opportunities	**Threats**

[16] Google AdSense http://www.google.com/adsense/start/

[17] Google AdWords https://support.google.com/adwords

1. Worldwide internet growth usage. 2. Large list of mobile applications. 3. Awareness of user preferences regarding installed applications. 4. Brand reputation. 5. Increasing worldwide online ad spending. 6. Important investment to the internet of things world.	1. Social networks advertising opportunities. 2. European Union antitrust laws. 3. Internet safety. 4. Large competition.

Table 27. Google SWOT

iAd: is Apple's mobile in-app ad platform. Advertisers can sign in with the same Apple ID that use for other services (e.g., iTunes, the Apple Online Store) or create a new Apple account. Once the iAd Workbench account has been set up, a campaign can be created from the Dashboard. After the campaign has been submitted, you'll be notified within 24-48 hours letting you know when your ads are up and running.

Strengths	**Weaknesses**
1. Large database of mobile applications. 2. Available context information for the applications that are stored at Apple's apps store. 3. Awareness of user preferences regarding installed applications 4. Brand reputation. 5. Strong marketing and advertising teams.	1. Incompatibility with different OS. 2. Smaller group of audience, comparing to their competitors. Focus only on mobile applications.
Opportunities	**Threats**
1. Integration of mobile payment functionalities. 2. Mobile apps discovery service may create new business opportunities. 3. Context-based information that mobile device sensors provide may lead to advanced advertising opportunities.	1. The growth of mobile web-based applications. 2. Strong competition with other mobile OS vendors.

Table 28. iAd SWOT

Facebook: Facebook offers a range of products that allow advertisers to reach audience people on and off Facebook[18]. An advertiser or a business creates an ad and they choose the type of audience they would like to reach. For audience selection advertisers use information such as location, demographics, information provided at registration or added to the account or timeline by the user, things users' share and do on Facebook (e.g., likes, interactions with advertisements, partners, or apps, keywords from users' stories), and things that have been inferred from the use of Facebook. When Facebook delivers ads, personal

[18] Advertising and Facebook content, https://www.facebook.com/about/privacy/advertising

information (e.g., name or contact information) is not shared with advertisers, unless the relevant permission has been provided. Facebook provides the capability to the end users to control the delivered ads:

- Adjust her ad preferences. For instance, receive an explanation of why she is seeing a specific ad it, and she can add or remove herself from audiences who are showing that ad.
- Use mobile device opt outs, for ads that are based on the apps that are installed on a mobile device.
- Facebook partners with the Digital Advertising Alliance (DAA) to help the Facebook users to understand which companies are customizing ads for their browser, and opt out with participating companies.

Strengths	**Weaknesses**
1. Integration with websites and applications. 2. Large number of monthly active users. 3. Understanding of user's needs and behaviour. 4. Excellent user experience. 5. Control delivered ads.	1. Weak protection of the information that users upload to their profile. 2. The way that ads are displayed (i.e. on the wall post). 3. One source of revenues.
Opportunities	**Threats**
1. Increasing number of people that use Facebook through mobile devices. 2. Expansion to new countries. 3. Diversify sources of revenue.	1. Popularity affection due to the protection of users' private information. 2. Strong competition; different types of social networks are developed.

Table 29. Facebook SWOT

TRUSTed Ads: is a comprehensive technology solution that addresses consumer privacy opt-outs across any platform, device, real-time bidding (RTB) technology, or cookie/non-cookie environment. TRUSTed Ads is easy to install and is in use by brands, publishers, and ad platforms worldwide in both desktop and mobile environments. A lightweight ad tag embeds the industry standard Advertising Option Icon on or near an advertisement. When clicked the icon launches an in-ad privacy notice that allows consumers to learn more or exercise advertising choices. Publishers can implement TRUSTed Ads anywhere on a page with a simple HTML code insert. Website publishers can use the Advertising Option Icon or an icon/textual notice of their choosing. When clicked, the icon opens a TRUSTe-powered pop-up that provides consumers with ad privacy notice and the opportunity to opt-out of behavioural advertising.

Strengths	**Weaknesses**
1. Provide to the user the opportunity to opt-out of behavioural advertising. 2. Supports different platforms (in ad, on site, mobile application). 3. Reach audiences across all devices regardless of platform or	1. There is not any special focus on Online Social Networks. 2. Provide the capability to opt-out from specific networks or receive ads based on specific interests, but it is not clear whether the end users have the option to allow or

cookie/non-cookie environments. 4. Facilitates the personalization of consumers digital advertising experience. 5. Approved by the Digital Advertising Alliance (DAA).	block the usage of specific data or information (e.g., geo-location).
Opportunities	**Threats**
1. Serves a large number compliant impressions a month. 2. Online advertising growing is increasing. 3. End users and publishers/ advertisers interest for privacy issues is increasing.	1. Wider adoption might be affect by the fact that TRUSTed Ads is a module of the TRUSTe Data Privacy Management Platform 2. The provision of consumers interests to advertisers might increase the suspiciousness for the service from the consumers side.

Table 30. TRUSTed Ads SWOT

Overview: Online advertising constitutes one of the major sources of revenues for business on the web, while different stakeholders are involved in this ecosystem. The number of viewers (clicks, impressions, downloads) and the information that are available for the target audience are some of the most important parameters for the effectiveness of an advertisement campaign. Different types of web sites (e.g., social networks, application stores, web search services) provide advertising services to advertisers adopting one or more roles in this complex ecosystem e.g., publisher, ad-network. Privacy is a key issue that that is increasingly discussed together with the growth of online advertisement. The need to increase end users awareness and control around the way that their personal data are used is of utmost importance both for legal issues and for the evolution of World Wide Web.

Towards this direction USEMP intends to provide to the end users the control over the exploitation of their personal data, exploiting different means described in this section. In addition, more personalized service will be provided by a wide range of stakeholders that aggregate and use users' personal data (e.g., Mobile Marketing Advertisers, ISPs), since the USEMP users will be aware about the (monetary) value and the usage of their information that they have either directly provided or indirectly observed. Transactions between service providers and users will benefit from the loyalty and trust that will be built as an outcome of the USEMP platform.

3.USEMP Results

The main outcome of USEMP is the proposal of personal data management tools which are informed by inputs from different disciplines: legal research, user and living lab studies, multimedia information extraction and social networks analysis. More specifically, we target two types of tools which correspond to important OSN user needs:

- User empowerment for improved OSN presence control, with real-time and long-term presence management functionalities.
- OSN data value awareness tool, with awareness about personal information value and simulated personal content licensing functionalities.

Legal research

The legal research is focused on developing requirements for Data Protection by Design, notably with regard to profile transparency. The aim of the USEMP DataBait tools is foremost to empower users of OSNs by reducing the information asymmetry between profilers and profiled. This does not necessarily mean that people will share less data or more data, but that they become aware of how their volunteered and observed data may be used to derive inferred knowledge that is applied to them. Users may start sharing different (types) of data and become more actively involved in the emerging personal data ecosystem (user participation). Simultaneously, iCIS conducts legal research into the nexus of data protection rights and intellectual property rights, noting that the latter concerns both the copyright of OSN users on their user generated content (postings, photographs) and Intellectual Property (IP) rights of data controllers on data bases, algorithms and profiles. Finally, while USEMP was preparing the Databait tools, the legal researchers developed a so-called data licensing agreement as a legal ground for the processing of personal data of DataBait users, clearly indicating what USEMP offers in return. Summing up, USEMP delivers the results of innovative legal research on four accounts:

1. By providing clear guidance on the legal requirements for counter profiling tools, i.e. tools that infer patterns and profiles from relevant user data, thus showing how OSN users may be profiled by their OSN provider and third parties.
2. By providing clear guidance on the legal constraints on profile transparency, due to the fact that OSNs may claim their profiles are protected by trade secret, copyright in the database or the database right sui generis.
3. By providing clear guidance on the copyright that users may have in their postings and photographs and on the idea of a portrait right in the digital portraits that OSN service providers or third parties develop and construct when they make sophisticated individual profiles of their customers or apply sophisticated aggregate profiles on their customers.
4. By developing a Data Licensing Agreement that is succinct, written in clear language, offering DataBait users the possibility to license the use of their personal data for a specific purpose in exchange for receiving a form of profile transparency. In principle such a DLA could also be developed for other purposes in exchange for other services. It may provide an explicit legitimization of exchanging personal data for free services, while simultaneously providing the data subjects with enforceable rights against inappropriate usage.

User and living lab studies

In USEMP a Living Lab approach will be used to engage users early and throughout the project so that all tests are done in collaboration with the users. Living Lab activities are based on needs and motivators which will be identified and the result from this will lead the pilot case deployment to have a pilot that really engage and motivate users.

In USEMP we have two active living labs who contribute to user studies and who will run the iterative and interactive piloting. The first is Botnia Living Lab which was founded in 2000 and is a world-leading environment for user-centric research, development and innovation (RDI), supported by innovative methods, tools and experts. iMinds is hosting the second Living Lab iLab.o which was founded in 2009 and started building a test panel straight away. These panels change continuously with people signing in and out every day.

Expected results in this area are:

- Within the USEMP project the endeavour is to strengthen current Living Lab practices by developing processes for user empowerment and emancipation focusing on guidelines for privacy by design in innovations.
- Strengthened benefits for citizens to participate in Living Lab activities, enabled by the innovative usage and exploitation of ICT tools and facilities available in FIRE and ENoLL.
- Increased knowledge on user motivation in the adoption process of privacy enhancement tools.
- User approved and tested usability of DataBait in terms of visualization and managing flow of personal information within the web/OSN.
- Raised user awareness related to economic value of their personal data and personal content licensing.
- Raised user awareness related to user privacy and privacy enhancement tools.
- Processes and tools that protect users privacy in user studies.
- Increased understanding of users' experiences of information and social privacy issues.
- Increased understanding of how Living Labs experiment should be structured and facilitated to support new strategies and tools for privacy in design.
- New methodologies and technical support for open user-driven innovation with a Living Lab approach and contribute to the collected knowledge in that area by adding the privacy issue.
- Strengthening and empowerment of users in protecting their privacy via data management.
- Processes for user engagement in privacy studies.

Multimedia information extraction

- Large-scale image recognition tool which is able to deal with thousands of different concepts. Focus will be put on places, face, logos/products but these modules will be derived from a more generic architecture.

- Innovative and robust modules for named entity recognition, text geolocation, semantic similarity and sentiment analysis.
- Text-image fusion modules which leverage results obtained with individual modalities.
- Integration of the developed tools in CEA's multimedia mining platform.
- Privacy-aware image classification and ranking.
- Visual analysis approaches for automatic estimation of images geographic location.

Social network profile mining and services

- User profile categorization in a number of personal dimensions (e.g. demographics, sexual orientation, political attitudes, etc.) based on behavioural data (likes, visited web pages, etc.).
- Private information leak risk prediction based on behaviour and personal social network analysis.
- Privacy settings learning and prediction.
- Monetary valuation of user personal data.
- Web trackers identification and setting of do not track policy rules.

4.First Report for Exploitation Activities

4.1. Velti Exploitation Plan

4.1.1. Partner Profile

Velti is a leading global provider of mobile marketing and advertising solutions that enable brands, advertising agencies, mobile operators, and media to implement interactive and measurable campaigns by communicating with and engaging consumers via their mobile devices.

Velti's technology platform enables its customers to use mobile media to plan, manage and optimize mobile advertising and marketing campaigns, reaching consumers, engaging them through mobile messaging, mobile Internet and mobile applications, and helping customers achieve their marketing performance targets with their respective audience. Velti holds a global infrastructure that allows it to deliver multiple campaigns globally every year reaching out practically to any consumer that has a mobile device and holds a number of patents in mobile marketing and advertising methods. As an example of Velti's clientele more than 10 of the top-20 mobile operators worldwide have run mobile marketing campaigns using Velti solutions in that last 5 years.

Velti's core skillset is analyzing, designing, prototyping, productizing and optimizing mobile marketing and advertising campaigns. In terms of the use of consumers personal data Velti's core value is to safeguard the transparency of the use of user's personal data, ensuring that all appropriate measures have been taken to receive user's consent before any such data are utilized in any way and conforming to the local administrations legislation across the globe.

Velti constantly experiments with new innovative ways to engage with consumers, new means for creating successful campaigns and new business models across the mobile marketing & advertising value chain. Velti's teams include experienced designers, developers, analysts and projects managers that have worked on a long list of applications/campaigns and products for mobile which have been developed either for the company's customers and or as standalone applications marketed directly to the consumers.

Velti holds a dedicated department for innovation, research & development with analytical and innovation skills with a broad range of expertise: from technology architects to experienced technical/business analysts, solution consultants and user experience/concept designers. In the past Velti's innovation team has participated in a number of EU FP7 research projects, examples of which are EFIPSANS, SKYMEDIA, DIG, 3DTVS, TEFIS. In the area of transparency and data privacy the Velti innovation team has developed expertise in the field with two active EU FP7 funded projects: OPENi and USEMP.

4.1.2. Individual Exploitation Strategy

Academic & research exploitation plans

As a leading global provider of mobile marketing and advertising technology, we understand the importance of privacy about public administrations, exclusively being our customers. The main focus is to disseminate the concept and tools towards various recipients focusing on organizations in the online privacy and data protection sector. More specifically dissemination actions will aim at the participation in selected exhibitions, workshops and scientific conferences, as well as scientific publications to allow distribution of project results to a wide range of audiences (GSMA MWC, AAAI International Conference on Weblogs and Social Media and the World Wide Web Conference will be among the candidate events and venues). Raising citizens' awareness concerning the opportunities and risks related to personal information sharing is of extreme importance as well as open communication channels with standardisation bodies.

Industrial exploitation plans

Velti is a leading global provider of mobile marketing and advertising technology. We see a very important social and commercial requirement for increasing end users' awareness and control capabilities regarding the privacy risks that arise due to the information that they distribute to or receive via an application, a website or an IoT device. The results of this project will help Velti to specify and develop future mobile marketing and mobile advertisement applications, where the end users will be more aware and can control how and where their data are used and the most important, with an increased trust. The latter will facilitate the advertisers to enjoy a highly targeted and successful campaign, since users will be less cautious to the proposals and recommendations of the advertisers. New business models will be explored based on the estimated value of the personal data. In addition Velti will also investigate the potential to develop a new product for privacy certification of application publishers that complies with the European legislation. Knowledge gained during USEMP work will help Velti to be ready for the upcoming challenges as a marketing and advertising technology provider.

4.2. HWC Exploitation Plan

4.2.1. Partner Profile

HW COMMUNICATIONS LIMITED (HWC) was founded in 1990 and has traditionally focussed on advanced research and development in mobile and wireless communications, which have been implemented as bespoke solutions for external companies and government agencies. HWC's unique breadth of capability spans all layers of the communication stack, allowing for optimum consideration for secure and resilient communication systems. Cyber Security & Resilience has been at the core of HWC's activity right from the start. Within the past 22 years, HWC has developed its capability from its baseline academic foundation in information theory and cryptography and developed many solutions for securing communication systems and ensuring that their operation is reliable and trustworthy.

Through both commercial and publicly funded R&D, HWC remains on the leading edge of Cyber Security and Resilient Communications. Research activity is grouped into the 'Protection of People and Infrastructure' and 'Protection of Identity, Privacy and Trust'.

4.2.2. Individual Exploitation Strategy

Academic & research exploitation plans

HWC does not have current academic and research exploitation plan.

Industrial exploitation plans

HWC's exploitation strategy is based on the Dynamic Consent Open Framework (DCEF) which is currently targeted for biomedical research, with a market expectation of £3-5million European licenses sales annually. Should USEMP successfully deliver its planned capability we open up a much larger consumer market place for DCEF. Considering the current stance of the European directives, this market place is considered difficult and potentially too large to quantify at this time. One could consider at least 10 fold increase in market size once European directives are in place. USEMP is well placed to deliver early deployable solutions within a 5 year timeframe from the writing of this document.

At the time of writing of this document DCEF is beginning to roll out in the healthcare sector. Whilst HWC do not necessary have direct routes to OSN markets right now, nor enough understanding to operate Dynamic Consent within OSN, it is expected that the involvement in USEMP will increase HWC's network and the expansion of the technology and market place into the OSN sector. As is evidenced by previous collaborative research work carried out by HWC, all relevant IP generated in USEMP will be carried forward to commercialisation of DCEF for OSN. The working relationships within the project are therefore also considered vital for future exploitation, impact and commercial success.

4.3. CEA Exploitation Plan

4.3.1. Partner Profile

CEA LIST is a key software systems and technology research centre working in three areas with vital societal and economic implications: embedded systems, interactive systems, signal detection and processing. The 45 engineers and researchers affiliated with CEA LIST's Vision & Content Engineering Laboratory (LVIC) work on multimedia and multilingual data analysis and understanding, with a focus on fast growing and large public application domains. The core activities of the lab are structured around: technological watch, information retrieval, video surveillance and new applications associated to mobility (augmented reality, multimedia content management, embedded mobile applications). The scientific challenges addressed by LVIC are twofold: developing efficient and robust multimedia content mining algorithms relying on the extraction, classification and semantic analysis of each modality, respectively developing methods and tools for the construction, the formalisation and the organisation of knowledge needed by the algorithms.

4.3.2. Individual Exploitation Strategy

USEMP is central to CEA’s roadmap regarding multimedia data mining and project results will be integrated in the lab’s offering. CEA role as a facilitator between academia and industry determines an exploitation positioning which combines scientific and applicative aspects which are described below.

Academic & research exploitation plans

USEMP results will be evaluated and exploited in scientific and international evaluation campaigns. The main venues targeted for publishing/testing the outcomes of the project are:

- **Conferences**: ACM Multimedia, WWW, ACM CIKM, AAAI ICWSM, ACM WSDM, ACM ICMR, Web Intelligence.
- **Journals**: IEEE Transactions on Multimedia, IEEE Multimedia, MTAP, IEEE TKDE
- **Evaluation campaigns**: Mediaeval, ImageCLEF

Depending on the advancement of WP5, in 2015, CEA plans to submit 2 or 3 papers to the conferences cited above and 1 journal paper stemming from the collaboration with CERTH. Equally important, following a joint participation to the Mediaeval 2014 Placing Task, CEA and CERTH plan to take part in at least one evaluation exercise in 2015.

Industrial exploitation plans

USEMP results will be integrated in the lab's offering and the creation of a start-up is currently investigated. Very promising results were already obtained in image mining and more particularly for copy detection and large scale recognition and retrieval. Patent applications are being prepared for each of these technologies for registration before the end of 2014. The two technological bricks are currently integrated in the lab's multimedia mining platform.

On the longer term, CEA will continue integrating its USEMP tools in its multimedia mining platform and will exploit them in its collaborations with industrial partners. Contacts were already established with French SMEs for the exploitation of the copy retrieval brick. Of prime importance in CEA's strategy is the creation of a spin-off which would exploit USEMP large scale recognition and retrieval results. A market analysis is scheduled before 2014 in order to determine the most promising exploitation paths and the effective creation of the start-up is foreseen for mid-2015.

4.4. iMinds Exploitation Plan

4.4.1. Partner Profile

iMINDS is an independent research institute founded by the Flemish government to stimulate ICT innovation. The institute brings together companies, authorities, and non-profit organisations to join forces on research projects. iMINDS unites more than 600 researchers from numerous Flemish universities and knowledge centres. It consists of 5 research departments. Each research group is specialized in one or more of the basic competencies of iMINDS: networks of the future, advanced software technologies, multimedia and interfaces, policy and law, market issues and user research. Since its establishment in 2004, iMINDS has run more than 250 projects, representing a total value of well over 250 million euro. In USEMP it is the iMINDS research group SMIT that participates, which is also part of the iMINDS Research Department 'Digital Society'. SMIT, established at the Vrije Universiteit Brussel (VUB) in 1990, is specialized in fundamental, applied and contract research in the area of ICT and media, markets and policy. With currently a staff of over 75 researchers, and an annual turnover of well over 3.5 M€, SMIT is a major research centre in Europe for policy & socio-economic research relating to ICT and media. SMIT research combines user, policy and business analysis with both quantitative and qualitative research methodologies.

4.4.2. Individual Exploitation Strategy

Academic & research exploitation plans

USEMP results will be investigated and exploited in scientific publications and international conferences and workshops. Key venues for publishing and discussing the outcomes of our USEMP results are:

- Conferences: IAMCR, ICA, ECREA, AOIR, SOUPS, CPDP, Digital Enlightenment Forum, 4S, EASST, ESA
- Journals: Telematics & Informatics; New Media and Society; European Journal of Communition; Computers in Human Behavior; Communications & Stratégies; Science, Technology & Human Values; Info - The journal of policy, regulation and strategy for telecommunications, information and media; Journal of Media Innovations; tripleC

Industrial exploitation plans

iMinds has no industrial exploitation plan.

4.5. CERTH Exploitation Plan

4.5.1. Partner Profile

The Centre for Research and Technology-Hellas (CERTH), founded in 2000, is the only research centre in Northern Greece and one of the largest in the country. CERTH has important scientific and technological achievements in many areas including: Energy, Environment, Industry, Mechatronics, Information & Communication, Transportation & Sustainable Mobility, Health, Agro-biotechnology, Smart farming, Safety & Security, as well as several cross-disciplinary scientific areas. CERTH is essentially a self-supported Research Centre generating an average annual turnover of ~€ 22 Million coming from: (a) >30% from bilateral industrial research contracts, (b) >60% from competitive research projects, (c) <10% as government institutional funding. CERTH participates in USEMP through ITI, and more specifically through the Multimedia Knowledge and Social Data Analytics laboratory (MKLab), which currently consists of more than 45 researchers.

4.5.2. Individual Exploitation Strategy

Academic & research exploitation plans

During the last years, the MKLab research team has focused on several key research areas, two of which include multimedia mining and social media analytics. These are well aligned with the R&D activities of CERTH within USEMP. Hence, the work carried out within USEMP is expected to lead to contribute to the further accumulation of research expertise in the two strategic areas of the team, and to contribute precious research resources (datasets, algorithm implementations, modules) to the team's repository.

Industrial exploitation plans

MKLab has recently launched a spin-out company (infalia) with the goal of transferring promising research results to the market. In particular, one of the key areas that are pertinent for the company strategic plan includes the development of sophisticated user profiling and analytics solutions.

4.6. LTU Exploitation Plan

4.6.1. Partner Profile

The Centre for Distance-spanning Technology (CDT) is competence centre within Luleå University of Technology (LTU) where industry works closely together with academia. CDT creates and develops knowledge based innovations to new business by creating and managing well integrated Research, Development and Innovation (RDI) projects based on advanced information technology that bridges distances in time and space for IT-oriented companies and entrepreneurs. The role of CDT is based on our capability to create cross-border collaboration between the university, companies and public administration (triple-helix) and together with an important group of real world end-users/testpilots which are engaged through our Living Lab Botnia (Quatro Helix).

CDT has a strong track record regarding creating spin-off companies based on knowledge based innovations. E.g. Effnet (IST Grand Prize winner 1999), Marratech (IST Grand Prize finalist 2000), Operax (IST Grand Prize finalist 2007), Oricane.

4.6.2. Individual Exploitation Strategy

Academic & research exploitation plans

In a short term perspective the project results will be used in upcoming project. Methods and tools will be developed based on the results from the project and it will be implemented into other projects. LTU-CDT also will use the results from the project into research and into our undergraduate program in Digital Service Innovation. In this education, students will use the results from the project to carry out student projects. The master program in Information Security at LTU is awarded as one of “Very High Quality” education programs in Sweden that also benefits from research within the security and privacy field and the work in USEMP. LTU recognizes research and education as an interwoven process and cutting edge security and privacy is potentially beneficial to USEMP both applied and research. Naturally, the future expectations of results also include getting scientific recognition and to do some publications as well.

One clear identified need in the user involvement research area is to develop theories, methods and tools that support user-driven innovation. The USEMP project will contribute to further development of the Living Lab concept by developing a methodology for user involvement among citizens and in open social networks. This methodology will provide valuable research on Living Lab related issues such as: how to balance different worldview among Living Lab stakeholders, how to design processes to facilitate user empowerment, how to balance and facilitate knowledge exchange among diverse stakeholders as well as between research disciplines’ interests, and how to engage and motivate end-users.

Through the multi-disciplinary, experimental, and iterative approach posed by USEMP, methodologies and tools to support the knowledge transfer will be developed and revised in accordance to the outcome of the experimental iterations. By means of this holistic approach, the approaches developed within the project will be directly applicable to users, companies, and academia aiming to experiment with future internet innovations with a user driven approach. This approach has the potential to provide the Living Lab community with an increased and validated knowledge on successful service ecosystem as well as methodologies to conduct and integrate user research into privacy research areas. This approach increases the understanding and knowledge on requirements on user devices when these are used for raising user awareness. We will learn especially about what requirements citizens have in relation to privacy in open social networks and on genres of disclosure.

Industrial exploitation plans

LTU have no industrial exploitation plans.

4.7. ICIS Exploitation Plan

4.7.1. Partner Profile

iCIS is the computer science department of the faculty of science at Radboud University. It has collaborated in a number of EU research projects and its principal investigators, such as professor Tom Heskes (Machine Learning), Professor Bart Jacobs (Digital Security) have received numerous grants and prizes. Since 2011 iCIS hosts the Chair of Smart Environments, Data Protection and the Rule of Law to integrate legal, ethical and social science perspectives in its research agenda. Since 2012 iCIS participates in the Privacy &

Identity Lab (PILab), together with SIDN - the company behind .nl, Tilburg University and TNO. The PILab develops solutions for managing online privacy and electronic identities, based on integrated research into the technical, legal and socio-economic aspects of privacy and identity.

4.7.2. Individual Exploitation Strategy

Academic & research exploitation plans

The USEMP DataBait tools present what Hildebrandt and others have coined Transparency Enhancing Tools (TETs) in the context of the EU FP6 FIDIS project, namely tools that provide transparency by counter profiling user data and sharing what profiling techniques may uncover about a user. We believe that next to PETs (privacy enhancing tools), that are based on the idea of hiding or minimisation of the processing of personal data, an economy that thrives on the emerging personal data ecosystem requires TETs, notably such as those now developed by USEMP. The Data License Agreement and the further legal requirements for the DataBait tools are preconditional for informed consent, for more participative sharing of behavioural data en more active involvement of prosumers in a data-driven economy. These requirements will be used to inform other research projects, both EU and Dutch, for instance with regards to smart grid, the sharing economy and the upcoming cyber-physical systems that nourish on behavioural data (smart city, smart home, robotics, remote healthcare). The collaboration within USEMP will be the first example of (1) TETs that deliver profile transparency without depending on the data controller providing clarity about its algorithms and (2) TETs for profile transparency that have been developed in close collaboration with legal experts.

Next to providing input for new research proposals and for assignments from private parties that wish to engage in creating added value from Big Data without taking their customers for a ride, iCIS will validate the ongoing findings of the USEMP research (1) at numerous conferences, workshops, seminars and panels (see the listings of previous dissemination activities) and (2) in scientific articles on the implementation of Data Protection by Design, responsible and sustainable data mining, and the balancing act required when IP rights threaten to limit the substance of the right to profile transparency, notably when data are processed on the basis of the so-called f-ground, being the legitimate interest of the data controller.

Industrial exploitation plans

iCIS will not engage in industrial exploitation.

4.8. Intellectual Property Management

In this section partner-specific IP that has been brought to the USEMP project are presented. The access rights to background made available to the USEMP parties is presented below:

CEA

- LIMA linguistic analyzer, including following components: tokenizer, morphological analyzer, tagging (morphosyntactic disambiguation), syntactic analyzer, named entity recognition, empty words elimination, normalization, composed words identification.
- Reformulation functional component: allowing to reformulate a word in its own language or in other languages (translation)

- Sentence alignment component: allowing to align sentences from bilingual parallel corpora for building translation memories
- Word alignment component: allows to align simple and complex words from bilingual parallel corpora for building and updating bilingual lexicons
- Document translation tool allows translating documents from one language to another one.
- Information extraction component allowing to extract entities and relation between entities.
- Relation filtering component allow to filter non relevant relations.
- Relation clustering component allowing to group together similar relations at topical and semantic level.
- Semantic relatedness allows to detect semantic similarities (synonyms, hyponyms, …) between words or phrases.
- Topic segmentation of documents allows to identify topically homogeneous excerpts
- Indexing functional component: allows to memorize some part of linguistic analysis from a document. It comprises the following software components: building of inverted files with statistical analysis, querying of inverted lists and statistical information, querying of factual information.
- Search functional component: allows textual queries and retrieval of all the related indexed documents, sorted by relevance. It comprises the following software components: comparing the results of the queries, spotting relevant words and passages.
- Image descriptor extractor: still images analyzer, generating digital descriptors (representing color, texture, shape) and semantic descriptors, based of predefined concepts (classification and ontology).
- Content-based image indexing and searching (Piria)
- Image classification: tool allowing to classify images into a predefined number of classes.
- Clustering: tool allowing to group similar images together, in order to build a descriptor-based image collection.
- Linguistic resources (automata, dictionary, grammars etc.) specific to the following languages: French, English, German, Arabic, Spanish, and used by linguistic analyzer, reformulation, sentence and word alignment components.

LTU

- Background accumulated and developed solely at Luleå University of Technology, in the disciplines of Social Informatics, within the areas of Living Lab methodologies and Needed for the implementation of the Project or Needed for the Use of a Party´s own Foreground. This includes the FormIT methodology and related tools and services founded by researchers at Luleå University of Technology, Sweden.
- References:

Ståhlbröst, A. (2008). Forming Future IT - The Living Lab Way of Involvement. Doctoral Thesis, Department of Business Administration and Social Sciences, University of Technology, Luleå.

Ståhlbröst, A, and B Bergvall-Kåreborn. (2008). FormIT - An Approach to User Involvement. In European Living Labs – A new approach for human centric regional innovation, edited by J. Schumacher and V.-P. Niitamo. Berlin: Wissenschaftlicher Verlag.

CERTH

- Topic detection Java implementations based on Soft Frequent Pattern Mining and Document-Pivot that extract important topics (represented as groups of documents and representative sets of keywords) from sets of documents (e.g. articles, tweets, etc.).
- Community detection implementation in Java that given a graph of user relations (could represent explicit connections or interactions) detects communities of users that are densely connected to each other and less connected to the rest of the network.
- Multimodal clustering Java implementation that takes into account different types of similarity between items (e.g. visual, textual, location, etc.) and learns an optimal clustering based on training examples.
- Multimedia crawler implementation (in Java) for the targeted collection of publicly available multimedia content (images/ videos) from a number of popular social networks (Twitter, YouTube, Facebook, Instagram, Flickr).
- Feature extraction Java implementation from images based on the combination SURF + VLAD, enabling compact feature representation and rapid similarity search.
- Java implementations of Product Quantization, Asymmetric Distance Computation (ADC) and Inverse Very Fast ADC for very fast similarity-based image search.
- MATLAB implementation of Approximate Laplacian Eigenmaps for detecting concepts (e.g. person, weather, sky, etc.) in images.

Furthermore, the background that is excluded from access rights is described below:

CEA

- CEA excludes the Background that was generated outside of its Vision & Content Engineering Laboratory, and not generated by researchers involved in this Project; furthermore, all Background is excluded which, due to third party rights, CEA LIST cannot grant Access Rights to.

LTU

- The project USEMP will be carried out at Luleå University of Technology by the Centre for Distance-spanning Technology in cooperation with the disciplines of Social Informatics. For the avoidance of doubt LTU hereby excludes all other Background, except for stated in Attachment 1.
- CERTH excludes the Background that was generated outside of its Multimedia Knowledge Lab (mklab.iti.gr), and not generated by researchers involved in this Project; furthermore, all Background is excluded which, due to third party rights, CERTH cannot grant Access Rights to.

Velti

- mGage Optimizer: mGage Optimizer is a set of specialized tools, multi-channel campaign optimization algorithms and advanced visualization techniques, that take into account customers demographics, service usage and personal information to improve the recommendations for services, digital content and targeting to improve the performance of mobile marketing and advertising campaigns.

- mGage product suite programming source code and algorithms: Velti mGage is a fully integrated mobile marketing and advertising platform able to create and manage all mobile marketing initiatives. Built on a modular architecture and delivered online, Velti mGage addresses the full cycle of mobile marketing and advertising, including campaign and media planning, ad serving and routing, mobile websites, marketing, CRM, analytics, and reporting, through a single end-to-end platform. Velti mGage Mobile Marketing Suite enables non-technical users to quickly create, execute, and monitor mobile marketing and advertising campaigns. A complete toolkit and storyboarding framework with more than 70 ready-to-use campaign templates speeds time-to-market for mobile campaign activities from the simplest opt-in text messaging campaign to branded mobile communities and loyalty clubs. A simple interface lets the user build interactive campaigns in minutes, test creative for optimal response, and manage short codes and key words without any carrier interaction. Each interaction type comes with its own set of tailored reports, and consumer response metrics can be fed into Velti mGage Analytics for even more comprehensive campaign performance measurement.

In the context of the USEMP project and taking into consideration the USEMP results, briefly described in the context of section 4, the USEMP platform aims at providing tools that enable OSN users to control their data and to understand how they are used by third parties. An approach is proposed that starts with the study of personal information sharing practices, coupled with a study of the complex legal framework related to this information. It proceeds with the proposal of innovative multimedia information extraction algorithms that infer new knowledge from user data and leverages insights from social and computer science developments to empower the users. As a second goal, USEMP is set to contribute to current debates concerning the way personal data are handled by OSNs and regarding the economic value of personal information and the way it is monetised. To attain its goals, USEMP proposes a multidisciplinary approach that relies on four core domains: (a) empirical user research that combines lab and living lab studies, (b) legal studies that deal with the complex legal framework related to personal data, (c) multimedia information extraction adapted to user empowerment in OSNs and (d) tools for semiautomatic user assistance in personal data sharing management.

USEMP results exploitation will be managed (i.e. joint exploitation plan, conflict management, etc.), taking into consideration the consortium agreement.

4.9. Methodology for creating Exploitation Plan

Towards an exact exploitation strategy for USEMP to be delivered at the end of the project lifetime, we include this section in order to provide a preliminary offering classification from USEMP according to the nature of the project’s exploitable results.

The approach is based on classifying the project's results according to their innovation and based on Norman's theory of innovation for technology products[19]. According to this, products are based on three categories according to their degree of innovation.

A. Products of low degree of innovation.

This category includes products with low degree of innovation that are targeting mass markets based mainly on their high-quality features and stability and not on the new services and capabilities that they offer. This market is usually saturated and high-capital and high quality of product is required in order to prevail over the competition. Price marketing and brand recognisability is also required in order to differentiate from competitors.

B. Products of medium degree of innovation.

These are products that offer a mix of quality and innovation, that are usually targeting specialist and not mass-market groups. These products offer moderate margins of profit and their success depends mainly on the marketing channels.

C. Products of high degree of innovation

These are products of high innovation that do not require stability or high quality but are based on offering features and services that no other competitor is able to offer. They require high capital spending on R&D for development, are of high risk, but offer large margins of profit and first market advantage. Appropriate marketing is also required in order to convince end users to adopt the new technology offered.

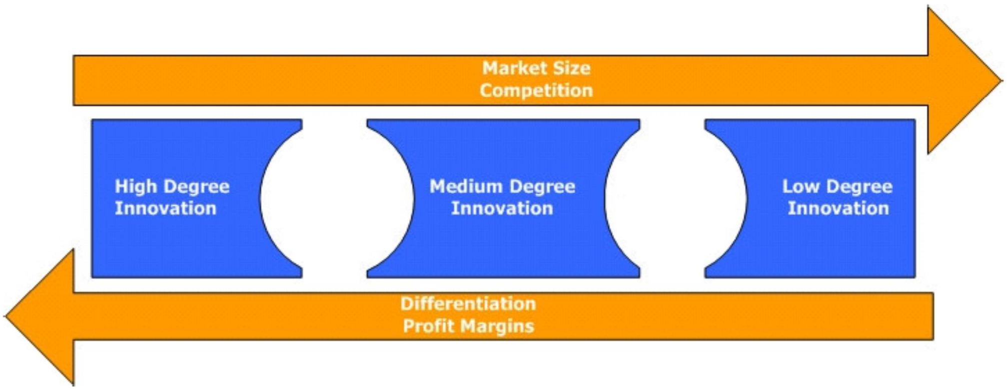

Figure 5: Market size and margins of profit based on the degree of innovation

The different market size and margins of profit based on the above classification is shown in Figure 3. The above analysis is also in line with Norman's analysis of early and late adapters and the percentage of consumers ready to adopt the offered products, as seen in the following figure.

[19] Norman, D. A. (1998), The invisible computer: Why Good Products Can Fail, the Personal Computer Is So Complex, and Information Appliances Are the Solution. Cambridge, MA: MIT Press

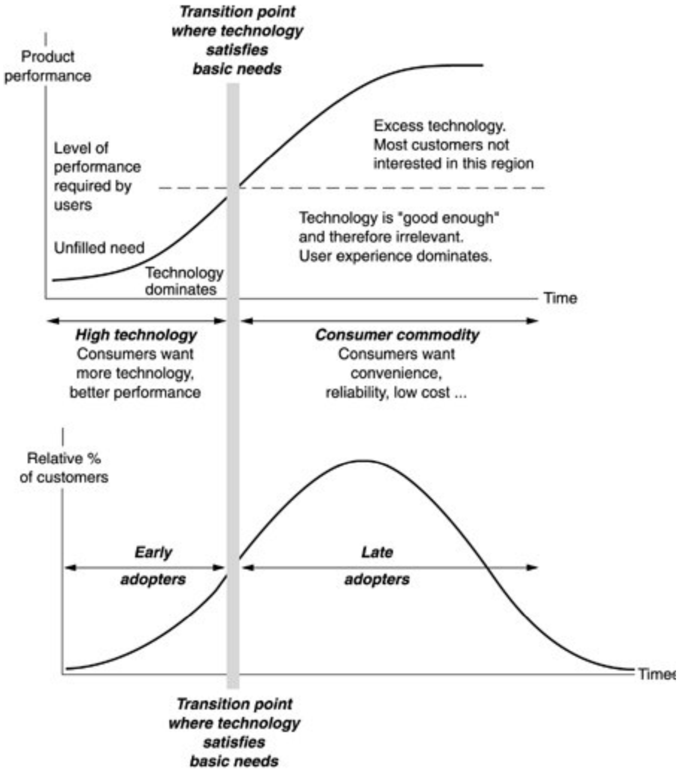
Transition point where technology satisfies basic needs
Product performance
Level of performance required by users
Unfilled need
Technology dominates
Excess technology. Most customers not interested in this region
Technology is "good enough" and therefore irrelevant. User experience dominates.
Time
High technology
Consumers want more technology, better performance
Consumer commodity
Consumers want convenience, reliability, low cost ...
Relative % of customers
Early adopters
Late adopters
Timee
Transition point where technology satisfies basic needs

Figure 6: Norman's analysis of early and late adapters

According to the above figures, typically low degree of innovation products address mostly mass market – commodity needs while high degree of innovation products are aiming mostly niche markets with special, specific needs. On top high-innovation related products need more time to mature and to be introduced compared with low-innovation related products that typically are providing solutions into existing markets and that are ready for immediate deployment[20].

[20] A typical case for the above analysis is the PDAs and SmartPhone technologies. PDAs were high innovative products aiming niche markets and it took time to be transformed into mass market products by the introduction of iPhone coupled with the support of mobile operators. http://www.zdnet.com/crash-of-the-mobile-titans-what-happened-to-palm-blackberry-nokia-and-htc-7000021189/

5. Conclusions

The scope of this report is to provide an overview of the market landscape regarding online social networks penetration in everyday life and online management. The main technology players (solutions, platforms) that are relevant to the USEMP project ecosystem have been studied:

- Privacy aware OSNs
- Privacy feedback & awareness
- Multimedia Information Extraction
- Monetisation of crowd sourced content
- Advertisement Filtering and Online advertising.

An analysis of strengths, weaknesses and identified opportunities and risks (SWOT) took place, while the business model has been presented wherever it is evident from the available sources. This analysis show that the different areas relevant for USEMP work are very active and that an increasing number of applications are dedicated to preserving users' privacy. However, existing applications make little use of multimedia and social network mining techniques in order to give users advanced insight into their shared data. In addition, from the above mentioned analysis it is obvious that innovative economic models need to be designed in order to reward not only the platforms that store or use personal data (e.g., online advertising) but also their creators. The increase of end users awareness for the usage of their personal data in conjunction with the monetary valuation of their personal data contributes towards user empowerment for enhanced online presence management.

Then, the key outcomes of the USEMP project have been highlighted. The main goal is the design of personal data management tools, which take into consideration inputs from different disciplines, such as legal research, user and living studies, multimedia information extraction and social networks analysis. According to the above analysis and based on the described profile of each partner, a brief plan is provided for each individual exploitation strategy of USEMP outcomes. Two types of exploitation plans have been considered: a) Academic and Research, b) Industrial. Moreover, partner-specific IP that has been brought to the USEMP have been described as well as the access rights to background made available to the USEMP parties. Finally, a discussion took place for the methodology that could be adopted for the creation of an exploitation plan according to the nature of the project's exploitable results: a) products of low degree of innovation, b) products of medium degree of innovation, c) products of high degree of innovation.

In the following relative deliverable (D9.5) the initial exploitation plan will be provided, while an exact exploitation strategy for USEMP will be delivered at the end of the project lifetime. In D9.5 the exploitable foreground to arise from the project will be specified. The plans for exploitation by all the partners will be provided in conjunction with specific business models from project assets.