Tilburg Institute for Law, Technology, and Society (TILT)

LL.M. Law and Technology

PRIVACY AND DATA PROTECTION IN THE LIGHT OF SMART TV TECHNOLOGY

Master Thesis

Candidate: Arda Aktan
ANR: 259019
Supervisor: Dimitra Stefanatou
Second Reader: Dr. Bryce Newell

Table of Content

ABSTRACT

The significant development of Smart TV is extremely changing consumers' online experiences through different features in house environment. In order to enjoy these features, consumers provide a variety of data such as their interests on TV programs, videos, products and services. This thesis will provide detailed information about stakeholders of Smart TVs, Smart TVs personalized services such as online behavioural advertising and its privacy related features, as called recommendation engine system, voice and facial recognition system. Additionally, this thesis will enlighten about data protection and privacy concerns arising from Smart TV features in terms of critical technical aspects and data protection principles, as called data minimization, transparency and limitation of purpose based on relevant legal research, discussions and opinions. Stakeholders of Smart TVs are obliged to take organisational and technical measures for ensuring data protection. In that regard, this thesis analyses and recommends effective mitigation methods, as called opt-in consent mechanisms, privacy by design and creating awareness of Smart TV consumers in terms of General Data Protection Regulation in EU.

Keywords: *Smart TV features, stakeholders, online behavioural advertising, privacy and data protection, privacy by design, General Data Protection Regulation*

Chapter 1: INTRODUCTION

1.1 Background

Smart TV, a television set with integrated interactive internet capabilities, is being developed as a new technology around the world. The rapid growth of high speed broadband connections is giving an opportunity to create a smart TV through delivery of content to users' devices in the house. This growth shows that smart TVs has been considerably influenced by the vogue of applications for smartphones. Smart TV is capable of providing television- e-commerce, internet browsing, online behavioural advertising, chat, and other things. Smart TVs provide navigation based on user experience which is obviously beyond of traditional broadcast systems. They enable users to find the right content as quickly and seamlessly as possible without any user's effort.[1] Smart TVs present new opportunities to consumer electronics manufacturers for product differentiation and value creation through user-driven product innovation.[2]

There is a widespread trend of connecting electronic devices particularly household goods to the Internet. First patent for Smart TV was filed in 1994 as an ''intelligent television system which linked with data processing systems by means of a digital or analog network''.[3]By the transition of television technology from analog television to digital TV in 2000s and significant improvement of this intelligent television system, TV manufacturers have officially started to demonstrate ''Smart TV'' as an alternative to traditional broadcasting system in the beginning of 2010s.[4]Smart TV Working Group established in Germany indicates that in the beginning of development of television technology, this internet based

[1] ''Smart-TV Usability: Accessing Content is Key'' by KIM FLAHERTY on 20th of September 2015 available at: https://www.nngroup.com/articles/smart-tv-usability/

[2] ''Smart TV: are they really smart in interacting with people? Understanding the interactivity of Korean Smart TV'' published by Dong-Hee Shina, YongsukHwangb and HyunseungChooc in 2013 available at: https://www.researchgate.net/publication/233271216_Smart_TV_Are_they_really_smart_in_interacting_with_people_Understanding_the_interactivity_of_Korean_Smart_TV

[3] **''**What Is a Smart TV & Do You Need One? [MakeUseOf Explains]''published by James Bruce on 9th of January 2013 available at: http://www.makeuseof.com/tag/what-is-a-smart-tv/

[4] Smart TV definition in Wikipedia available at: https://en.wikipedia.org/wiki/Smart_TV

technology was called ''Hybrid TV or ''Connected TV''. At the present time, the term ''Smart TV'' is granted to this technology and accepted by consumers and stakeholders in digital market.[5]

The most characteristic feature of Smart TV is providing opportunity to interact through the open Internet (broadband) or through a closed network, with a service provider's platform or a web site.[6]

1.1.1 Smart TV Apps and Online Services

Smart TV brings all kinds of online Apps, information and entertainment to the living room. Smart TV application is developed based on the same principles of operations as a mobile application.[7] In other words, if a consumer buys smart TV, he/she can access to the Internet and benefit from online services (such as e-commerce and online behavioural advertising) in the form of apps like in tablets and smartphones.

The features available on Smart TV allow access to popular social networking sites like Facebook and Twitter. By means of optional or embedded webcam, Smart TVs are allowing consumers to do video calling through instant calling and messaging applications such as Skype.[8] Video on Demand services, for instance Youtube for watching video clips, music videos and Netflix in which TV series and movies are mostly available on Smart TVs.[9] These specifications show that interaction between TV and consumer via Smart TV is basically the distinguishing feature in comparison with traditional TV devices.

[5] ''Market Analysis Smart TV'' published by Smart TV Working Group, p.5 available at: http://www.tv-plattform.de/images/stories/pdf/marktanalyse_smart-tv_2014_en.pdf

[6]''Challenges of Connected TV'' published by DIRECTORATE-GENERAL FOR INTERNAL POLICIES POLICY DEPARTMENT B: STRUCTURAL AND COHESION POLICIES in September 2013 p.3 available at: http://www.europarl.europa.eu/RegData/etudes/note/join/2013/513976/IPOL-CULT_NT(2013)513976(SUM01)_EN.pdf

[7]''What is Smart TV app definition?'' published by Digital Marketing Glossary on 6th of April 2015 available at: http://digitalmarketing-glossary.com/What-is-Smart-TV-app-definition

[8] ''What is a Smart TV'' written by Agent Plummer and Agent Hall published on 21 August 2015 available at: http://www.geeksquad.co.uk/articles/What-is-a-smart-tv

[9] ''What is a Smart TV'' written by Agent Plummer and Agent Hall published on 21 August 2015 available at: http://www.geeksquad.co.uk/articles/What-is-a-smart-tv

The available apps you can find for user's TV depend on the Smart TV manufacturers because they mostly provide their own app stores.[10] Particularly, by inspiration from Apple store and Google's Play Store, some TV manufacturers are following in the footsteps of modern smartphones and developing their own online stores, allowing users to download extra apps to their TVs.[11]

1.1.2 Technological Convergence of Smart TV

The term technological convergence is often defined in a very generalized and simplified terms as a process by which telecommunications, information technology and the media, sectors that originally operated largely independent of one another, are growing together. Technological convergence has both a technical and a functional side.[12] The technical side refers to the ability of any infrastructure to transport any type of data, while functional side means the consumers may be able to integrate in a seamless way the functions of computation, entertainment, and voice in a unique device able to execute a multiplicity of tasks[13].

In the light of above mentioned definition, Smart TV is an example of technological convergence which is allowing users to switch from television programs to Internet content and applications by using the same device. In this context, Smart TV users can benefit from most of the applications that are currently available on their smartphones and computers. For instance, Smart TVs make most of popular video-streaming apps on smartphones such as Netflix and Youtube available on user's television screens. Despite some minor functional distinctions, users are also capable of surfing on Internet through Smart TV compatible web browsers which are mostly embedded into Smart TV platform. However, smart remote controls make Smart TVs functions almost the same with computers functions.[14]Technological convergence of Smart TV also brings the same stakeholders such as manufacturers, application developers and third parties of smart devices together with all similar services such as personalised

[10] ''Smart TV app development: it's not rocket science, it's HTML'' published by Jukka Eklund on 28th of January 2015 available at:https://www.linkedin.com/pulse/smart-tv-app-development-its-rocket-science-html-jukka-eklund

[11] ''Smart TV app development: it's not rocket science, it's HTML'' published by Jukka Eklund on 28th of January 2015 available at:https://www.linkedin.com/pulse/smart-tv-app-development-its-rocket-science-html-jukka-eklund

[12] ''Technological convergence: Opportunities and Challenges'' published by Stelios Papadakis: https://www.itu.int/osg/spu/youngminds/2007/essays/PapadakisSteliosYM2007.pdf

[13] ''Technological convergence: Opportunities and Challenges'' published by Stelios Papadakis: https://www.itu.int/osg/spu/youngminds/2007/essays/PapadakisSteliosYM2007.pdf

[14] Samsung Forum in 2014 available at: https://www.samsungdforum.com/UxGuide/2014/03_input_method.html

services and e-commerce. Before the advent of Smart TV technology, all these services have been already offered by several manufacturers and application developers on other smart devices such as smart phones. In that sense, the following analysis will show that all data protection concerns raised from the services on other devices also emerge for Smart TV services.

1.2 Focus on Privacy and Data Protection

This thesis will focus on data protection raised by Smart TV under EU law. Smart TVs are dealing with the services associated with the plenty of personal data collected and transmitted to the manufacturer and third parties (for instance, consumer preferences, viewing habits and transactional decisions) that make a television "smart".[15]For instance, if consumers have an access to Smart TV platforms, they are likely to provide personal data such as name, address, date of birth, and sex when they register for specific services. When consumers intend to be provided online personalized services of Smart TVs, they have to agree on sharing their viewing habits and personal interests called as behavioural data with the relevant stakeholders of Smart TVs. These behavioural data are collected using cookies and recommendation engine systems, which has been subject to much debate, regulatory scrutiny and legislative activity in recent years.

1.3 Central Research Question and Sub-Questions

The central research question of this thesis is:

‘’What are the legal implications for data protection concerns raised by Smart TV, and to what extent does the General Data Protection Regulation mitigate them?’’

In order to substantiate the answer of the central research question the following sub-questions has been prepared:

1) Which are the data protection concerns especially relevant for Smart TV?

2)Which are the relevant data protection concerns for Smart TV services under the General Data Protection Regulation?

[15]‘’Samsung's Smart TVs Are Collecting And Storing Your Private Conversations’’ published by Tim Cushing on 9th of September 2015:https://www.techdirt.com/articles/20150206/04532329928/samsungs-smart-tvs-are-collecting-storing-your-private-conversations.shtml

3) Which are the possible mitigation methods for data protection concerns raised by Smart TV platform?

1.4 Significance

Today's television industry visibly changed peoples' habits in front of the television with creation of Smart TV technology on televisions. With Smart TVs, people are enabled to do nearly everything what they do on their smartphones, computers and tablets which entail collection and processing of personal data. Additionally, Smart TVs are capable of collecting and processing viewing habits and personal preferences in order to recommend customised content and advertisements in which users are interested.

According to a report by the NPD Display Search[16], within just over five years after its launch in 2007, with BBC iPlayer in the United Kingdom and Hulu in the United States, the global installed base of Smart TVs had reached approximately 104 million in 2012. In that sense, the European Commission is intent on looking into what this new technology Smart TV could mean for Europe's economic growth and innovation, cultural diversity, and consumers (especially those that may need protection.)[17] Since there is a significant development on Smart TVs over the last years and this fact also recognized by Neelie Kroes, European Commission Vice-President quoted that *"Connected TV is the next big thing in the creative and digital worlds. Convergence between sectors means people can enjoy a wider choice of great content - but it also creates disruptions and challenges. We need a converged and EU-wide debate to help deal with these changes. To help business flourish, nurture creativity and protect our values.''*[18]

On the other hand, with increasing use of Smart TV services over the last years, Smart TV users' concerns have emerged regarding what Smart TVs do with the personal data of users. The Consumer Federation of America and Consumers Union indicates that "*there is a fundamental mismatch between the technologies of tracking and targeting and consumers' ability to exercise informed judgment and control over their personal data." The information being collected online is not information that consumers*

[16]NPD DisplaySearch, Quarterly Smart TV Shipment and Forecast Report, Santa Clara, California, published on 17th of October 2012 available at:http://www.displaysearch.com/cps/rde/xchg/displaysearch/hs.xsl/121017_smart_tv_shipments_grow_worldwide_in_2012.asp

[17]''Internet on TV, TV on Internet: Commission seeks views on rapidly converging audio visual world'' European Commission Press Release, Brussels, published on 24th of April 2013 available at: http://europa.eu/rapid/press-release_IP-13-358_en.htm

[18] Idem

voluntarily share with these tracking companies or online advertising businesses.''[19]Electronic Privacy Information Center stresses that *''the world of online tracking has grown increasingly complicated and poses a great threat to consumer privacy''*[20] The enhanced online tracking systems of Smart TVs enable the relevant stakeholders to collect and process all kinds of personal data (such as biometric data, voice commands and behavioural data). For most of the cases, users don't have knowledge about who process their personal data and for what purposes stakeholders process their personal data due to lack of detailed information or consent.[21] Users do not have control over their personal data. Because most of the tools used for personalized services are invisible.[22] Based on these privacy and data protection concerns, data protection authorities around Europe demand that users are adequately informed of how and for what purposes their data will be processed, as well as exactly which data will be processed, and that prior consent is obtained in each instance.

There are obviously several discussions and analysis held by privacy professionals, private and legal entities about data protection regarding Internet of Things and smart home devices. However, the existing discussions and analysis for Smart TVs are mostly bounded by criticisms on the heels of emerged particular cases (such as Samsung and Philips Smart TV cases). Furthermore, they are generally published for informing purposes which are deprived of extensive remarks for data protection and analysis of applicability of possible mitigation methods for Smart TV services. In other words, there is no comprehensive research focused on data protection concerns raised by Smart TV features. In that regard, beside referring to the existing discussions and analysis, this thesis aims at analysing the variable roles of Smart TV stakeholders for Smart TVs intrinsic privacy related features and applicability of possible mitigation methods for ensuring data protection in line with EU Law. In the light of this purpose, this thesis can contribute to comprehensive analysis of Smart TV stakeholders and relevant parties who have concerns and interests about data protection for operations of Smart TVs. Additionally, this thesis

[19]''Online Tracking and Behavioral Profiling'' published by Electronic Privacy Information Center available at: https://epic.org/privacy/consumer/online_tracking_and_behavioral.html

[20]''Online Tracking and Behavioral Profiling'' published by Electronic Privacy Information Center available at: https://epic.org/privacy/consumer/online_tracking_and_behavioral.html

[21]''Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems'' published by Eran Toch, Yang Wang and Lorrie Faith Cranor in User Modeling and User-Adapted Interaction April 2012, Volume 22, Issue 1, pp 203-220, available at: https://link.springer.com/article/10.1007%2Fs11257-011-9110-z

[22]''Self-Regulatory Principles For Online Behavioral Advertising'' published by FTC Staff Report in February 2009 p.10 available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-on line-behavioral-advertising/p085400behavadreport.pdf

is being written at the time that General Data Protection Regulation (hereinafter referred to as ''GDPR'') in EU was agreed by three European institutions (Council of Ministers, European Commission and European Parliament), on 15th of December 2015. Therefore, this thesis also intends to contribute to the future discussions and analysis with respect to data protection for Smart TV features in the context of new regulation GDPR.

1.5 Methodology and Sources

Firstly, this thesis will identify the roles of Smart TV stakeholders pursuant to the descriptions of data controller, data processor and third parties under GDPR. Secondly, Smart TV services provided by relevant stakeholders will be analysed based on their personalized services which require the processing of personal data with the contributions of articles and publications focused on existing services of Smart TVs and the underlying reason of data protection concerns arising from implementation of Smart TV services will be analysed and discussed with the contributions of current case studies, academic literatures and research papers about personalized services offered by online service providers including Smart TV relevant stakeholders. As mentioned under the section 1.4, due to lack of extensive academic literatures and research papers focused on merely Smart TV services, academic remarks and considerations regarding online personalized services will be applied to Smart TV privacy related features. Thirdly, the provisions of GDPR which are connected with Smart TV services will be introduced and they will be applied to relevant Smart TV services provided by identified stakeholders who involved in the processing of personal data. Applying of relevant provisions will contribute to analysis of relevant services whether they are compatible with the legal requirements under GDPR and finding the relevant stakeholders who must comply with these relevant provisions under GDPR. Ultimately the possible mitigation methods for data protection concerns recommended by GDPR and relevant experts will be discussed in order to analyse the applicability of these methods in line with GDPR and Smart TVs intrinsic services.

1.6 Outline of Chapters

In the second chapter, the stakeholders of Smart TV services and its relevant features which creates data protection concerns are described and analysed. In third chapter, GDPR and its relevant provisions are introduced and analysed within the context of their applicability for Smart TV services and its

stakeholders. In the fourth chapter, possible mitigation methods for data protection recommended by experts and authorities will be introduced and evaluated. In the conclusion, the analysis of the facts revealed from the research shall be indicated and answers to the central question will be found.

CHAPTER 2: SMART TV AND DATA PROTECTION

2.1. Stakeholders

There is a diversity on stakeholders (TV Manufacturers, internet service providers, application developers, content providers, Smart TV users, third parties,) having a role with respect to the delivery of Smart TV services. In order to abide by scope of thesis, this section will examine the role of TV manufacturers, application developers and third parties who directly involve in data collecting and processing of personal data.

The identification of actors is necessary to understand who is responsible for protection of personal data based on EU Protection Law.[23] In that regard, describing of data controllers and processors based on EU Data Protection Law will contribute to find answers to who can be data processors and controllers for Smart TV services under the following sub-sections.

Pursuant to Article 4 of GDPR, data controller is ‘’*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union law or Member State law…*’’The underlined elements of definition of controller constitute the notion of concept of data controller. The first underlined element ‘’*the natural or legal person, public authority, agency or any other body*’’ determine who can act as data controller. Second underlined element defines that when the parties indicated under the first element alone or jointly determine ‘’*the purpose and means of the processing of personal data*’’, they can be considered as data controllers. Determination of purpose and means of processing is finding answers to questions like ‘’what is anticipated outcome of processing of

[23] Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor" p.4 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

personal data?'', ''which data shall be processed?'', "for how long shall they be processed?", "who shall have access to them?'' or '' when data shall data be deleted" etc. [24]

Data processor is ''a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.'' The key element of this definition is the processing ''on behalf of data controller.'' As it is understood from the definition of data processor, as long as the indicated parties process personal data on behalf of data controllers who determine purpose and means of the processing of personal data, these indicated parties can be considered as data processors.

Based on Article 4(3) of GDPR, operations for data processing can be ''*recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.''*[25]All these indicated operations will be taken into account in order to analyse if stake holders are data controller or data processor.

2.1.1. Smart TV Manufacturers

In this sub-section, it is aimed at providing clarification of Smart TV Manufacturer's roles in processing of personal databased on their Smart TV services provided by them. In the light of the given information under the section 2.1, the relationship between Smart TV features[26] and Smart TV Manufacturers will be analysed under the following paragraphs in order to find whether Smart TV Manufacturers are data controller or data processor.

It is obvious that TV manufacturers, who operate Smart TV platforms, priorly have to produce and sell their televisions to consumers and enable broadcasting services. However, as it is explained under Chapter 1, Smart TVs provide more features than mere TV broadcasting to their consumers. Article 29 Working Party point out that many Smart TV manufacturers are mostly '*collect and process personal*

[24] Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor" p.13-14 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf
[25] Article 4 of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf
[26] Smart TV features are online behavioural advertising, recommendation engine, voice and facial recognition systems herein.

data which is generated by the device, for purposes and means which they have wholly determined."[27]From this point of view, Smart TV manufacturers can be frequently considered as data controllers.

Online behavioural advertising[28] is one of the features which is service which can provided by Smart TV manufacturers to users who voluntarily receive personalized adverts on Smart TVs. In order to carry out user-targeted advertising services, Smart TV manufacturers must collect and process online behaviours of Smart TV users through like buttons, user's search preferences on web browsers or collection data from smart remote controls for gathering viewing habits. According to these findings, Smart TV Manufacturers can be considered as data controller for online behavioural advertising services on Smart TVs.

The other relevant feature of Smart TV created and mostly used as a mean of processing of personal data by Smart TV Manufacturers is Recommendation Engine system[29]. In order to recommend certain contents based on user's interests, Smart TV manufacturers collect which kind of broadcast or program users have watched, the time users have watched the broadcast or the program, as well as collecting and storing users' TV media access control (MAC) address and process the collected data. In the context of this particular service, Smart TV manufacturers act in their capacity as data controller.

The last privacy related features of Smart TV created by Smart TV Manufacturers are facial and voice recognition systems[30]. These systems are controlled by Smart TV manufacturers and capture all user's biometric data and voice commands in order to provide comfortable handling facility through specific devices embedded into televisions in favour of user's control over their Smart TVs. Additionally, the collected data through voice and facial recognition systems can also be used for recommendation of any kind of online services and content and authentication of Smart TV users. Based on the given information above, Smart TV Manufacturers determine means of processing of personal data and

[27] Article 29 Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things, p.11 available at:http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
[28] Online Behavioural Advertising is described in detail under the sub-section 2.2.2
[29] See detailed analysis under the sub-section 2.2.
[30] Facial and Voice Recognition system are described in detail under the sub-section 2.3.4

process these data for their own purposes. In that regard, they can be called as data controller for facial and voice recognition systems.

2.1.2 Application Developers

The aim of this sub-section is ascertaining whether app developers are data controllers or processors and analysing to what extent they carry out the services based on Smart TV user's personal data. Article 29 Working Party highlight that applications *''are able to collect large quantities of data from the device (location data, data stored on the device by the user and data from the different sensors) and process these in order to provide new and innovative services to the end user.''* [31] As it is described under the Chapter 1, Smart TV apps are developed by application developers and running on Smart TV platforms in order to provide their online services. Due to variety of app services, there is wide range of services provided by application developers on Smart TVs.[32] In that regard, it is quite difficult to analyse each service provided by application developers on Smart TVs individually. Therefore, the following analysis will rely on current services provided by application developers who involve in the processing of Smart TV user's personal data instead of taking into account all services which do not exist on Smart TVs however they can be compatible with Smart TV platforms.

Application developers build software compatible with Smart TV platforms and decide *''the extent to which the application will access and process the different categories of personal data in the device''*[33] In other words, they can gain access to user's data stored by Smart TV manufacturers and also allow third parties to access to user's data for their own purposes such as online behavioural advertising.[34] In the light of these information, it can be stated that as long as application developers determine the

[31]Article 29 Working Party, Opinion 2/2013 on apps on smart devices p.5 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
[32]Article 29 Working Party, Opinion 2/2013 on apps on smart devices p.4 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
[33] Article 29 Working Party, Opinion 2/2013 on apps on smart devices p.9 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
[34] Article 29 Working Party, Opinion 2/2013 on apps on smart devices p.10 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

purposes such as online behavioural advertising and means of processing of personal data, they can be called as data controller in line with GDPR.

2.1.3 Third Parties

In this sub-section, it is intended to firstly highlight what third parties perform on Smart TV platform and subsequently analyse whether third parties who involved in collecting and processing of personal data are data controllers or processors in terms of their actions for Smart TV applications.

Pursuant to Article 4(7a) of GDPR, third party is *''any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data''*[35]Based on the definition, it can be denoted that third parties can be commercial actors which is indicated by Article 29 Working Party opinion below or public authorities who are allowed to process personal data by any stakeholders on Smart TVs.

According to Article 29 Working Party, third parties can be advert network providers or analytic providers and carry out two different tasks: 1) execution of operations for the app owner such as performing analysis for applications 2) collecting ''*information from applications to supply additional services, for instance carrying out analytics figures at a larger scale (app popularity, personalized recommendation) or avoiding the display of the same advert to the same user''*.[36]For the first task, when third parties act exclusively on behalf of the app developer and process data on behalf of app developers or Smart TV Manufacturers, they can be called as data processors. [37] For the second task, third parties process personal data for their own purposes, they act as data controllers.[38]

[35] Article 4(7) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf
[36]Article 29 Working Party, Opinion 2/2013 on apps on smart devices p.13 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
[37]Article 29 Working Party, Opinion 2/2013 on apps on smart devices p.13 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
[38] Idem p.13

2.2 Privacy related features of Smart TVs

As it is highlighted under Chapter 1, there are many technical and commercial features and services carried out on Smart TVs. In this context, this section is intended to address privacy related features - online behavioural advertising through cookies and recommendation engine systems and facial and voice recognition systems as a mean of recommendation of user-targeted content and personalized advertising services and analyse implications of these features in terms of privacy and data protection concerns.

2.2.1 Profiling for Online Behavioural Advertising

This sub-section will firstly define what profiling is and address characteristics of profiling for online behavioural advertising, subsequently introduce cookies and recommendation engine system as relevant tools for online behavioural advertising and finally, discuss privacy and data protection concerns raised by profiling for online behavioural advertising.

- *Characteristics of Profiling*

Hildebrandt defines profiling as ‘’*the process of discovering correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category*’’[39]

According to GDPR, *profiling is analysis or prediction of natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement.* ’’[40]GDPR defines the scope of profiling by including analysis of performance at work, health, location, economic situation and movement of users as a profiling in broad terms. In that regard, it is important to highlight that analysis or prediction of personal preferences, interests and behaviour can be deduced as profiling

[39]‘’Defining Profiling: A New Type of Knowledge?’’ published by Mireille Hildebrandt In: Profiling the European Citizen, Cross-Disciplinary Perspectives’’ (Hildebrandt, M., Gutwirth, S., eds.), in 2008, Springer Science, p. 19

[40] Article 4(3aa) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

for online behavioural advertising based on the definition of profiling under General Data Protection Regulation.

Profiling is a significant process for the stakeholders of Smart TVs. Since the companies are capable of gaining remarkable profit by profiling for online behavioural advertising and believe that online behavioural advertising offers consumers a much better experience of online advertising.[41] On the other hand, profiling may affect privacy and data protection.[42] Under the following paragraphs, characteristics of online behavioural advertising including categorization of user's specific profiles and relevant actors are emphasized in detail.

Article 29 Working Party indicated that profiling for online behavioural advertising seeks analytic outcome from user's behavioural data such as *''repeated site visits, interactions, keywords, online content production, etc. in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests*.''[43]As it is mentioned in the opinion of Article 29 Working Party, the main purpose of one behavioural advertising is creation of user specific profiles.

- *Categorization of user specific profiles*

Recital 58a of GDPR rules that ''*profiling as such is subject to the rules of this Regulation governing processing of personal data, such as legal grounds of processing or data protection principles*.''[44]Article 29 Working Party also state that *"When a cookie contains a unique user ID, this ID is clearly personal data.*[45]The recital of GDPR and Article 29 Working Party opinion show that in case of generating of user's specific profiles which results in creation of unique user ID, these user specific profiles can be treated as

[41] ''Advertising Standards Authority'' definition of online behavioural advertising available at: https://www.asa.org.uk/Consumers/What-we-cover/Online-behavioral-advertising.aspx
[42] ''The limits of privacy in automated profiling and data mining'' published by Bart W. Schermer in Computer law & security review 27 in 2011, p.45 available at: http://ac.els-cdn.com/S0267364910001767/1-s2.0-S0267364910001767-main.pdf?_tid=bcc5d40c-e313-11e5-9192-00000aab0f27&acdnat=1457211141_fe073a0b06276960f58cc1acd6b568c9
[43] Idem p.4
[44] Recital 58a of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf
[45] Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines available at:http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf

personal data. Therefore, it is important to enlighten the types of user specific profiles under the following paragraphs.

There are two types of user specific profiles which can be generated by relevant actors of online behavioural advertising, as follows:

Predictive profiles: They are generated by analytic outcome from collection of users and collective behaviours over time. The sources of predictive profiles are visited pages and ads viewed or clicked on.[46]

Explicit profiles: They are created by user's who provide their personal data such as login credentials to the websites. [47]

- *Actors of Online Behavioural Advertising*

Advert network providers, publishers and advertisers are the relevant actors of online behavioural advertising. Their roles obviously have impact on user's data. Therefore, it is crucial to describe their roles for online behavioural advertising in order to prescribe the impact on user's information.

Article 29 Working Party precisely define the roles of actors for online behavioural advertising as follows:

''Publishers rent out space on their websites for ad networks to place adverts. They set up their web sites in a way that visitors' browsers are automatically redirected to the webpage of the ad network provider which will then send a cookie and serve tailored advertising.''[48]Based on this scenario, publishers and ad network providers agree on cooperation regarding the way of processing of user's data. In other words, they determine the means of processing of personal data. Additionally, they cooperate together for tailored advertising. In the context of these facts, both of them can be called joint data controllers.

[46]Article 29 Working Party Opinion 2/2010 on online behavioural advertising p.7 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf
[47]Article 29 Working Party Opinion 2/2010 on online behavioural advertising p.11 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf
[48]Article 29 Working Party Opinion 2/2010 on online behavioural advertising p.11 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

Advert Network Providers *''rent space from publishers' web sites to place adverts; they set and/read cookie related information and, in most cases, collect the IP address and possible other data that the browser may reveal. Further, the ad network providers use the information gathered on Internet users' surfing behaviour to build profiles and to select and deliver the ads to be displayed on the basis of this profile.*[49]In other words, Advert network providers collect relevant data and subsequently analyse them in order to generate specific user profile and place relevant adverts in compliance with user's interests and actions. On the basis of their role, they determine the purpose and means of processing of personal data for their own purposes, as a data controller.

Data subject clicks through on an ad and visits the advertisers' website, the advertiser can track which campaign resulted in the click-through. If the advertiser captures the targeting information (e.g. certain demographic data such as "young mothers" or an interest group such as "extreme sports fan") and combines it with the data subject's onsite surfing behaviour or registration data.[50]In the context of this definition, advertisers collect targeting information and seek analytic outcome from user's actions in order to reveal user's interest and preferences related to advertisers' products and services. Briefly, they act as a data controller in terms of European Data Protection Law.

2.2.1.1 Profiling through Cookies

Smart TVs contain many web applications and different types of web browsers. Smart TV users are enabled to use and benefit from these applications and visit websites through these web browsers such as Mozilla Firefox and Opera generally embedded into Smart TV platforms. This sub-section is intended to enlighten implications of cookies on web sites in the context of online behavioural advertising.

- *Characteristics of cookies*

European Commission describe cookies as ''*a small piece of data that a website asks browser to store on the computer or mobile device. The cookie allows the website to "remember" user's actions or*

[49] Idem, p.10
[50] Idem, p.12

preferences over time.''[51]If this description applies to Smart TVs, the mentioned browser on Smart TV store that ''small piece of data'' on Smart TV devices.

The favoured monitoring instrument for online behavioural advertising companies are cookies. Because cookies allow advert network providers and advertisers to generate user-specific profile for user-specific advertising. [52]

There are two types of cookies - first part cookies and third party cookies - which are mostly used by online behavioural advertising companies.[53]Third party cookie is sent to users by advert network providers that do not operate the website visited by the users. First party cookie is used on the website of advertisers or publishers operating the website visited by the user.[54]

As indicated under the section 2.2.2, profiling is subject to legal grounds for processing of personal data and there are legal requirements for use of cookies such as user's consent for cookies and transparency for processing of personal data through cookies. Consent for cookies in compliance with EU Data Protection Law are described and analysed under Chapter 3.

2.2.1.2 Profiling through Recommendation Engine System

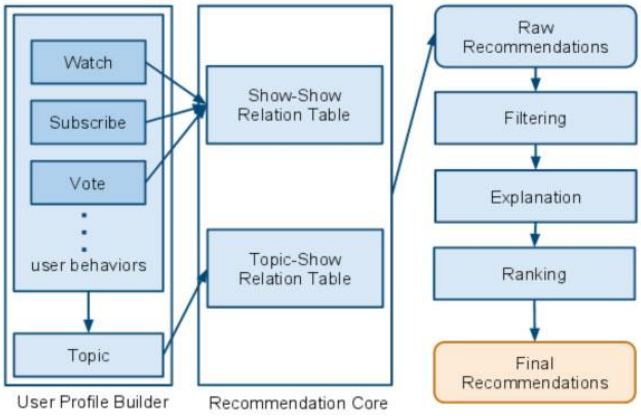
This sub-section describes recommendation engine which process personal data of users in order to create user-specific profile and analyse its implications in the context of online behavioural advertising.

Recommendation engine systems can be defined as a tool ''*which attempt to recommend the most suitable items (products or services) to particular users (individuals or businesses) by predicting a user's interest in an item based on related information about the items, the users and the interactions between items and users.*''[55]It is important feature of Smart TVs used by Smart TV Manufacturers and capable of

[51] European Commission – Information Provider's Guide – The EU Internet Handbook available at: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm
[52]Article 29 Working Party Opinion 2/2010 on online behavioural advertising p.6 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf
[53]Article 29 Working Party Opinion 2/2010 on online behavioural advertising p.5 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf
[54] Article 29 Working Party, Opinion 04/2012 on Cookie Consent Exemption, p.5 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf
[55]''Recommender System Application Developments: A Survey'' -Faculty of Engineering and Information Technology, University of Technology Sydney, Australia – published by Jie Lu, Dianshuang Wu, Mingsong Mao,

providing customized recommendations for their users and providing customized advertisements based on its statistical outcome(Figure 1).[56]Profiling on content of TV programs and videos through recommendation engine is distinctive feature in comparison with profiling through cookies. On the other hand, both cookies and recommendation engine systems can serve as means for the provisioning of online behavioural advertising services.

Figure 1- Architecture of Hulu Recommendation System[57]



Recommendation Engine Systems on Smart TVs collect many sort of information, as follows[58]:

- Information about content watched, purchased, downloaded, or streamed through Samsung applications on Smart TV or other devices;
- Information about applications which have been accessed through the Smart TV panels;
- Information about clicks on the "Like," "Dislike," "Watch Now," and other buttons on Smart TV;
- The query terms entered into Smart TV search features, including when search for particular video content; and

Wei Wang, Guangquan Zhang p.1 available at: http://www.uts.edu.au/sites/default/files/desi-publication-recommender%20system%20application%20developments%20a%20survey-accepted%20menuscript.pdf

[56] ''LG Smart TV - Voice Recognition and Content Discovery'' published by John Archer on 26th of June 2013 available at: http://www.trustedreviews.com/lg-smart-tv-review-voice-recognition-and-recommendations-page-2

[57] ''Hulu's Recommendation System'' published by Liang Xiang on 19th of September 2011 available at: http://tech.hulu.com/blog/2011/09/19/recommendation-system/

[58]Samsung Global Privacy Policy - SmartTV Supplement available at: http://www.samsung.com/uk/info/privacy-SmartTV.html

The collected data mentioned above can be deemed as mere user's preferences. However, as explained in the beginning of this sub-section, recommendation engine systems use this information in order to recommend customized TV programs or adverts.

2.2.1.3 Concerns about Profiling

So far, relevant operations for profiling preferred by Smart TV stakeholders have been described. As it can be understood that profiling for online behavioural advertising may provide advantages for relevant stakeholders and profiled users who voluntarily request this service. However, despite the fact that Smart TV users voluntarily provide all their personal preferences and interests, users can encounter privacy and data protection breaches, for example in case that the provided information are processed incompatible with the purpose of the service or Smart TV users are not informed about the extent of processing or transfer of these processed information to third parties.[59]In that regard, it should be denoted that there is a need for transparency of operations and the purposes of relevant stakeholders which is important key condition in order to achieve well-informed decisions of users.[60]Maglena Kuneva, the Commissioner for Consumer Affairs of the EU, has criticized that some advertisers are operating contrary to the consumer rights in terms of transparency, control and risk through data collection and behavioural targeting.[61]Gutwirth and Hildebrandt also argue that '*profiling tend to remain opaque, incomprehensible and evasive*''.[62] The opacity of profiling and pervasiveness of instruments used for

[59]''Internet and Wireless Privacy: A Legal Guide to Global Business Practices'' published by Eloise Gratton in 2003, p.7 available at: https://books.google.com.tr/books?id=IjKRjVzQtOIC&printsec=frontcover&dq=Internet+and+Wireless+Privacy:+A+Legal+Guide+to+Global+Business+Practices&hl=en&sa=X&ved=0ahUKEwj83oLB2eHLAhWIIJoKHZ1-AF0Q6AEIJDAA#v=onepage&q=Internet%20and%20Wireless%20Privacy%3A%20A%20Legal%20Guide%20to%20Global%20Business%20Practices&f=false

[60]''Big Data and smart devices and their impact on privacy'' published by DIRECTORATE GENERAL FOR INTERNAL POLICIES POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS published in September 2015, p.20-21 available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf

[61]''EU issues ultimatum on internet privacy behavioral targeting investigated'' published by Christopher Williams on 31st of March 2009available at: http://www.theregister.co.uk/2009/03/31/kuneva_behavioural/

[62]''Some Caveats on Profiling'' edited by Serge Gutwirth and Mireille Hildebrandt in the book Data Protection in a Profiled World published by Serge Gutwirth, Yves Poullet, Paul de Hert in 2010, p.39 available at:http://www.newbooks-services.de/mediafiles/texts/2/9789048188642_excerpt_001.pdf

profiling directly influences the ability of users to know how data collected about them is used.[63] Based on these considerations, this sub-section will focus on analysis of the underlying reason of these concerns.

- *Lack of transparency, consent and knowledge about profiling*

There are several legal concerns about profiling for online behavioural advertising. First of all, created user profiles are collected and processed without user's knowledge or consent. ''[64]In other words, they don't know how the relevant stakeholders use their profiles and what the likely consequences are about profiling.[65]Secondly, these created user profiles are mostly ''*invisible and uncontrollable for*'' users.[66]

Invisibility and lack of control of online behavioural advertising processes are one of the main concerns for users. For instance, as indicated under the sub-section 2.2.2.1, small piece of data (cookies) is stored on the television databases. It is obviously not easy for users to access to these data on television databases and control over it. The same concerns also exist for recommendation engine systems. Even though, TV Manufacturers inform about what the purpose and scope of collected personal data and request for consent on data processing, users don't have knowledge to what extent online behavioural advertising services can affect them. These facts show that there is a necessity to establish more control over processing of personal data for Smart TV users and transparency of functions of cookies and

[63] ''Big Data and smart devices and their impact on privacy'' published by DIRECTORATE GENERAL FOR INTERNAL POLICIES POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS published in September 2015, p.11-12 available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf

[64] Article 29 Working Party, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation'' adopted on 13th of May 2013 p.2 available at:http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf

[65] ''Some Caveats on Profiling'' edited by Serge Gutwirth and Mireille Hildebrandt in the book Data Protection in a Profiled World published by Serge Gutwirth, Yves Poullet, Paul de Hert in 2010, p.36 available at:http://www.newbooks-services.de/mediafiles/texts/2/9789048188642_excerpt_001.pdf

[66] ''Some Caveats on Profiling'' edited by Serge Gutwirth and Mireille Hildebrandt in the book Data Protection in a Profiled World published by Serge Gutwirth, Yves Poullet, Paul de Hert in 2010, p.36 available at:http://www.newbooks-services.de/mediafiles/texts/2/9789048188642_excerpt_001.pdf

recommendation engine systems at a reasonable degree, despite of the pressure of necessity of big amount of data on the ability of users to control processing of their personal data.[67]

Violation of TP Vision (a Philips Smart TV manufacturer) is considerable case regarding the concerns about lack of consent and transparency of profiling. ''*Smart TV TP Vision collects data in relation to user habits such as: when users watch TV; their favourite programmes and apps; which programmes are being recorded; which videos are being rented; and which shows they view on-demand''.*[68]They offer personalized viewing recommendations and user-specific advertisement services. Dutch Data Protection Authority found out that ''*there is a lack of clear and accessible information concerning the processing of personal data and lack of viewer's valid consent for data collection and processing.''*[69]Due to any reason, TP vision apparently underestimated the legal requirements for profiling whilst they focused on providing viewing recommendations and advertisements for increasing their income.

Beside Philips Smart TV's shortcomings regarding legal grounds for processing of personal data, this case can be deemed as example of a reason why users have concerns despite of existence of legal requirements related to profiling for online behavioural advertising. In that regard, ''*policy makers, lawyers and computer scientists should join forces to explore the possibility of a new legal approach of profiling, focusing on anticipating how the emerging socio-technical infrastructure could articulate legal norms.''*[70]

- *Security Concerns about Profiling*

[67]''Big Data and smart devices and their impact on privacy'' published by DIRECTORATE GENERAL FOR INTERNAL POLICIES POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS published in September 2015, p.22 available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf

[68]''Netherlands Smart TV's in Breach of Dutch Data Protection Act'' published by Rade Obradović in 2013 available at: http://merlin.obs.coe.int/iris/2013/9/article21.en.html

[69] ''Collecting personal data via smart TVs violates Dutch Data Protection Act'' published by Friederike van der Jagt on 7th of February 2014 available at: http://www.lexology.com/library/detail.aspx?g=dd89be0a-bdf0-41ad-962b-84a0abbdb0d5

[70]''Some Caveats on Profiling'' edited by Serge Gutwirth and Mireille Hildebrandt in the book Data Protection in a Profiled World published by Serge Gutwirth, Yves Poullet, Paul de Hert in 2010, p.37-38 available at:http://www.newbooks-services.de/mediafiles/texts/2/9789048188642_excerpt_001.pdf

With the increase of the value of profiling, potential security risks are also being questioned such as that could be exploited to harm consumers by: (1) unauthorized access and misuse of personal data; (2) possible attacks on Smart TV platform and its relevant services.[71]

Some critics pointed out that ''*there is the direct risk that someone will learn information that the user wished to keep private. For example, revealing identifying information could lead to identity theft. There are also risks of finding a personal information about a user in one system that could identify the user in another system. The users may not have expected others to be able to "connect" their identities from the two systems''.*[72]These statements obviously emphasize that there is a lack of control over user profiles due to accessibility of different systems used for the same or different purposes. It seems that the main problem is lack of sufficient information why personal data of users are accessible in different systems. As such, informed decisions of user's may be affected due to lack of information in question.

- *Surveillance of Users by Governments*

Disclosure of created profiles by data controllers of Smart TV services in order to facilitate criminal investigations and law enforcements is discussed briefly in this section. Because this thesis particularly focuses on privacy and data protection concerns raised by commercial stakeholders' services on Smart TVs. Therefore, further details and discussions regarding surveillance by governments will not be analysed in the following Chapters.

One of the biggest risks of tracking is global surveillance by governments.[73]Governments are willing to access to all collected information including user profiles in order to proceed criminal investigations. There are currently discussions about whether law enforcement agencies must request ''*user information, the dates and times the subscriber contacted other users, the length of such*

[71] Report of ''The Internet of Things: Privacy and Security in a Connected World'' Workshop hosted by FTC on 19 November 2013 p.2

[72]Idem

[73] ''Privacy considerations of online behavioural tracking'' published by ENISA on 14th of November 2012, p.13 available at: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking

communications, the location of the user, etc.''[74]With respect to the surveillance of users, Apple CEO represented a considerable statement and admitted that ''*US government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.*''[75]

2.2.2 Gesture, Facial and Voice Recognition

This sub-section will enlighten and analyse gesture, facial and voice recognition systems on Smart TVs based on their relationship with user's biometric data and voice commands.

Most of high-tech television manufacturers have recently introduced the growing technology gesture, facial and voice recognition on Smart TVs, which enable the users to access to Smart TVs online services. In other words, within the capability of this technology in question, the televisions are able to listen and record what user say and their movements in front of it.[76]On the other hand, according to Article 29 Working Party, all these data can be deemed as personal data.[77] Particularly, biometric data is described under the Article 4(11) of GDPR, as ''*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data*'' In that regard, Smart TV Manufacturers should comply with data protection principles for processing of biometric data. In other words, the application of gesture and facial recognition technology to an individual's facial

[74]''Encryption Needn't Be An Either/Or Choice Between Privacy and National Security'' published by John Chen - Executive Chairman and CEO at BlackBerry on 21th of January 2015 available at: https://www.linkedin.com/pulse/you-can-balance-privacy-national-security-heres-how-john-chen?trkInfo=VSRPsearchId%3A1283793021455802136676%2CVSRPtargetId%3A5963629768090931200%2CVSRPcmpt%3Aprimary&trk=vsrp_influencer_content_res_name

[75] ''A Message to Our Customers'' published by Tim Cook on 16th of February 2016 available at: http://www.apple.com/customer-letter/

[76]''Why George Orwell would never buy a Smart TV by Samsung'' published by KHADIJA KHAN on 16th of February 2015, available at:http://www.theplaidzebra.com/george-orwell-never-buy-smarttv-samsung/

[77] Article 29 Working Party Opinion 3/2012 on developments in biometric technologies, p. 15 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

image constitutes processing of personal data and, therefore, can only take place if a legal justification exists.[78]

These technical innovations that are very often presented as technologies that only improve the user experience and convenience of applications could lead to loss of user's privacy if no adequate safeguards are implemented.[79]When these technologies are taken into account from the point of user's privacy, the risk is arising from ability of these technologies which can record users in their *''physical surroundings''* such as home environment.[80]These innovative technologies are *''ubiquitous and practically invisible''* which obviously lead to user's control over the operations of these technologies more difficult.[81]Because they can record all information regardless of user's intent, unless Smart TV manufacturers take technical and security measures in order to avoid such unexpected, perpetual and excessive recording of user's physical information. Loss of control obviously arises from autonomy of these technologies given by their designers in order to make these technologies capable of making automated decisions.[82]As such, the capability of these technology technologies lead to revealing of more complex and detailed user profiles and lack of detailed information about the nature of these

[78] ''Say cheese! Privacy and facial recognition'' published by Ben Buckley, Matt Hunter (Linklaters LLP) in 2011 p.3 available at: http://ac.els-cdn.com/S0267364911001567/1-s2.0-S0267364911001567-main.pdf?_tid=68f7016e-c047-11e5-90ba-00000aab0f26&acdnat=1453385044_fef44766d048fa3280d5a93155753cb9

[79] Article 29 Working Party Opinion 3/2012 on developments in biometric technologies, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

[80] ''The Convergence of Virtual Reality and Social Networks – Threats to Privacy and Autonomy'' published by O'Brolcháin, Fiachra; Jacquemard, Tim; Monaghan, David; O'Connor, Noel; Novitzky, Peter; Gordijn, Bert in Science & Engineering Ethics ;Feb 2016, Vol. 22 Issue 1 , in February 2016, p.5 available at: http://connection.ebscohost.com/c/articles/112358475/convergence-virtual-reality-social-networks-threats-privacy-autonomy

[81] ''The Convergence of Virtual Reality and Social Networks – Threats to Privacy and Autonomy'' published by O'Brolcháin, Fiachra; Jacquemard, Tim; Monaghan, David; O'Connor, Noel; Novitzky, Peter; Gordijn, Bert in Science & Engineering Ethics ;Feb 2016, Vol. 22 Issue 1 , in February 2016, p.5 available at: http://connection.ebscohost.com/c/articles/112358475/convergence-virtual-reality-social-networks-threats-privacy-autonomy

[82] ''IoT Privacy, Data Protection, Information Security'' published by European Commission available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753

technologies and security measures create uncertainties whether organizational and technical measures based on this data variety outweigh privacy and data protection risks.[83]

Example of Smart TV Privacy Policy[84] provided useful details about the implications of the technology pursuant to privacy protection concerns above:

Voice Recognition: You can control your Smart TV, and use many of its features, with voice commands. If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some interactive voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service provider (currently, Nuance Communications, Inc.) that converts your interactive voice commands to text and to the extent necessary to provide the Voice Recognition features to you. **Gesture Controls and Facial Recognition:** Your Smart TV is equipped with a camera that enables certain advanced features, including the ability to control and interact with your TV with	gestures and to use facial recognition technology to authenticate your Samsung Account on your TV. The camera can be covered and disabled at any time, but be aware that these advanced services will not be available if the camera is disabled. **Facial Recognition:** The camera situated on the Smart TV also enables you to authenticate your Samsung Account or to log into certain services using facial recognition technology. You can use facial recognition instead of, or as a supplementary security measure in addition to, manually inputting your password. Once you complete the steps required to set up facial recognition, an image of your face is stored locally on your TV; it is not transmitted to Samsung

2.2.2.1 Gesture and Facial recognition

This sub-section will introduce specific features of gesture and facial recognition systems and inform about how user's gestures and their biometric data are treated by facial and gesture recognition systems.

New developments in facial and gesture recognition applications are increasing in their accuracy and the scope of their use. Facial recognition technology has been primarily used for crime prevention,

[83] ''Internet of Things IoT Governance, Privacy and Security Issues'' published by EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS in January 2015 p.18 available at: http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf

[84] ''Samsung Global Privacy Policy – Smart TV Supplement'' available at: http://www.samsung.com/uk/info/privacy-SmartTV.html

detection and enforcement.[85] It has also been used for law enforcement purposes in Europe.[86]Nowadays, they are also used for providing advanced features in digital market.

According to Samsung Smart TV Privacy Policy, gesture recognition system uses a camera which is capable of providing certain advanced features on Smart TVs and additionally, it provides handling facility to control and interact with Smart TV through user's gestures. Facial recognition system can be used as a unique identifier for authentication of a Smart TV account. Particularly, 3D facial recognition software allows comprehensive collection of distinctive features on the surface of a face, such as the contours of the eye sockets, cheekbones, nose, and chin.[87] Such applications have the advantage of the identification of faces from a variety of angles, including a profile view.[88]

Al Franken represents *''There is nothing inherently right or wrong with facial recognition technology.''*[89]However, facial recognition systems can be a big threat against user's privacy, unless they are used within the framework of privacy and data protection law.[90]Ann Cavoukian emphasizes that the possible threats are misuse, lost or theft of facial images or other *''biometric representations of our*

[85]''Oops- We didn't mean to do that-How Unintented consequences can hijack good privacy and security policies'' published by Thomas P. Kenan in August 2010 under ''Privacy and Identity Management for Life'' edited by Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes, Ge Zhang p.114 availableat:https://books.google.nl/books?id=kJk30cDn_sC&pg=PA107&lpg=PA107&dq=Hildebrandt,+M.+(2009).+Profiling+and+AmI.+In+The+Future+of+Identity+in+the+Information&source=bl&ots=T62UypGWZr&sig=_UHEwad4j0EoK2HxOGBJhf8Uk&hl=en&sa=X&ved=0ahUKEwiXh8ac0fnKAhWFhhoKHW6B40Q6AEIMDAE#v=onepage&q=Hildebrandt%2C%20M.%20(2009).%20Profiling%20and%20AmI.%20In%20The%20Future%20of%20Identity%20in%20the%20Information&f=false

[86] ''Say cheese! Privacy and facial recognition'' published by Ben Buckley, Matt Hunter (Linklaters LLP) in 2011 p.1 available at: http://ac.els-cdn.com/S0267364911001567/1-s2.0-S0267364911001567-main.pdf?_tid=68f7016e-c047-11e5-90ba-00000aab0f26&acdnat=1453385044_fef44766d048fa3280d5a93155753cb9

[87] ''Say cheese! Privacy and facial recognition'' published by Ben Buckley, Matt Hunter (Linklaters LLP) in 2011 p.3 available at: http://ac.els-cdn.com/S0267364911001567/1-s2.0-S0267364911001567-main.pdf?_tid=68f7016e-c047-11e5-90ba-00000aab0f26&acdnat=1453385044_fef44766d048fa3280d5a93155753cb9

[88] ''Say cheese! Privacy and facial recognition'' published by Ben Buckley, Matt Hunter (Linklaters LLP) in 2011 p.3 available at: http://ac.els-cdn.com/S0267364911001567/1-s2.0-S0267364911001567-main.pdf?_tid=68f7016e-c047-11e5-90ba-00000aab0f26&acdnat=1453385044_fef44766d048fa3280d5a93155753cb9

[89]''Hearing Minutes Before the Subcommittee On Privacy Technology and The Law of The Committee On The Judiciary United States Senate'' - Opening Statement Of Hon. Al Franken, A U.S. Senator From The State Of Minnesota, p.1 available at:https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf

[90] ''Hearing Minutes Before the Subcommittee On Privacy Technology and The Law of The Committee On The Judiciary United States Senate'' - Opening Statement Of Hon. Al Franken, A U.S. Senator From The State Of Minnesota, p.1 available at:https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf

bodies which are reflection of our identities''.[91] Additionally, there are also other possible negative effects such as ''*leading to unauthorized matching, tracking, impersonation and other deceptive practices*.''[92] Whilst these systems provide better experiences to users in terms of access to a wide variety of media content, these systems may undermine the control of the user over the processing of their personal data.[93] In a nutshell, if these technologies are fairly used without causing any possible privacy risks mentioned in the above paragraph, there is no reason to avoid application of these technologies on Smart TVs.

2.2.2.2 Voice Recognition

Voice recognition system is not a new technology offered by Smart TVs. [94] Apple, Google and Amazon have currently provided this service by the names Siri, OK Google and Alexa.[95]This sub-section will introduce specific features of voice recognition system on Smart TVs and inform about how voice biometrics are treated by voice recognition systems.

Voice recognition is defined as ''*Through enabling the voice recognition feature, users can establish interaction with their Smart TVs using their voices. In order to provide voice recognition feature, their voices are transmitted (along with information about user device, including device identifiers) to service provider converting voice commands to the necessary format which is necessary for Voice Recognition''*.[96]Based on this definition, voice commands can be deemed as personal data, as long as they are combined with unique identifiers such as IP address or device identifiers.

---

[91] ''Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment'' published by Cavoukian, A., Chibba, M., &Stoianov, A. - Review Of Policy Research29(1) p.1 in 2012

[92] ''Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment'' published by Cavoukian, A., Chibba, M., &Stoianov, A. - Review Of Policy Research29(1) p.1 in 2012

[93] ''Threat Landscape and Good Practice Guide for Smart Home and Converged Media'' published by ENISA on 1st of December 2014, p.7 available at: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-for-smart-home-and-media-convergence

[94]''Samsung rejects concern over 'Orwellian' privacy policy'' published by Alex Hern on 9th of February 2015 available at: http://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy

[95]''Samsung rejects concern over 'Orwellian' privacy policy'' published by Alex Hern on 9th of February 2015 available at:http://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy

[96]''Samsung Global Privacy Policy – SmartTV Supplement'' available at: http://www.samsung.com/uk/info/privacy-SmartTV.html

The issue of voice recognition in relation to Smart TV was addressed in a case brought by US consumer rights organisation the Electronic Privacy Information Center (''Epic'') before Federal Trade Commission (''FTC'').[97]They complained that "*Samsung routinely intercepts and records the private communications of consumers in their homes. Consumers who have learned of this practice have described it is as both "unfair" and "deceptive"*[98]

Subsequently, Federal Trade Commission started an investigation regarding the accusation of Epic against Samsung. Samsung ignored the accusation of Epic that *''Epic are not correct and do not reflect the actual features of our Smart TV. Samsung takes consumer privacy very seriously and our products are designed with privacy in mind.''*[99]Additionally, Samsung provided very questionable advice for their customers about the voice recognition feature that *''be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition*.''[100]That is to say, Samsung suggests that their consumers don't talk about private issues in front of their TVs and they will keep recording all conversations of users. Such a case absolutely creates big concerns among users what Smart TV manufacturers do with their personal data. This is obviously a clear example of loss of user's control over the personal data. They were not aware of such an unnecessary processing of personal data. This case will also be discussed in detail under Chapter 3 based on GDPR's data minimisation principles.

CHAPTER 3: ANALYSIS OF GENERAL DATA PROTECTION REGULATION

3.1 Privacy and Data Protection in Europe

[97] ''Samsung's voice-recording smart TVs breach privacy law, campaigners claim'' composed by Samuel Gibbs and published in the Guardian on 27 February 2015 available at: http://www.theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim

[98]''Samsung's voice-recording smart TVs breach privacy law, campaigners claim'' composed by Samuel Gibbs and published in the Guardian on 27 February 2015 available at: http://www.theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim

[99] Idem.

[100]''Disable this feature to stop your Samsung Smart TV from listening to you'' published by Dan Graziano on 10th of February 2015 available at: http://www.cnet.com/how-to/samsung-smart-tv-spying/

This section takes into account general aspects of the GDPR and gives brief information about the replacement of Data Protection Directive by GDPR. The specific provisions challenged by Smart TV services are analysed based on GDPR in the following sections.

With the technical developments which involve high risk for privacy of individuals (such as profiling and illegitimate data processing) and several cases (such as Edward Snowden Leak[101] and Smart TVs - TPVision- lack of consent, clear and accessible information[102]), adoption of new strong data protection rules has become a primary necessity for EU Member States.[103]

Subject to this necessity, in 2012, European Commission released a draft regulation which aims to strengthen privacy of EU Citizens and Digital Economy.[104]After the trilogue discussions[105] between three institutions (Council of Ministers, European Commission and European Parliament), on 15th December 2015, the EU Commission, Parliament and Council of Ministers agreed on the GDPR. It will come into force two years from date of publication.[106]

3.2 Specification of purpose for processing of personal data

As mentioned in previous Chapters, Smart TVs collect big data a variety of personal data through various tools (such as cookies, recommendation engine systems, facial and voice recognition systems) and retain these data for their different types of services. There are also some concerns about the lack of clear and specified purposes for collection of personal data and generation of user-specific profiles in order to provide personalized services. As it is indicated by Article 29 Working Party, ''*specification of*

[101]Snowden was hired by Booz Allen Hamilton, an NSA contractor, in 2013 after previous employment with Dell and the CIA.On May 20, 2013, Snowden flew to Hong Kong after leaving his job at an NSA facility in Hawaii and in early June he revealed thousands of classified NSA documents to journalists Glenn Greenwald, Laura Poitras and Ewen MacAskil available at: https://en.wikipedia.org/wiki/Edward_Snowden

[102]''Smart TV's in Breach of Dutch Data Protection Act'' published by Rade Obradović Institute for Information Law (IViR), University of Amsterdam available at: http://merlin.obs.coe.int/iris/2013/9/article21.en.html

[103]Chairman of WP29, Jacob Kohnstamm's statement on 25th of January 2012 available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2012/20120125_pr_dp_proposals_en.pdf

[104] European Commission press release on 25 January 2012 related to comprehensive reform of the data protection rules available at:http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[105] ''General Data Protection Regulation: Document pool'' https://edri.org/gdpr-document-pool/

[106] European Commission press release on 15 December 2015 on agreement on ''Commission's EU data protection reform will boost Digital Single Market'' available at: http://europa.eu/rapid/press-release_IP-15-6321_en.htm

purpose is an essential first step in applying data protection laws and designing data protection safeguards for any processing operation.''[107]Because specification of purpose of processing contributes to other principles of data protection law regulated under GDPR.

Due to these above mentioned considerations, this section will analyse how stakeholders of Smart TVs must specify the purpose for processing of personal data under GDPR in connection with privacy and data protection concerns arising from Smart TVs services.

Specification of purpose of processing of personal data is regulated under Article 5(b) of GDR.[108] In compliance with Article 5 (b) of GDPR[109]*, data* controllers of Smart TV services must ensure that personal data are *''processed for* ***specified, explicit and legitimate purposes and not further processed in away incompatible with those purposes****; further processing of personal data for archiving purposes in the public interest*, *or scientific and historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes''*

The terms ***''specified, explicit and legitimate''*** are the essential required conditions for processing of personal data for the Smart TV services described in Chapter 2. Therefore, it will be useful to clarify these terms below and their connections with the other data protection principles described under this Chapter.

''Specified and explicit purpose'' means detailed and clear determination of purpose of processing. The specified and explicit purpose must be provided for informed consent which is legal grounds of processing of personal data under Article 4(8). It can be noted that there is a link between requirements for specific purpose of processing of personal data and informed consent as a legal ground for processing of personal data. In that regard, specified and explicit purpose of processing can be interpreted as a pre-requisite for informed consent of users for Smart TVs personalized services. As long as data controllers determine specifically and explicitly the purpose of the processing of personal data,

[107]Article 29 Working Party, Opinion 3/2003 on purpose limitation p.4 available at: http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf
[108] Article 5(b) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf
[109] Article 5(b) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

they can request the consent of data subjects for specified and explicit purpose. Because data subjects must be informed about the purpose of the processing of personal data in order to take informed decision about the processing of their personal data.

The underlying reason of requirement of ***''legitimate''*** process in Article 5(b) is that interests of stakeholders, which provide personalized services, must be legitimate on processing of personal data provided that those interests are not overridden by the fundamental rights and freedoms of the individual. [110]

The expression '' ***not further processed in away incompatible with those purposes'' rules that*** GDPR allows data controllers of Smart TV services to further process of personal data of users provided that the further processing is compatible with the specified purpose determined by data controllers of Smart TV services. In other words, automated processing of personal data for profiling is allowed under GDPR provided that the automated further processing for profiling is compatible with the purpose determined by data controllers of personal data. In case, personal data are further processes for a secondary purpose, data controllers of Smart TV services cannot rely on the previous specified purpose in order to further process of personal data.

As it is indicated under Chapter 2, the main concern about profiling for online behavioural advertising is the relevant stakeholders collect personal data of users and generate profiles without any knowledge or consent of users. The concern is arising from lack of stakeholder's necessary actions or wilful negligence regarding specification of purpose of profiling. When the TPVision case referred in Chapter 2 is examined, TPVision didn't determine the purpose of processing of personal data. Most likely, due to lack of specified and explicit purpose of processing, they didn't request their user's consent for profiling either.

Conversely, there is also contribution to specification of purpose from other principle, as called ''data minimization'' which is introduced under Article 5(c) of GDPR. EDPS points out that pursuant to data minimization principle, data controllers may retain the data only for as long as is necessary to fulfil

[110] Article 29 Working Party, Opinion 3/2003 on purpose limitation p.4 available at: http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf

specific purpose.[111]In other words, data minimization is a pre-condition for limitation of purpose. Article 29 Working Party also emphasizes the contribution of data minimization to the specification of purpose and represents that *''the data collected on the data subject should be **strictly necessary for the specific purpose** previously determined by the data controller (the "data minimisation" principle). Data that is unnecessary for that purpose should not be collected and stored "just in case" or because "it might be useful later."*[112]

Based on these above mentioned inputs from EDPS and Article 29 Working Party about data minimization and Article 5(c) of GDPR[113], it is certain that limitation of the collection of personal information is directly relevant and necessary to achieve a specified purpose. Beside of this fact, it can facilitate data protection and reduce the concerns of users by limitation of collected big data. If stakeholders can comply with data minimization principle, Smart TV users can have more control over the stored data,[114]because they will be sure that there is no unnecessary collected personal information.

When Samsung Smart TV voice recognition system case addressed in Chapter 2 is examined, the problem is collection of all voices including conversations which is uncontrollable for users. In other words, Samsung Smart TV voice recognition system collects all conversations, if the conversation is within its coverage area. The main purpose of processing of voice commands through this system is providing better experiences for Smart TV services. It is obvious that collection of all conversation in front of Smart TVs is not within objectives of the services for voice recognition system. Therefore, collection of all conversation is absolutely unnecessary process for the purpose determined by Samsung. It is also further processing of personal data which is incompatible with the purpose specified by Samsung, as a data controller, who is responsible to determine the purpose and means of processing of personal data for the voice recognition system. In the context of these findings, it is easy to admit that

[111] European Data Protection Supervisor - definition of data minimization available at: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74
[112] Article 29 Working Party Opinion 8/2014 on recent developments on the Internet of Things p.16 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
[113] Article 5(c) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf
[114] Approach of European Digital Rights to Data minimization available at: https://edri.org/files/04-minimisation.pdf

this Samsung Smart TV case is crucial example of breach of principles of data minimization and limitation of purpose.

Despite of the breach of fundamental principles of data protection mentioned above, there are still criticisms from these stakeholders that data minimisation principle is unreasonable for the sake of future of Smart TVs.[115]Because the more personal data means more personalized services for users and more income from stakeholders' point of view. Therefore, stakeholders have an intention to disregard the principle of data minimization.[116]However, stakeholders' concerns can be deemed as reasonable in the context of their commercial purposes. On the other hand, it should be admitted that stakeholders cannot override and ignore data minimization principle for the sake of their business interests.

3.3 Informed consent

Data subject's consent is an important concept and pre-requisite for lawful data processing beside the other legal processing requirements. Since the consent of data subject opens the doors to personal data and more tailored services for all online service users including Smart TV users. On the other hand, it should be noted that consent does not create an exemption for lawful data processing. It is primarily one of the legal grounds for lawfulness of processing of personal data, and does not waive the application of other principles.[117]This section will describe and analyse the informed consent regulated under GDPR in the context of privacy related features addressed in Chapter 2.

Under the Article 4(8) of GDPR[118], legitimate consent of data subject listed under the exhaustive list of lawful processing grounds is briefly stated that *''data subject's consent is any **freely given**, specific, informed and **unambiguous indication** of his or her wishes by which the data subject, either by a statement or by a clear **affirmative action** signifies agreement to personal data relating to them being processed.(…)''Obviously,* with the terms ''unambiguous'' and ''affirmative action'', GDPR determined

[115] Comments on ''Future of Privacy Forum'' held on November 19, 2013 p.7 available at: https://fpf.org/wp-content/uploads/FPF-IoT-Comments_January-2014.pdfIdem.
[116]''Big Data for All: Privacy and User Control in the Age of Analytics'' published by Tene, Omer and Polonetsky, Jules, on 20th of September 2012. 11 Northwestern Journal of Technology and Intellectual Property 239 (2013) p.22 available at SSRN: http://ssrn.com/abstract=2149364
[117] Article 29 Working Party Opinion 15/2011on the definition of consent, p.7 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf
[118] Article 4(8) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

the criteria about consent on processing of personal data for online services. Based on this provision, implied consent does not comply with the conditions for informed consent.

Recital 25 of GDPR clarifies that users can give their consents for processing of personal data through affirmative action.[119] It can appear through such as ticking a box on a website. In general manner, "*choosing technical settings for information society services,*" or "*any other statement or conduct*" are tools for giving consent for the processing.[120] However, "*silence, pre-ticked boxes or inactivity"* shall not be deemed as affirmative action or free consent.[121]In other words, consent for processing of personal data must be specific and clear. Therefore, ''*blanket consent without specifying the exact purpose of the processing is not acceptable*''.[122]

- *Request consent for privacy related features on Smart TVs*

As analysed in Chapter 2, one of the main concerns regarding online services are lack of informed consent and informed decision of users, particularly for profiling. Users are mostly not aware of the extent and purpose of processing of personal data. For some cases such as ''TPVision case'' referred in Chapter 2, users are not even requested for consent by Smart TV stakeholders for processing of their personal data. However, as mentioned in the above paragraphs, informed consent is the legal grounds of lawful processing of personal data. Therefore, in that TPVision case, lack of informed consent for processing of personal data is obviously breach of Article 7(2) of GDPR. Due to importance of informed consent, legal conditions for informed consent regulated under Article 7(2) of GDPR will be analysed based on the privacy and data protection concerns raised by Smart TV services.

Article 7(2) of GDPR indicates that *the request for consent must be clear and distinguishable from other matters, in* ***an intelligible and easily accessible form****, using* ***clear and plain language***. [123]

[119] Recital 25 of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf
[120] ''Top 10 operational impacts of the GDPR: Part 3 – consent'' published by Gabriel Maldoff on 12th of January 2016 available at: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/
[121] ''Top 10 operational impacts of the GDPR: Part 3 – consent'' published by Gabriel Maldoff on 12th of January 2016 available at: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/
[122] Article 29 Working Party, Opinion 15/2011 on the definition of consent p.17 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf
[123] Article 7(2) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

The terms ''Intelligible and accessible'' are crucially important for data controllers. Because they have to formulate the form of request in compliance with these required terms. Therefore, it is useful to describe these terms used in Article 7(2).

''Intelligible request for consent'' means that request should ''*refer clearly and precisely to the scope and the consequences of the data processing. It cannot apply to an open-ended set of processing activities.''*[124]''Accessible request for consent'' means that request for consent which contains clear and precise information about the data processing should be easily accessible for users without their extreme effort. When the meanings of these concepts are examined, it can be presumed that these relevant concepts exactly address to the lack of information and consent about profiling for personalized services on Smart TVs. Because, as mentioned in Chapter 2, users mostly don't have sufficient knowledge about the scope and the consequences of data processing.

''Clear and plain language'' means that request for consent should be formulated clearly ''*without any complicated legal and technical jargon, in a language understandable and noticeable by users''*[125]It is obvious that Smart TVs use different technical instruments such as cookies and recommendation engine systems in order to provide personalized services on Smart TVs. Due to lack of users' knowledge, they may have some problems in order to make a decision whether these instruments may affect them or not. On the other hand, Smart TV manufacturers, application developers and third parties, who are obliged to inform the users about processing of personal data, shouldn't expect from users that they should have known technical backgrounds of these instruments in advance. Therefore, these data controllers of Smart TV services have to precisely explain thefunctions of these instruments and purpose

[124]''Customer Centric Marketing in the European Union from a Legal Perspective written by Eleni Tzoulia published in Handbook of Research on Managing and Influencing Consumer Behavior'' Chapter 4, p.85 available at: https://books.google.nl/books?id=GiKXBQAAQBAJ&pg=PA85&lpg=PA85&dq=open-ended+set+of+processing+activities.&source=bl&ots=CfYhl7mqe5&sig=zZFzGL3U_b3kBl7ooLhhC09lTbM&hl=nl&sa=X&ved=0ahUKEwjap97Y3L3LAhWmQpoKHTjQCssQ6AEIKjAC#v=onepage&q=open-ended%20set%20of%20processing%20activities.&f=false

[125]''Customer Centric Marketing in the European Union from a Legal Perspective written by Eleni Tzoulia published in Handbook of Research on Managing and Influencing Consumer Behavior'' Chapter 4, p.85 available at: https://books.google.nl/books?id=GiKXBQAAQBAJ&pg=PA85&lpg=PA85&dq=open-ended+set+of+processing+activities.&source=bl&ots=CfYhl7mqe5&sig=zZFzGL3U_b3kBl7ooLhhC09lTbM&hl=nl&sa=X&ved=0ahUKEwjap97Y3L3LAhWmQpoKHTjQCssQ6AEIKjAC#v=onepage&q=open-ended%20set%20of%20processing%20activities.&f=false

of using them. For instance, below mentioned declaration can be a good example[126]of plain and clear consent request for recommendation engine system:

Consent Declaration for the Recommendation Engine

The "Recommendation Engine" service will recommend to you certain broadcasts, programs, videos, etc. by analyzing the broadcasts and programs that are followed by you, and will record such broadcasts, programs, videos, etc. on your device for future viewing in cases where the device is turned off.
For this service, VestelElektronik San. Ve Tic. A.S. ("**Vestel**") collects personal data such as which kind of broadcast or program you have watched, the time you have watched the broadcast or the program, as well as collecting and storing your TV MAC address **("Your Data").**
Vestel will collect, record or use Your Data and transfer Your Data to its servers for providing the Recommendation Engine service. Vestel may transfer Your Data to countries outside the European Union and/or the European Economic Area subject to appropriate safeguards to ensure an adequate data protection level.
You hereby consent to the tracking, recording and use as well as to the transfer of Your Data to Vestel's servers, limited to the scope of said service. That may include any transfer of Your Data to countries outside the European Union and/or the European Economic Area subject to appropriate safeguards to ensure an adequate data protection level.

In the first paragraph of consent declaration, the purpose of the processing of personal data is determined through informing that recommendation system will recommend certain broadcasts, programs and videos through analysis of user's past viewings. Briefly, it gives clear information about the purpose of processing which is recommendation of certain content and the identified engine as a mean of processing of personal data. In the second paragraph, it gives information about personal data to be processed such as watched contents and the time users watched them. Additionally, the paragraph informs that TV MAC address which is unique identifier of televisions will also be collected by Smart TV manufacturers.

As it is known that some companies knowingly use complicated language in order to take consent of users.[127] Therefore, users are mostly *''not aware of the amount of information about themselves that they are ''agreeing'' to make available''*.[128]In that regard, data controllers of Smart TV services must aim

[126] This statement is taken from Vestel Smart TV.
[127] ''The Convergence of Virtual Reality and Social Networks – Threats to Privacy and Autonomy'' published by O'Brolcháin, Fiachra; Jacquemard, Tim; Monaghan, David; O'Connor, Noel; Novitzky, Peter; Gordijn, Bert in Science & Engineering Ethics ;Feb 2016, Vol. 22 Issue 1 , in February 2016, p.8 available at: http://connection.ebscohost.com/c/articles/112358475/convergence-virtual-reality-social-networks-threats-privacy-autonomy
[128] ''The Convergence of Virtual Reality and Social Networks – Threats to Privacy and Autonomy'' published by O'Brolcháin, Fiachra; Jacquemard, Tim; Monaghan, David; O'Connor, Noel; Novitzky, Peter; Gordijn, Bert in

at reaching intelligible language for their users. Subject to these considerations, it can be noted that the above mentioned declaration describes exactly what kind of personal data they use for providing recommendation service without using complicated technical concepts or confusing language.

Overall, with regard to the features used for providing personalized services on Smart TVs, relevant stakeholders should comply with certain legal requirements, as called request for prior consent with indication of wishes expressed by user's active behaviour and an ability to choose freely.[129]

3.4 Profiling

As described in Chapter 2, profiling is the key element of Smart TVs personalised services and the relevant concerns about their services mostly arise from profiling for online behavioural advertising and its other features. GDPR ensures several opportunities for users in order to reduce the concerns of users regarding their personal data processed for profiling. These opportunities obviously bring several obligations for data controllers of stakeholders under GDPR. In the light of these concerns and practices on profiling, this section will analyse the legal requirements for profiling based on the GDPR.

GDPR allows profiling under certain requirements which are regulated under Article 19(2) of the GDPR that *''where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.* In other words, this article rules that users who are provided online behavioural advertising services by relevant stakeholders have the right to object to the processing of their personal data at any time. These provisions obviously address to the necessity of mechanisms which should enable the users to object to the processing of personal data for online behavioural advertising. In the context of the necessity of a mechanism, E- Privacy Directive (Directive 2002/58/EC) provisions provide several requirements such as opt-in and opt-out mechanisms for online behavioural advertisings. As mentioned in Chapter 2, online

Science & Engineering Ethics ;Feb 2016, Vol. 22 Issue 1 , in February 2016, p.8 available at: http://connection.ebscohost.com/c/articles/112358475/convergence-virtual-reality-social-networks-threats-privacy-autonomy

[129] Article 29 Working Party Document 02/2013 on providing guidance on obtaining consent for cookies p.3 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

behavioural advertising tools are uncontrollable and invisible. Based on these negative sides of the tools for users, it can be noted that such mechanisms definitely facilitate more control over user's profiles in favour of users.[130] These two mechanisms will be thoroughly discussed based on GDPR under Chapter 4.

Another relevant article of GDPR is article 20(1) which states that ''*the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*.'' [131] As it is described under Chapter 2, user-specific profiles are generated from different types of collected information about users based on mathematical and statistical outcome which is obviously retrieved by relevant stakeholders. From these mathematical and statistical outcome, stakeholders make a decision concerning users' interests and preferences. Obviously, these decisions can cause negative and positive consequences concerning users. Based on these possible consequences, users have the right not to be subject to these decisions created by profiling according to Article 20 of GDPR. Briefly, as indicated by Koops, data subjects will be informed about profiling activities before they decide on whether they avoid profiling-based decisions despite of informed consent of data subjects.[132]

Koops also emphasizes that ''*threshold of significant affect*'' should be determined for online profiling practices to be done in compliance with Article 20 of GDPR.[133]Data controllers of Smart TV services will receive additional guidance from the European Data Protection Board to abide by what automated data processing activities fall within the definition of profiling under GDPR.[134]In that regard, it can be presumed that European Data Protection Board will give guidance about the threshold of significant affect concerning users.[135]

---

[130] Article 29 Working Party Opinion 2/2010 on online behavioural advertising p.16 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[131]Article 20 of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

[132] ''On Decision Transparency, or How to Enhance Data Protection after the Computational Turn'' published by Koops, Bert-Jaap on 1st of September 2013 p.5 available at SSRN: http://ssrn.com/abstract=2367510

[133] ''On Decision Transparency, or How to Enhance Data Protection after the Computational Turn'' published by Koops, Bert-Jaap on 1st of September 2013 p.5 available at SSRN: http://ssrn.com/abstract=2367510

[134]''On Decision Transparency, or How to Enhance Data Protection after the Computational Turn'' published by Koops, Bert-Jaap on 1st of September 2013 p.5 available at SSRN: http://ssrn.com/abstract=2367510

[135] Recital 58a of GDRP available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

3.5 Transparency

As indicated under Chapter 2, there are some concerns about lack of transparency about Smart TVs personalized services. Particularly, invisibility of instruments used for Smart TV services is one of the main data protection concerns, particularly for profiling. Invisibility is obviously the underlying reason of lack of transparency. In that regard, this sub-section aims at analysing relevant provisions about transparency of processing of personal data.

The principle of transparency is established as a core component of GDPR under Article 5 1(a) of GDPR stating that personal data must be *''processed (….) in a **transparent manner** in relation to the data subject''*[136]

Recital 30 of GDPR explains the underlying reason of indication of the expressing the term **''in a transparent manner.''** It states that *''the principle of transparency is subject to ensuring transparent processing in respect of the individuals concerned and **data subject's right to get confirmation and communication of personal data** being processed concerning them.''*[137] From this Recital, it can be presumed that GDPR aims at strengthen the communication between data subjects and controllers regarding the processing of personal data which obviously contributes to increasing of transparency of processing of personal data. Particularly, the expression ***''data subject's right to get confirmation''*** refers to informed consent and transparent information for processing of personal data regulated under Article 4(8) and Article 12(1) of GDPR. However, the underlying meaning of the expression ***''get confirmation and communication of personal data''*** is that transparency of data processing is not limited with giving detailed information before consent of data subjects. In that regard, all relevant stakeholders of Smart TVs must constitute transparency of data processing at every stage of processing. By the agreement on GDPR, organizational and technical measures will become more significant than before in order to establish transparency of personal data. Possible technical and organizational measures will be discussed in detail under Chapter 4. Additionally, As Koops remarked, GDPR's approach

[136] Article 5 1(a) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf
[137] Recital 30 of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

to enhancement of transparency is remarkable and it will obviously contribute to strengthening of user control over their personal data.[138]

Article 12(1) of GDPR prescribes that *''information related to processing of personal data must be provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.''*[139]It can be presumed from this Article that Smart TVs standard privacy policies and relevant stakeholders statements for lawful processing of personal data will not be sufficient, therefore more precise information should be provided concerning processing of personal data through effective ways.[140]

CHAPTER 4: MITIGATION METHODS FOR DATA PROTECTION ISSUES RAISED BY SMART TV

So far, relevant privacy and data protection concerns regarding Smart TV personalized services have been described and GDPR's relevant provisions have been analysed in the light of Smart TV features. Under this Chapter, firstly, possible mitigation methods regulated by GDPR and adopted by industries will be analysed and discussed whether these methods are compatible with GDPR and privacy related features of Smart TVs. Secondly, the possible methods will be discussed for building up confidence of consumers in the context of privacy and data protection concerns.

4.1. Consent Mechanisms for Smart TVs Personalised Services

As described under Chapter 3, informed consent is one of the legal conditions for lawful processing of personal data according to GDPR, particularly for Smart TV personalized services which process personal data of users. Data Protection Directive requires the explicit consent in order to legitimise the processing of sensitive data which is regulated under Article 8 of Data Protection Directive. However, according to

[138]''On Decision Transparency, or How to Enhance Data Protection after the Computational Turn'' published by Koops, Bert-Jaap on 1st of September 2013 p.5 available at SSRN: http://ssrn.com/abstract=2367510
[139] Article 5 of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf
[140] ''Data Protection Within Digital Economy'' published by Deloitte in 2015 p.4 available at: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-data-protection-within-digital-economy-102015.pdf

Article 4(8) of GDPR, explicit consent must be obtained for the processing of all types of personal data, provided that it shows unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action signifies agreement[141] With the clear emphasize on affirmative action, GDPR aims at prohibiting implied consent for personal data due to uncertainties arising from different interpretations of the term ''unambiguous''. Therefore, there is obviously a necessity for relevant stakeholders to determine a consent mechanism in line with the legal conditions of GDPR.

Despite of trend of collection and process of user's online behaviours, there are several tools that users are capable to control their online behavioural advertising experiences. Information Commissioner Officer describes that ''*consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website''*[142]In other words, data controllers may provide information through pop-up ticking box in order to request consent of users for processing of personal data. The most preferred tool among relevant stakeholders is ''opt-out" mechanism. With opt-out box mechanism, users can tick to object to collection and processing of online behavioural information.[143]Until the moment of tick to opt-out, user's consent is implied by the relevant stakeholders and all user's information are collected for online behavioural advertising. As described in Chapter 2 and 3, processing of personal data for personalized services is regulated with strict legal requirements under GDPR. Explicit consent with affirmative action is a legal condition pursuant to Article 4(8) of GDPR.[144] However, opt-out mechanism seeks for implied consent of users regarding collection of information of users. Therefore, opt-out mechanism cannot be applied to Smart TVs personalized services described under Chapter 2, as long as data controllers of Smart TV services process personal data of users.

[141] Executive Briefing Paper Proposed General Data Protection Regulation published by Hunton&Williams p.3available at: https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Executive_Briefing_Paper_Proposed_General_Data_Protection_Regulation.pdf

[142] ''Direct Marketing Guidance'' published by Information Commissioner Officer, p.22 available at: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

[143] ''Direct Marketing Guidance'' published by Information Commissioner Officer, p.23 available at: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

[144] Article 4(8) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

On the other hand, prior opt-in mechanisms which require an affirmative user's explicit consent prior to the processing of personal data, are in line with Article 4(8) of GDPR[145] and in that regard, advert network providers and advertisers, as data controllers can use prior opt-in mechanism for cookies provided that option to object to the processing of personal data is available and accessible at any time for users pursuant to Article 19(2) of GDPR and detailed information are given to user's regarding processing of user's data for online behavioural advertising pursuant to Article 12(1) of GDPR. Additionally, prior opt-in mechanism is also suitable for recommendation engine systems, voice and facial recognition systems as long as Smart TV manufacturers process biometric data, identifiable voice commands and create user profiles through these tools for personalized services. The same legal requirements obviously exist for these systems pursuant to Article 19(2) and Article 12(1) of GDPR.

4.2 Privacy by Design

Privacy by Design is ''*an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures*.''[146] It means that companies take privacy by design into account at every stage of the development of products or services. The main purpose of this concept is enhancement of security measures for personal data. In that regard, privacy by design can be a significant solution to data protection concerns raised by Smart TV services, as described under Chapter 2. It should be denoted that pursuant to Article 79 of GDPR, data protection authorities are enabled to impose fines for breach of GDPR principles. The fines can be 4% of total annual worldwide turnover; or €20,000,000.[147] In other words, if relevant stakeholders do not take organizational and technical measures for data protection, they will be faced with such a big amount of fine. Due to the importance of establishment of organizational and technical measures, this section will focus on the relevant organisational and technical measures encouraged by GDPR and industries and analyse which measures are compatible with Smart TV features in line with GDPR.

[145] Article 29 Working Party Opinion 2/2010 on online behavioural advertising p.16 available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf
[146] Definition of Privacy By Design by ''Information and Privacy Commissioner of Ontario'' available at: https://www.ipc.on.ca/english/privacy/introduction-to-pbd/
[147] Article 79 of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

The concept of privacy by design is developed by a joint corporation of the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and the Netherlands Organisation for Applied Scientific Research in 1995 for the first time.[148] From that year to this, it has been analysed in order to contribute to the development of technologies in compliance with privacy aspects. The concept of "Privacy by Design" is closely related to the concepts of "privacy enhancing technologies" and ''transparency enhancing technologies''.[149] In that sense, apart from analysis of general aspects of privacy by design, this section will focus on both privacy and transparency enhancing technologies.

There have been several crucial contributions to the principle of privacy by design in Europe. Such as, Article 29 Working Party recommended that *''every stakeholder in the Internet of Things should apply the principles of Privacy by Design"*.[150]

By adoption of GDPR, implementation of privacy by design will be obligation of data controllers under Article 23 of GDPR as follows ''*the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures''*[151]With the terms ''*....at the time of the determination of the means for processing' and at the time of the processing itself*' used in this Article, this Article points out that data controllers should take into account privacy and data protection concerns and relevant requirements regarding their instruments which are intended to use for processing of personal data before they start to process personal data. Technical and organisational measures for privacy by design are not defined under GDPR. Lack of specific definition for technical and organisational measures is not a drawback of GDPR. It is conversely creating a flexible field to develop measures provided that they comply with GDPR.

---

[148]''Privacy by design: delivering the promises'' published by Peter Hustinx, Identity in the Information Society, 2010, Volume 3, Number 2, p.253available at: http://link.springer.com/article/10.1007/s12394-010-0061-z

[149]''Privacy by design: delivering the promises'' published by Peter Hustinx, Identity in the Information Society, 2010, Volume 3, Number 2, p. 253available at: http://link.springer.com/article/10.1007/s12394-010-0061-z

[150] Article 29 Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things, p.21 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[151] Article 23(1) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

4.2.1 Privacy Enhancing Technologies

The use of privacy enhancing technologies ease to develop information and communication systems and services provided that they minimise the collection and use of personal data in compliance with data protection rules.[152] In other words, they can contribute to the data minimization principles regulated under GDPR and reduce the risks of unnecessary collection and processing of personal data for Smart TV services described under Chapter 2 and 3.

There are several types of privacy enhancing technologies[153], however this sub-section will focus on the possible privacy enhancing technologies – anonymization and pseudonymization encouraged by GDPR and their compatibility with Smart TV privacy related features.

- *Anonymization*

Article 29 defines that *''anonymization is a technique applied to personal data in order to achieve irreversible de- identification. Therefore, the starting assumption is that the personal data must have been collected and processed in compliance with the applicable legislation on the retention of data in an identifiable format.''*[154] It means that the anonymized data is no longer personal data suitable for personalized services. Because ''Irreversible de-identification'' does not facilitate personalized services of Smart TVs. Additionally, the main objective of Smart TV services is processing more personal information in order to provide users with personalized services. Therefore, anonymization doesn't seem feasible for personalized services. However, if the purpose of data controllers of Smart TV services is achievement of statistical analysis of user's behaviour, anonymization of personal data can be a safety technique in order to reduce the risks for data protection concerns and comply with data minimisation principles.

[152]European Commission press release ''Privacy Enhancing Technologies (PETs)The existing legal framework'' published on 2nd of May 2007 available at: http://europa.eu/rapid/press-release_MEMO-07-159_en.htm

[153] Idem

[154] Article 29 Working Party Opinion 05/2014 on Anonymization Techniques, p.23 available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

- *Pseudonymization*

By introduction of pseudonymization, as a privacy enhancing technology under GDPR, legislators aims at ''*reducing risks for the data subjects concerned and helping controllers and processors meet their data protection obligations*.''[155] It is apparently an affirmative step for ensuring data protection. However, implementation of pseudonymization is also important in order to meet data protection obligations. In other words, such technologies can facilitate data protection for every stakeholder as long as they are operated in a good manner and compatible with its services and purposes. In that regard, compatibility of pseudonymization is also discussed under the following paragraphs apart from detailed information about its capabilities.

Article 4(3b) defines that ''*pseudonymisation is the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person''*[156]In other words, data subject is unidentifiable as long as additional information is kept separately.

Pseudonymization technically removes identifiable data such as an IP address, which can single out data subject, and replaces it with a machine-generated identifier.[157]However, as a result of pseudonymization process, identifiable data is still exist as an encrypted data. In other words, there is still possibility to re-identify the data subject.[158]In that regard, pseudonymization is still subject to the processing of personal data and data protection obligations within GDPR as described under Chapter 3.

[155]Recitals 23a of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

[156] Article 4(3) of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

[157]''UK: Pseudonymisation: The Benefits And Getting Regulation Right'' published by Victoria Hordern on 17th of March 2014 availableat:http://www.mondaq.com/x/300206/Data+Protection+Privacy/Pseudonymisation+The+Benefits+And+Getting+Regulation+Right

[158]''UK: Pseudonymisation: The Benefits And Getting Regulation Right'' published by Victoria Hordern on 17th of March 2014 availableat:http://www.mondaq.com/x/300206/Data+Protection+Privacy/Pseudonymisation+The+Benefits+And+Getting+Regulation+Right

In the light of the above mentioned findings, pseudonymization is not an ideal solution for relevant stakeholders and users. Because the risks of access to unique identifiers and re-identification are still exist. When the relevant concerns of Smart TV features, particularly about security measures, are examined, pseudonymization can be an affirmative instrument for relevant stakeholders in order to meet data protection obligations under GDPR. If it is used for their personalized services, it can also create more flexibility and comfort for processing of personal data and establishment of security measures. As mentioned in the above paragraphs, pseudonymization does not create exemption from data protection requirements. Because pseudonymization is still subject to legal requirements for processing of personal data. When the compatibility of pseudonymization process for Smart TV features is examined, pseudonymization is a useful technique, as long as the unique identifiers (such as MAC address) collected for Smart TV features are secured. In that regard, security measures cannot be underestimated by relevant stakeholders at any time.

4.2.2 Transparency Enhancing Technologies

As described under Chapter 3, GDPR prescribes a pre-requisite for information of users as in case of any personal information is collected, stored, processed and disclosed. In that regard, transparency enhancing technologies can be significant instruments in order to fulfil the legal requirements of GDPR.[159]As such, transparency enhancing technologies can be deemed as one of the mitigation method in the context of privacy risks raised by Smart TV services.

Hansen indicated that ‘’*transparency tools are tools which can provide to the individual concerned clear visibility of aspects relevant to personal data and the individual's privacy.*’’[160]The user's privacy should be secured by relevant ICT systems which process the user's personal data. In particular users have to be informed about the consequences of privacy infringement and actors involved in processing, for

[159]‘’Transparency enhancing tools (TETs): an overview’’ published by Milena Janic, Jan Pieter Wijbenga, Thijs Veugen from TNO Delft University of Technology, Delft, The Netherlands in 2013, p.1 available at:http://quantum.ewi.tudelft.nl/sites/defauPlt/files/TETs%20paper%20STAST2013.pdf

[160] ‘’Marrying Transparency Tools with User-Controlled Identity Management’’ published by Hansen, M. in 2008 In The Future of Identity in the Information Society. (Springer US), pp. 205available at: http://download.springer.com/static/pdf/194/chp%253A10.1007%252F9780387790268_14.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fchapter%2F10.1007%2F9780387790268_14&token2=exp=1455530180~acl=%2Fstatic%2Fpdf%2F194%2Fchp%25253A10.1007%25252F9780387790268_14.pdf%3ForiginUrl%3Dhttp%253A%252F%252Flink.springer.com%252Fchapter%252F10.1007%252F9780387790268_14*~hmac=3ebe3d749ee1b91d47f1e4a548c5e33b7d077a6220eee31a6ea8e925c4a568ad

instance, who definitely or potentially has access to personal data, and about the likely results.[161]Since users are generally not able to analyse what data about them is collected and which information about them is inferred from collected data and how that data is being used.[162]

There are many transparency enhancing technologies which are already adopted by industries for different services. The above mentioned transparency enhancing technologies are recommended in this thesis based on their compatibilities with Smart TV features in the compliance with transparency principles adopted by GDPR.

- *Privacy dashboard*

Nik Doty from Berkeley describes privacy dashboard as a tool which ''*answers the common user question "what do you know about me?" and does so in a way that the user can understand and take appropriate action if necessary. they provide a summary or highlight of important personal data*.''[163]In other words, privacy dashboards are designed to inform users about purpose of collection and processing of personal data for a particular consumer. This is a significant opportunity for users to have control over their personal data and get information about the processing. However, establishment of privacy dashboard is a challenging decision for stakeholders who are extremely in need of processing personal data for online behavioural advertising and other personalized services.

Generally, users are not explicitly informed about the context of data collection and processing in the event that they install or use an App and moreover, they have to accept the requests submitted through App system for data collection, sharing or processing in order to provide the content or service.

[161] ''Marrying Transparency Tools with User-Controlled Identity Management'' published by Hansen, M. in 2008 In The Future of Identity in the Information Society. (Springer US), pp. 213available at: http://download.springer.com/static/pdf/194/chp%253A10.1007%252F9780387790268_14.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fchapter%2F10.1007%2F9780387790268_14&token2=exp=1455530180~acl=%2Fstatic%2Fpdf%2F194%2Fchp%25253A10.1007%25252F9780387790268_14.pdf%3ForiginUrl%3Dhttp%253A%252F%252Flink.springer.com%252Fchapter%252F10.1007%252F9780387790268_14*~hmac=3ebe3d749ee1b91d47f1e4a548c5e33b7d077a6220eee31a6ea8e925c4a568ad

[162] ''A Categorization of Transparency-Enhancing Technologies'' published by Christian Zimmermann from Institute of Computer Science and Social Studies University of Freiburg in 2015 p.1 available at: http://arxiv.org/ftp/arxiv/papers/1507/1507.04914.pdf

[163]''Privacy dashboard'' published by Nick Doty on 2nd of August 2011 available at: https://github.com/mohit/privacypatterns/wiki/Privacy-dashboard

[164]Subject to the lack of informed decision, the Privacy Dashboard can be deemed as an instrument which should be capable to provide reasonable overview of operations of each app based on user personal data. [165]

Smart TV privacy dashboard can be useful method for users who have not efficient control on their personal data and feel uncomfortable about how Smart TV platform and applications collect and use their personal data. In that regard, that user-centred approach of privacy dashboard can contribute to transparency of data processing and raise awareness of Smart TV users about the processing of their personal data. In a Smart TV privacy dashboard scenario, data breach notifications can be easily sent to users via dashboard mechanism in an efficient way. In that case, interoperability of dashboard expedites the efficiency of data breach notifications, if users have access to Smart TV privacy dashboard through their other devices such as smartphone, tablet and computers. Privacy dashboard is compatible with the transparency principle ruled under Article 12(1) of GDPR, provided that it is established in an intelligent and accessible form. As ruled under Article 12(1) access to information at any time is the main principles of transparency of processing of personal data. In the light of the above mentioned information, privacy dashboard is capable of informing users and enabling them to control over their personal data. However, as mentioned in this part, when the relevant cases and risks are examined, it can be a challenging and significant decision of the relevant stakeholders on establishment of such a dashboard.

4.3 Confidence of Smart TV users

As mentioned under Chapter 2, users are anxious about their personal data collected and processed in the context of online services. Users have doubts on how data controllers of Smart TV services collect their personal data and to what extent they process personal data. TrustE -websites privacy certifications provider- states that ''*92% of consumers are concerned about privacy and 89% avoid doing*

[164] ''Because we care: Privacy Dashboard on FirefoxOS'' published by Marta Piekarska, Dominik Strohmeier, Yun Zhou, Alexander Raake in 2015 p.4 available at: http://ieee-security.org/TC/SPW2015/W2SP/papers/W2SP_2015_submission_28.pdf

[165] ''Because we care: Privacy Dashboard on FirefoxOS'' published by Marta Piekarska, Dominik Strohmeier, Yun Zhou, Alexander Raake in 2015 p.4 available at:http://ieee-security.org/TC/SPW2015/W2SP/papers/W2SP_2015_submission_28.pdf

business with companies they don't trust.''[166]In other words, users don't trust the stakeholders even though they take organisational and technical measures. This fact also affects the stakeholders' businesses. They make huge investments on personalized services in order to provide better experiences on their television. However, they are still not able to gain their users' trust. Because the previous experiences such as TPVision and Samsung cases mentioned in this thesis already created preconceived opinions in user's mind. Based on the current position, it is not easy to achieve confidence of users and therefore there should be a cooperation of relevant actors in order to find methods on establishment of user's confidence. However, there is a big risk for stakeholders that ''*lack of confidence may slow down the development of innovative uses of new technologies.*''[167] *In that sense,* this section aims at finding answers to how confidence of users can be established and who can play this important role for the sake of user's confidence.

First of all, relevant stakeholders have to put consumers' privacy concerns at front and make internal and external analysis for improvement of their privacy practices in line with user's confidence. Secondly, stakeholders should become aware of the importance of cybersecurity and the complexity of threats against consumer privacy and look forward to find solutions and facilities in order to keep their consumers confident. On the other hand, privacy sphere is getting more complex in the framework of legislation and technological developments.[168]Therefore, establishment of confidence of users becomes more difficult for stakeholders.

In the light of above mentioned difficulties regarding establishment of confidence of users, this section will firstly recommend privacy seals which can boost confidence of consumers and secondly, two actors – Smart TV Alliances and European Consumer Organizations which can create significant awareness and confidence of users in the context of data protection issues, as follows:

- *Privacy Seals*

[166] Statement of TrustE related to privacy concerns available at: https://www.truste.com/business-products/trusted-websites/

[167] ''IoT Privacy, Data Protection, Information Security'' published by European Commission, p.8 available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753

[168]''Consumer Confidence In Privacy Online Is Decreasing'' published by Trisha Leon on 16th of July 2014 available at: http://www.bsminfo.com/doc/consumer-confidence-in-privacy-online-is-decreasing-0001

A privacy seal is a 'stamp of approval' which demonstrates quality of privacy practice and high data protection compliance standards.[169]Privacy seals provide consumers with information about companies' privacy policies, their business activities. Particularly, they give insights to consumers concerning how companies process and collect their personal data. It can be deemed as a guaranty for adequate data protection.[170]

Privacy seals are introduced and recognized by governments and companies and adopted in GDPR as a mitigation method under GDPR.[171] Article 39 of GDPR supports "*the establishment of data protection certification mechanisms and of data protection seals and marks*", as a means of enabling data subjects to "*assess the level of data protection provided by controllers and processors*".[172]Recital 77 of GDPR also encourages the "*establishment of certification mechanisms, data protection seals and marks" to enhance transparency, legal compliance and to permit data subjects the means to make quick assessments of the level of data protection of relevant products and services*.''[173]However, Joint Research Centre represents that ''*the mere presence of a seal is no guarantee*'', since there is no control mechanism such as similar to current Data Protection Authority whether the seal holder operates in compliance with GDPR. In that regard, there is a need for an additional layer of protection concerning privacy certification scheme, otherwise the presence of a seal may actively mislead consumers and create false confidence.[174]

[169] ''What are privacy seals?'' published by Information Commissioner's Office available at: https://ico.org.uk/for-organisations/improve-your-practices/privacy-seals/

[170] ''EU Privacy seals project Inventory and analysis of privacy certification schemes'' published by The Institute for the Protection and Security of the Citizen of the Joint Research Centre in 2013 p.12 available at: http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf

[171] ''EU Privacy seals project Inventory and analysis of privacy certification schemes'' published by The Institute for the Protection and Security of the Citizen of the Joint Research Centre in 2013 p.12 available at: http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf

[172] Article 39 of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

[173]Recital 77 of GDPR available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

[174] 'EU Privacy seals project Inventory and analysis of privacy certification schemes'' published by The Institute for the Protection and Security of the Citizen of the Joint Research Centre in 2013 p.15 available at: http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf

There are many privacy seals which provided by the companies in EU and outside EU.[175]As a consequence of vast amount of privacy seals and their certification schemes, consumers may consider that scopes of all certification schemes are same which may result in misunderstanding of assurance that the insufficient certification schemes are appropriate for protection of their personal data.[176]

One of the well -known privacy seal is EuroPrise which is developed by ''UnabhängigesLandeszentrumfürDatenschutzScheswig-Holstein (ULD)'' acting as a public independent privacy seal holder. ''*EuroPriSe envisions an information technology that recognizes, enhances and ensures privacy by integrated technology (Privacy by Design)*.[177]EuroPrise offers certification to manufacturers and vendors of IT products and IT-based services. The procedure consists of an evaluation of the product or service by accredited legal and IT experts and a validation of the evaluation report by an independent certification body.[178]EuroPrise seems a better option in order to clear the concerns on whether the third-party private privacy seal holders operate in compliance with GDPR. Because EuroPrise is established by independent German Data Protection Authority which is primarily entitled to take appropriate actions for ensuring effective data protection and it can be presupposed that they can properly assess compliance of their evaluation methods and certification schemes with GDPR by itself regardless of their position as a privacy seal holder due to their main responsibility.

Based on Smart TV scenario, when users realize the seals or marks on websites, applications or Smart TV platforms, they will consider that data controllers of these platforms take appropriate technical and organisational measures for their personal data and obviously comply with data protection obligations. Because as indicated under Recital 77 of GDPR, privacy seals are enable data subjects to consider the level of data controller's data protection they ensure. In that regard, such a mechanism can facilitate transparency of processing of personal data and confidence of users regarding the process of their personal data for Smart TV's personalized services. However, as mentioned in the above paragraphs,

[175] ''Privacy Seals and Privacy Snake Oil'' published by Toby Stevens on 19th of November 2014, available at:http://www.computerweekly.com/blogs/the-data-trust-blog/2014/11/privacy-seals-and-privacy-snak.html
[176]''Privacy Seals and Privacy Snake Oil'' published by Toby Stevens on 19th of November 2014, available at:http://www.computerweekly.com/blogs/the-data-trust-blog/2014/11/privacy-seals-and-privacy-snak.html
[177] ''Definition of EuroPrise'' published by European Privacy Seal available at: https://www.european-privacy-seal.eu/EPS-en/Vision
[178] 'EU Privacy seals project Inventory and analysis of privacy certification schemes'' published by The Institute for the Protection and Security of the Citizen of the Joint Research Centre in 2013 p.170 available at: http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf

there are still concerns about confidence on privacy seal holders and their certification schemes. Therefore, EuroPrise, as an independent privacy seal holder, can be better option for relevant stakeholders of Smart TVs in order to make their users confident about the processing of personal data and establish appropriate certification scheme in line with GDPR regulations.

- *Smart TV Alliance and Consumer Organizations*

Smart TV Alliance is established by LG Electronics, TP Vision and Toshiba in 2012 to create platform-independent services for Smart TV applications.[179] They aim at creating a large and productive ecosystem for smart TV application development that gives manufacturers a faster path to more and better TV applications, enables developers to write applications once for many different platforms, and provides consumers with a rich source of content and services. [180] Briefly, all relevant stakeholders come together in order to enhance their technologies and services through the benefits of Smart TV Alliance. This thesis recommends that Smart TV Alliance and its members can also contribute to create common approach such as general guidelines to be agreed and followed by members of Smart TV Alliance for ensuring organisational and technical measures in order to establish confidence of users. Such an approach may force to relevant actors in order to take appropriate measures for ensuring data protection measures which subsequently can create confidence of users. For instance, agreement on guidelines can be pre-requisite for membership of Smart TV Alliance. If they had managed to come together in a common business interest, they can also manage to discuss possible methods on establishment of confidence of users regarding data protection concerns.

European Consumer Organisation(''BEUC'')is a *''umbrella group in Brussels for its members and our main task is to represent them at European level and defend the interests of all Europe's consumers. BEUC investigates EU decisions and developments likely to affect consumers. Their current mission is to bring together consumer organisations of the European Union and other European countries in order to promote, defend and represent the interests of European consumers in the elaboration and implementation of European Union policies with the European Union institutions and with other*

[179] About Smart TV Alliance available at: http://smarttv-alliance.org/
[180] About Smart TV Alliance available at: http://smarttv-alliance.org/

bodies.''[181]In the lights of BEUC missions mentioned above, it seems feasible that BEUC can also bring together all mentioned consumer organizations in EU in order to create confidence of consumers regarding data protection measures. Moreover, cooperation of Smart TV Alliances and BEUC can also create confidence of users on data protection through many ways such as education of consumers and business actors. BEUC can contribute to the recommended Smart TV Alliance guidelines focused on interests of users. This is obviously just an illustrated and recommended method for cooperation of actors of business and consumer rights organizations. Different actors such as NGOs, other associations, competent governmental authorities obviously may take the recommended position of BEUC as well. In other words, creating awareness through cooperation on establishment of confidence of users is more important than who can lead this recommended method.

CHAPTER 5: CONCLUSION

This thesis aimed at giving insights into Smart TV privacy concerns and mitigation methods in terms of legal and technical aspects which have been analysed for other mentioned devices. As it is pointed out in Chapter 4, privacy and transparency enhancing technologies are essential instruments in order to challenge with privacy based problems. However, even though some of privacy enhancing methods such as pseudonymization and anonymization are also recommended by GDPR. There is no doubt that these identified methods definitely contribute to pursuit of data protection solutions. Because strengthening of principles depends on some technological and organizational measures which are even explicitly revealed in GDPR. This is obviously significant achievement of legislators of GDPR. On the other hand, sanctions ruled by GDPR will play important role to let relevant stakeholders to pay more attention to data protection concerns more than before. Because with the adoption of GDPR, there will be a big risk of loss of profit due to breach of GDPR principles.

As prescribed in Chapter 4, privacy dashboard allows users to control over their collected data and access to information about the purpose of processing of users' personal data and contributes to most of the relevant privacy principles such as data minimization and transparency of processing. This thesis

[181] Mission of European Consumer Organisation BEUC available at: http://www.beuc.eu/about-beuc/mission

strongly recommends privacy dashboard for enhancing of transparency of processing. Because it creates transparent field in order to realize the operations of data controllers among the complexity of technical instruments. Pseudonymization which can reinforce security measures against re-identification of users through third parties or employees of organizations. However as mentioned in Chapter 4, pseudonymization of personal data does not remove the unique identifiers. In that regard, this thesis recommends pseudonymisation. However, this thesis does not guarantee that data protection concerns can be absolutely solved by application of pseudonymization. Because, the risk of re-identification of users still remains due to existence of unique identifiers. Privacy Seals can help users to consider whether the websites and or applications abide by privacy legislations and provide technical and organizational measures regarding data protection. In that regard, EuroPrise can be better option to reduce the concerns about the independency of private privacy seal providers and the lack of control mechanism for operations of private privacy seal holders.

As identified in Chapter 3, GDPR seeks strengthening of privacy principles previously adopted in Data Protection Directive with significant provisions such as precise and detailed identification of profiling. GDPR clears the uncertainties about legal grounds for processing of personal data such as how unambiguous consent must be interpreted and rules that implicit consent does not legitimise the processing of personal data anymore. As mentioned in Chapter 2, Smart TV services may cause several vulnerabilities for ensuring data protection. Due to these concerns, adoption of these extended provisions related to profiling is vital.

As mentioned under Chapter 4, confidence of consumers is crucially important for all digital market including Smart TV. Since organizations realize that their financial interests significantly rely on confidence of consumers. In other words, achievement of organizations' goal is impossible without confidence of consumers. This thesis emphasizes that there is a big necessity of taking collective educational actions and determining collective self-regulatory principles such as through guidelines for establishment of confidence of users. In that regard, cooperation of Smart TV Alliances and BEUC and other organizations can contribute to realize the underlying reason of lack of confidence of consumers and take collective actions.

To sum up, GDPR addresses the key challenges for Smart TV services analysed in this thesis. However, GPDR does not give guidance by its very nature about being ideal data controller or processor beside regulating legal requirements for data protection. Therefore, there is a necessity of initiatives of all relevant actors who are specialized or interested in or responsible for taking organizational and technical measures in order to achieve efficient data protection.

BIBLIOGRAPHY

- GENERAL DATA PROTECTION REGULATION AVAILABLE AT: HTTP://WWW.STATEWATCH.ORG/NEWS/2015/DEC/EU-COUNCIL-DP-REG-DRAFT-FINAL-COMPROMISE-15039-15.PDF
- DIRECTIVE 98/34/EC AVAILABLE AT: HTTP://EUR-LEX.EUROPA.EU/LEXURISERV/LEXURISERV.DO?URI=CONSLEG:1998L0034:20070101:EN:PDF
- E-COMMERCE DIRECTIVE 2000/31/EC AVAILABLE AT: HTTP://EUR-LEX.EUROPA.EU/LEGAL-CONTENT/EN/TXT/PDF/?URI=CELEX:32000L0031&FROM=EN
- CONSUMER RIGHTS DIRECTIVE 2011/83/EU AVAILABLE AT: HTTP://EUR-LEX.EUROPA.EU/LEGAL-CONTENT/EN/TXT/PDF/?URI=CELEX:32011L0083&RID=1
- ARTICLE 29 WORKING PARTY OPINION 8/2014 ON THE ON RECENT DEVELOPMENTS ON THE INTERNET OF THINGS, AVAILABLE AT:HTTP://EC.EUROPA.EU/JUSTICE/DATA-PROTECTION/ARTICLE-29/DOCUMENTATION/OPINION-RECOMMENDATION/FILES/2014/WP223_EN.PDF
- ARTICLE 29 WORKING PARTY, OPINION 2/2013 ON APPS ON SMART DEVICES AVAILABLE AT: HTTP://EC.EUROPA.EU/JUSTICE/DATA-PROTECTION/ARTICLE-29/DOCUMENTATION/OPINION-RECOMMENDATION/FILES/2013/WP202_EN.PDF
- ARTICLE 29 WORKING PARTY, OPINION 1/2008 ON DATA PROTECTION ISSUES RELATED TO SEARCH ENGINES AVAILABLE AT:HTTP://EC.EUROPA.EU/JUSTICE/DATA-PROTECTION/ARTICLE-29/DOCUMENTATION/OPINION-RECOMMENDATION/FILES/2008/WP148_EN.PDF
- ARTICLE 29 WORKING PARTY, OPINION 04/2012 ON COOKIE CONSENT EXEMPTION, AVAILABLE AT: HTTP://EC.EUROPA.EU/JUSTICE/DATA-PROTECTION/ARTICLE-29/DOCUMENTATION/OPINION-RECOMMENDATION/FILES/2012/WP194_EN.PDF
- ARTICLE 29 WORKING PARTY OPINION 2/2010 ON ONLINE BEHAVIOURAL ADVERTISING AVAILABLE AT:HTTP://EC.EUROPA.EU/JUSTICE/POLICIES/PRIVACY/DOCS/WPDOCS/2010/WP171_EN.PDF

- ARTICLE 29 WORKING PARTY OPINION 3/2012 ON DEVELOPMENTS IN BIOMETRIC TECHNOLOGIES, AVAILABLE AT: HTTP://EC.EUROPA.EU/JUSTICE/DATA-PROTECTION/ARTICLE-29/DOCUMENTATION/OPINION-RECOMMENDATION/FILES/2012/WP193_EN.PDF

- ARTICLE 29 WORKING PARTY OPINION 1/2010 ON THE CONCEPTS OF "CONTROLLER" AND "PROCESSOR" AVAILABLE AT: HTTP://EC.EUROPA.EU/JUSTICE/POLICIES/PRIVACY/DOCS/WPDOCS/2010/WP169_EN.PDF

- ARTICLE 29 WORKING PARTY, OPINION 3/2003 ON PURPOSE LIMITATION AVAILABLE AT: HTTP://IDPC.GOV.MT/DBFILE.ASPX/OPINION3_2013.PDF

- ARTICLE 29 WORKING PARTY, ADVICE PAPER ON ESSENTIAL ELEMENTS OF A DEFINITION AND A PROVISION ON PROFILING WITHIN THE EU GENERAL DATA PROTECTION REGULATION'' ADOPTED ON 13TH OF MAY 2013 AVAILABLE AT:HTTP://EC.EUROPA.EU/JUSTICE/DATA-PROTECTION/ARTICLE-29/DOCUMENTATION/OTHER-DOCUMENT/FILES/2013/20130513_ADVICE-PAPER-ON-PROFILING_EN.PDF

- ARTICLE 29 WORKING PARTY DOCUMENT 02/2013 ON PROVIDING GUIDANCE ON OBTAINING CONSENT FOR COOKIES AVAILABLE AT: HTTP://EC.EUROPA.EU/JUSTICE/DATA-PROTECTION/ARTICLE-29/DOCUMENTATION/OPINION-RECOMMENDATION/FILES/2013/WP208_EN.PDF

- ARTICLE 29 WORKING PARTY OPINION 05/2014 ON ANONYMISATION TECHNIQUES, AVAILABLE AT: HTTP://EC.EUROPA.EU/JUSTICE/DATA-PROTECTION/ARTICLE-29/DOCUMENTATION/OPINION-RECOMMENDATION/FILES/2014/WP216_EN.PDF

- ''PERSONALIZATION AND PRIVACY: A SURVEY OF PRIVACY RISKS AND REMEDIES IN PERSONALIZATION-BASED SYSTEMS'' PUBLISHED BY ERAN TOCH, YANG WANG AND LORRIE FAITH CRANOR IN USER MODELING AND USER-ADAPTED INTERACTION APRIL 2012, VOLUME 22, ISSUE 1, PP 203-220, AVAILABLE AT: HTTPS://LINK.SPRINGER.COM/ARTICLE/10.1007%2FS11257-011-9110-Z

- '' SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING''PUBLISHED BY FTC STAFF REPORT IN FEBRUARY 2009 P.10 AVAILABLE AT: HTTPS://WWW.FTC.GOV/SITES/DEFAULT/FILES/DOCUMENTS/REPORTS/FEDERAL-TRADE-COMMISSION-STAFF-REPORT-SELF-REGULATORY-PRINCIPLES-ON LINE-BEHAVIORAL-ADVERTISING/P085400BEHAVADREPORT.PDF

- ''SMART-TV USABILITY: ACCESSING CONTENT IS KEY'' BY KIM FLAHERTY ON 20TH OF SEPTEMBER 2015 AVAILABLE AT: HTTPS://WWW.NNGROUP.COM/ARTICLES/SMART-TV-USABILITY/

- EXECUTIVE BRIEFING PAPER PROPOSED GENERAL DATA PROTECTION REGULATION PUBLISHED BY HUNTON&WILLIAMS AVAILABLE AT: HTTPS://WWW.HUNTONREGULATIONTRACKER.COM/FILES/UPLOADS/DOCUMENTS/EU%20DATA%20PROTECTION%20REG%20TRACKER/EXECUTIVE_BRIEFING_PAPER_PROPOSED_GENERAL_DATA_PROTECTION_REGULATION.PDF

- ''INTERNET AND WIRELESS PRIVACY: A LEGAL GUIDE TO GLOBAL BUSINESS PRACTICES'' PUBLISHED BY ELOISE GRATTON IN 2003

- ''HULU'S RECOMMENDATION SYSTEM'' PUBLISHED BY LIANG XIANG ON 19TH OF SEPTEMBER 2011 AVAILABLE AT: HTTP://TECH.HULU.COM/BLOG/2011/09/19/RECOMMENDATION-SYSTEM/

- ''SMART TV: ARE THEY REALLY SMART IN INTERACTING WITH PEOPLE? UNDERSTANDING THE INTERACTIVITY OF KOREAN SMART TV'' PUBLISHED BY DONG-HEE SHINA, YONGSUKHWANGB AND HYUNSEUNGCHOOC IN 2013 AVAILABLE AT: HTTPS://WWW.RESEARCHGATE.NET/PUBLICATION/233271216_SMART_TV_ARE_THEY_REALLY_SMART_IN_INTERACTING_WITH_PEOPLE_UNDERSTANDING_THE_INTERACTIVITY_OF_KOREAN_SMART_TV

- ''Market Analysis Smart TV'' published by Smart TV Working Group, available at: http://www.tv-plattform.de/images/stories/pdf/marktanalyse_smart-tv_2014_en.pdf
- ''Challenges of Connected TV'' published by DIRECTORATE-GENERAL FOR INTERNAL POLICIES POLICY DEPARTMENT B: STRUCTURAL AND COHESION POLICIES in September 2013 available at: http://www.europarl.europa.eu/RegData/etudes/note/join/2013/513976/IPOL-CULT_NT(2013)513976(SUM01)_EN.pdf
- ''What is Smart TV app definition?'' published by Digital Marketing Glossary on 6th of April 2015 available at: http://digitalmarketing-glossary.com/What-is-Smart-TV-app-definition
- ''What is a Smart TV'' written by Agent Plummer and Agent Hall published on 21 August 2015 available at: http://www.geeksquad.co.uk/articles/What-is-a-smart-tv
- ''Smart TV app development: it's not rocket science, it's HTML'' published by JukkaEklund on 28th of January 2015 available at:https://www.linkedin.com/pulse/smart-tv-app-development-its-rocket-science-html-jukka-eklund
- Samsung Forum in 2014 available at: https://www.samsungdforum.com/UxGuide/2014/03_input_method.html
- ''Samsung's Smart TVs Are Collecting And Storing Your Private Conversations'' published by Tim Cushing on 9th of September 2015:https://www.techdirt.com/articles/20150206/04532329928/samsungs-smart-tvs-are-collecting-storing-your-private-conversations.shtml
- NPD Display Search, Quarterly Smart TV Shipment and Forecast Report, Santa Clara, California, published on 17th of October 2012 available at:http://www.displaysearch.com/cps/rde/xchg/displaysearch/hs.xsl/121017_smart_tv_shipments_grow_worldwide_in_2012.asp
- ''Internet on TV, TV on Internet: Commission seeks views on rapidly converging audio visual world'' European Commission Press Release, Brussels, published on 24th of April 2013 available at: http://europa.eu/rapid/press-release_IP-13-358_en.htm
- ''Defining Profiling: A New Type of Knowledge?'' published by Mireille Hildebrandt In: Profiling the European Citizen, Cross-Disciplinary Perspectives'' (Hildebrandt, M., Gutwirth, S., eds.), in 2008, Springer Science,
- ''Advertising Standards Authority'' definition of online behavioural advertising available at: https://www.asa.org.uk/Consumers/What-we-cover/Online-behavioral-advertising.aspx
- ''The limits of privacy in automated profiling and data mining'' published by Bart W. Schermer in Computer law & security review 27 in 2011, available at: http://ac.els-cdn.com/S0267364910001767/1-s2.0-S0267364910001767-main.pdf?_tid=bcc5d40c-e313-11e5-9192-00000aab0f27&acdnat=1457211141_fe073a0b06276960f58cc1acd6b568c9

- European Commission – Information Provider's Guide – The EU Internet Handbook available at: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

- ''Recommender System Application Developments: A Survey'' -Faculty of Engineering and Information Technology, University of Technology Sydney, Australia – published by Jie Lu, Dianshuang Wu, Mingsong Mao, Wei Wang, Guangquan Zhang available at: http://www.uts.edu.au/sites/default/files/desi-publication-recommender%20system%20application%20developments%20a%20survey-accepted%20menuscript.pdf

- ''LG Smart TV - Voice Recognition and Content Discovery'' published by John Archer on 26th of June 2013 available at: http://www.trustedreviews.com/lg-smart-tv-review-voice-recognition-and-recommendations-page-2

- ''EU issues ultimatum on internet privacy behavioral targeting investigated'' published by Christopher Williams on 31st of March 2009available at: http://www.theregister.co.uk/2009/03/31/kuneva_behavioural/

- ''Some Caveats on Profiling'' edited by Serge Gutwirth and Mireille Hildebrandt in the book Data Protection in a Profiled World published by Serge Gutwirth, Yves Poullet, Paul de Hert in 2010, available at:http://www.newbooks-services.de/mediafiles/texts/2/9789048188642_excerpt_001.pdf

- ''Netherlands Smart TV's in Breach of Dutch Data Protection Act'' published by RadeObradović in 2013 available at: http://merlin.obs.coe.int/iris/2013/9/article21.en.html

- ''Collecting personal data via smart TVs violates Dutch Data Protection Act'' published by Friederike van der Jagt on 7th of February 2014 available at: http://www.lexology.com/library/detail.aspx?g=dd89be0a-bdf0-41ad-962b-84a0abbdb0d5

- Smart TV definition in Wikipedia available at: https://en.wikipedia.org/wiki/Smart_TV

- Report of ''The Internet of Things: Privacy and Security in a Connected World'' Workshop hosted by FTC on 19 November 2013

- ''IoT Privacy, Data Protection, Information Security'' published by European Commission available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753

- ''Big Data and smart devices and their impact on privacy'' published by DIRECTORATE GENERAL FOR INTERNAL POLICIES POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS published in September 2015, available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf

- ''What Is a Smart TV & Do You Need One? [MakeUseOf Explains]''published by James Bruce on 9th of January 2013 available at: http://www.makeuseof.com/tag/what-is-a-smart-tv/

- ''Privacy considerations of online behavioural tracking'' published by ENISA on 14th of November 2012, available at: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking

- ''Encryption Needn't Be An Either/Or Choice Between Privacy and National Security'' published by John Chen - Executive Chairman and CEO at BlackBerry on 21th of January 2015 available at:https://www.linkedin.com/pulse/you-can-balance-privacy-national-security-heres-how-john-chen?trkInfo=VSRPsearchId%3A1283793021455802136676%2CVSRPtargetId%3A5963629768090931200%2CVSRPcmpt%3Aprimary&trk=vsrp_influencer_content_res_name

- ''A Message to Our Customers'' published by Tim Cook on 16th of February 2016 available at: http://www.apple.com/customer-letter/

- ''Why George Orwell would never buy a Smart TV by Samsung'' published by KHADIJA KHAN on 16th of February 2015, available at:http://www.theplaidzebra.com/george-orwell-never-buy-smarttv-samsung/

- ''Say cheese! Privacy and facial recognition'' published by Ben Buckley, Matt Hunter (Linklaters LLP) in 2011 available at: http://ac.els-cdn.com/S0267364911001567/1-s2.0-S0267364911001567-main.pdf?_tid=68f7016e-c047-11e5-90ba-00000aab0f26&acdnat=1453385044_fef44766d048fa3280d5a93155753cb9

- ''The Convergence of Virtual Reality and Social Networks – Threats to Privacy and Autonomy'' published by O'Brolcháin, Fiachra; Jacquemard, Tim; Monaghan, David; O'Connor, Noel; Novitzky, Peter; Gordijn, Bert in Science & Engineering Ethics; Vol. 22 Issue 1, in February 2016, available at: http://connection.ebscohost.com/c/articles/112358475/convergence-virtual-reality-social-networks-threats-privacy-autonomy

- ''Samsung Global Privacy Policy – Smart TV Supplement'' available at: http://www.samsung.com/uk/info/privacy-SmartTV.html

- ''Oops- We didn't mean to do that-How Unintended consequences can hijack good privacy and security policies'' published by Thomas P. Kenan in August 2010 under ''Privacy and Identity Management for Life'' edited by Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes, Ge Zhang

- ''Hearing Minutes Before the Subcommittee On Privacy Technology and The Law of The Committee On The Judiciary United States Senate'' - Opening Statement Of Hon. Al Franken, A U.S. Senator From The State Of Minnesota, available at:https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf

- ''Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment'' published by Cavoukian, A., Chibba, M., &Stoianov, A. - Review Of Policy Research29(1in 2012

- ''Samsung rejects concern over 'Orwellian' privacy policy'' published by Alex Hern on 9th of February 2015 available at: http://www.theguardian.com/technology/2015/feb/09/samsung-rejects-concern-over-orwellian-privacy-policy

- ''Internet of Things IoT Governance, Privacy and Security Issues'' published by EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS in January 2015 available at: http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf

- ''Samsung's voice-recording smart TVs breach privacy law, campaigners claim'' composed by Samuel Gibbs and published in the Guardian on 27 February 2015 available at: http://www.theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim

- ''Online Tracking and Behavioral Profiling'' published by Electronic Privacy Information Center available at: https://epic.org/privacy/consumer/online_tracking_and_behavioral.html

- ''Disable this feature to stop your Samsung Smart TV from listening to you'' published by Dan Graziano on 10th of February 2015 available at: http://www.cnet.com/how-to/samsung-smart-tv-spying/

- ''Smart TV's in Breach of Dutch Data Protection Act'' published by RadeObradovićInstitute for Information Law (IViR), University of Amsterdam available at: http://merlin.obs.coe.int/iris/2013/9/article21.en.html

- Chairman of ARTICLE 29 WORKING PARTY, Jacob Kohnstamm's statementon 25 January 2012 available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2012/20120125_pr_dp_proposals_en.pdf

- European Commission press release on 25 January 2012 related to comprehensive reform of the data protection rules available at:http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

- ''General Data Protection Regulation: Document pool'' https://edri.org/gdpr-document-pool/

- European Commission press release on 15 December 2015 on agreement on ''Commission's EU data protection reform will boost Digital Single Market'' available at: http://europa.eu/rapid/press-release_IP-15-6321_en.htm

- ''Threat Landscape and Good Practice Guide for Smart Home and Converged Media'' published by ENISA on 1st of December 2014, available at: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-for-smart-home-and-media-convergence

- European Data Protection Supervisor - definition of data minimization available at: https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74

- Approach of European Digital Rights to Data minimization available at: https://edri.org/files/04-minimisation.pdf

- Comments on ''Future of Privacy Forum'' held on November 19, 2013 available at: https://fpf.org/wp-content/uploads/FPF-IoT-Comments_January-2014.pdf

- ''Big Data for All: Privacy and User Control in the Age of Analytics'' published by Tene, Omer and Polonetsky, Jules, on 20th of September 2012. Northwestern Journal of Technology and Intellectual Property 239 (2013) available at SSRN: http://ssrn.com/abstract=2149364

- ''Top 10 operational impacts of the GDPR: Part 3 – consent'' published by Gabriel Maldoff on 12th of January 2016 available at: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/

- ''Customer Centric Marketing in the European Union from a Legal Perspective'' written by Eleni Tzoulia published in Handbook of Research on Managing and Influencing Consumer Behavior'' Chapter 4,
- ''On Decision Transparency, or How to Enhance Data Protection after the Computational Turn'' published by Koops, Bert-Jaap on 1st of September 2013 available at SSRN: http://ssrn.com/abstract=2367510
- ''Data Protection Within Digital Economy'' published by Deloitte in 2015 available at: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-data-protection-within-digital-economy-102015.pdf
- ''What Control do I have'' published by TRUSTe available at: https://www.truste.com/consumer-privacy/about-oba/#&panel1-2
- Definition of Privacy By Design by ''Information and Privacy Commissioner of Ontario''available at: https://www.ipc.on.ca/english/privacy/introduction-to-pbd/
- ''Privacy by design: delivering the promises'' published by Peter Hustinx, Identity in the Information Society, 2010, Volume 3, Number 2, available at: http://link.springer.com/article/10.1007/s12394-010-0061-z
- European Commission press release ''Privacy Enhancing Technologies (PETs)The existing legal framework'' published on 2nd of May 2007 available at: http://europa.eu/rapid/press-release_MEMO-07-159_en.htm
- ''UK: Pseudonymisation: The Benefits And Getting Regulation Right'' published by Victoria Hordern on 17th of March 2014 available at:http://www.mondaq.com/x/300206/Data+Protection+Privacy/Pseudonymisation+The+Benefits+And+Getting+Regulation+Right
- ''Transparency enhancing tools (TETs): an overview'' published by Milena Janic, Jan Pieter Wijbenga, Thijs Veugen from TNO Delft University of Technology,Delft, The Netherlands in 2013, available at:http://quantum.ewi.tudelft.nl/sites/defauPlt/files/TETs%20paper%20STAST2013.pdf
- ''Marrying Transparency Tools with User-Controlled Identity Management'' published by Hansen, M. in 2008 In The Future of Identity in the Information Society. (Springer US),
- ''A Categorization of Transparency-Enhancing Technologies'' published by Christian Zimmermann from Institute of Computer Science and Social Studies University of Freiburg in 2015 available at: http://arxiv.org/ftp/arxiv/papers/1507/1507.04914.pdf
- ''Privacy dashboard'' published by Nick Doty on 2nd of August 2011 available at: https://github.com/mohit/privacypatterns/wiki/Privacy-dashboard
- ''Because we care: Privacy Dashboard on FirefoxOS'' published by Marta Piekarska, Dominik Strohmeier, Yun Zhou, Alexander Raake in 2015 available at: http://ieee-security.org/TC/SPW2015/W2SP/papers/W2SP_2015_submission_28.pdf
- ''What are privacy seals?'' published by Information Commissioner's Office available at: https://ico.org.uk/for-organisations/improve-your-practices/privacy-seals/

- ''EU Privacy seals project Inventory and analysis of privacy certification schemes'' published by The Institute for the Protection and Security of the Citizen of the Joint Research Centre in 2013 available at: http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf
- ''Privacy Seals and Privacy Snake Oil'' published by Toby Stevens on 19th of November 2014, available at:http://www.computerweekly.com/blogs/the-data-trust-blog/2014/11/privacy-seals-and-privacy-snak.html
- ''Definition of EuroPrise'' published by European Privacy Seal available at: https://www.european-privacy-seal.eu/EPS-en/Vision
- Statement of TrustE related to privacy concerns available at: https://www.truste.com/business-products/trusted-websites/
- ''Direct Marketing Guidance'' published by Information Commissioner Officer, available at: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf
- ''Managing Consumer Trust in Intercultural E-Commerce Transactions'' published by Ray, Jeffrey S. on 26th of November 2011, available at SSRN:http://ssrn.com/abstract=2110349 or http://dx.doi.org/10.2139/ssrn.2110349
- ''Consumer Confidence In Privacy Online Is Decreasing'' published by Trisha Leon on 16th of July 2014 available at: http://www.bsminfo.com/doc/consumer-confidence-in-privacy-online-is-decreasing-0001
- About Smart TV Alliance available at: http://smarttv-alliance.org/
- Mission of European Consumer Organisation BEUC available at: http://www.beuc.eu/about-beuc/mission