IRIS Special

Published by the
European Audiovisual Observatory

Smart TV and data protection

EUROPEAN AUDIOVISUAL OBSERVATORY

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS *Special*
Smart TV and data protection

European Audiovisual Observatory, Strasbourg 2016
ISBN 978-92-871-8239-5
EUR 49

Director of publication – Susanne Nikoltchev
Executive Director, European Audiovisual Observatory

Editorial supervision – Maja Cappello
Head of Department for legal information, European Audiovisual Observatory

Editorial team – Francisco Javier Cabrera Blázquez, Maja Cappello, Sophie Valais
European Audiovisual Observatory

Authors – Britt van Breda, Nico van Eijk, Kristina Irion, Tarlach McGonagle, Sander van Voorst
Institute for Information Law (IViR), University of Amsterdam

Editorial assistant – Olivier Mabilat, Snezana Jacevski, European Audiovisual Observatory

Marketing – Markus Booms, markus.booms@coe.int, European Audiovisual Observatory

Press and Public Relations – Alison Hindhaugh, alison.hindhaugh@coe.int, European Audiovisual Observatory

Translators / Proof-readers – Aurélie Courtinat, Johanna Fell, Julie Mamou, Maco Polo Traductions, Stefan Pooth, Roland Schmid, Sonja Schmidt, Lucy Turner, Anne-Lise Weidmann

Publisher
European Audiovisual Observatory, 76, allée de la Robertsau F-67000 Strasbourg, France
Tél. : +33 (0)3 90 21 60 00, Fax : +33 (0)3 90 21 60 19
E-mail: info.obs@coe.int, www.obs.coe.int

Contributing Partner Institution
Institute for Information Law (IViR), University of Amsterdam, Vendelstraat 7, 1012 XX Amsterdam, The Netherlands
Tel: +31 (0) 20 525 3406, Fax: +31 (0) 20 525 3033
E-mail: ivir@ivir.nl, www.ivir.nl

Cover layout – P O I N T I L L É S, Hoenheim, France

Please quote this publication as:
Cappello M. (ed.), *Smart TV and data protection*, IRIS Special 2015-2, European Audiovisual Observatory, Strasbourg, 2016

A publication of the European Audiovisual Observatory

Smart TV and data protection

Britt van Breda

Nico van Eijk

Kristina Irion

Tarlach McGonagle

Sander van Voorst

EUROPEAN AUDIOVISUAL OBSERVATORY

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Foreword

A man walks through a shopping centre. His eyes are flashed by a multitude of cameras equipped with eye-recognition software. Immediately the shop windows start to show on flashy screens advertising specially tailored to him…

This is obviously a scene taken from a science-fiction film (Steven Spielberg's "Minority Report"). However, it is not so far away from what we can experience today. In the age of the Internet, connected TV sets and "second screens", the possibilities of obtaining personal data of media users – in both legal and illegal ways – have multiplied exponentially. Such data is a very important commodity for advertisers, which can be used to provide individually targeted ads on online services and on various kinds of connected devices. Furthermore, personal data obtained via search engines, social media and connected devices can be used as a means to provide a better experience for the user of an online service.

However, the obtaining and use of personal data by third parties, whether provided willingly or inadvertently by the users, can also have a very intrusive effect on their personal lives. Moreover, there are situations in which the insight into a user's life exceeds what a user is prepared to accept.

This becomes particularly evident in the case of audiovisual consumption through Smart TVs, which are becoming a common equipment in our homes. Their worldwide presence has doubled from 2011 to 2015, and their average penetration will soon reach the majority of European households.

According to a very general definition, a Smart TV is a TV that possesses a variety of connective capabilities, including in any case an internet connection. When connected, these devices are able to collect a variety of information about their users, including social backgrounds and financial profiles, which can be used to influence online user behaviour for direct marketing purposes or for the profiling of the users for advertising activities. Their functions include voice and facial recognition, motion sensing, account creation and many other interactive capabilities.

Considering the constant substitution process of traditional broadcasting with non-linear interactive (and smart) consumption of audiovisual content, it becomes more and more important to have adequate tools capable of ensuring an effective balance between the providers' wish to optimise their offers and give recommendations based on the personal choice of the users and the increased need to protect the latter against the risk of reduction of choice, information isolation and, in the worst cases, manipulation.

The current regulatory framework in this domain is particularly scattered and includes a variety of sources: a special media regulation in the audiovisual media services directive; sector-specific rules in the e-communications framework, the e-commerce directive and the e-privacy directive; a general privacy framework in the data protection directive and the general data protection regulation; and an umbrella regulation including the consumer protection framework and the human rights dimension.

Against this multifaceted legal background, various interpretative issues are rising at national level as to the processing of personal data by Smart TV operators. This IRIS *Special*, which has been

written by the Institute of Information Law (IViR) of the University of Amsterdam, provides an overview of the specifics of Smart TVs compared with other forms of audiovisual media. It further examines the regulatory framework that governs them, before investigating four case-studies and reflecting upon the on-going regulatory reforms.

The developments we are already witnessing, which for instance include Smart Homes equipped with family hub refrigerators and Smart Things such as connected healthcare belts, seem indeed to require an integrated perspective where all issues are consistently dealt with. This also becomes important from an institutional point of view, where a coordination between the various public actors is probably more necessary than ever. These issues are being addressed, among others, by the new General data protection regulation on which an agreement was reached between the Council, the Parliament and the Commission on 15 December 2015.[1]

This publication gives a first insight into the outcome of this long-lasting decision making process, which started in 2012. Its draft also contributed to setting the scene for a workshop organised by the Observatory on 11 December 2015 in Strasbourg, entitled "The grey areas between media regulation and data protection"[2], which discussed, among other things, the challenges that the various stakeholders – media regulators, data protectors, industry, media service providers and consumers – are currently facing. The issues at stake deserve well-informed participation, and the following chapters are intended to contribute an outline of the main questions concerning the interactive consumption of audiovisual content. More will certainly have to follow.

Strasbourg, January 2016
Maja Cappello
Head of the Department for Legal Information
European Audiovisual Observatory

[1] See http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-data-protection/.

[2] See http://www.obs.coe.int/workshops/-/asset_publisher/kNG5qM2wH8Kq/content/dli-workshop-obs-epra-the-grey-areas-between-media-regulation-and-data-protection.

Table of contents

Acronyms and Abbreviations

API	Application Programming Interface
AVMS	Audiovisual Media Services
BCRs	Binding Corporate Rules
CBP	*College bescherming persoonsgegevens* (Dutch Data Protection Authority)
CCPA	(US) Cable Communications Policy Act
COPPA	(US) Children's Online Privacy Protection Act
DPD	Data Protection Directive (Directive 95/46/EC)
ECPA	(US) Electronic Communications Privacy Act
EPG	Electronic Programme Guide
EPIC	Electronic Privacy Information Center
FTC	(US) Federal Trade Commission
GDPR	General Data Protection Regulation
HbbTV	Hybrid Broadcast Broadband TV
IoT	Internet of Things
WBP	*Wet bescherming persoonsgegevens* (Dutch Data Protection Act)

Introduction

With the advent of various forms of interactive television, the dystopian predictions of authors like Aldous Huxley, Ray Bradbury and most famously, George Orwell, appear closer to contemporary reality than ever. Today, the underlying technology of the sinister 'telescreens' of *Nineteen Eighty-Four*, which receive and transmit simultaneously, can only be dimmed but never switched off, picking up every sound "above the level of a very low whisper" and capturing every movement within their fields of vision, is widely available and widely in use.[3]

Certain types of television ('smart TVs') are capable of responding to visual/motion and acoustic stimuli, like facial recognition/body movements and voices, respectively. The ability of smart TVs to collect, store and process personal information provided by their users, raises a gamut of privacy-related issues that are not dealt with in regulatory frameworks governing traditional forms of audiovisual media. This study[4] examines the role of privacy-related regulation in the audiovisual media sector, with particular emphasis on smart TV.

In the past, televisions were unwieldy appliances in the corner of the living room and not much more than 'lights and wires in a box', as Ed Murrow once famously put it.[5] Technologies and markets later advanced to embrace more portable, lighter and flat-screen models, but the basic concept remained the same: televisions were devices that received broadcast signals and displayed programmes on their screens. The signals were sent from point-to-multipoint and the relationship between viewers and their television sets was one-directional. The privacy of viewers was, in consequence, simply not an issue in media law and policy.

It is only very recently, with the accelerated emergence of interactive televisions, which have changed the relationship between viewers and their television sets into a bi-directional one, that privacy-related concerns have begun to make their way onto the agendas of media law- and policy makers. This sea change is due first and foremost to the existence of interactive capacities in television sets, but also to a slow but sure public sensitisation to privacy-related issues generally.

'Connected TV', 'hybrid TV', and 'smart TV' are all largely synonymous terms used to describe interactive televisions. Essentially, they all refer to television sets – or the combination of televisions and similar technology in 'set top boxes' - which integrate the ability to watch linear television, while also offering the enhanced value of being able to use additional services delivered via an Internet connection. 'Connected', then, refers to the Internet connection that enables viewers (who are now better described as users) to avail themselves of the additional services. 'Hybrid' refers to the converged nature of the technology: a hybrid of a television and a computer. 'Smart' is a term with obvious commercial/marketing appeal, which seeks to distinguish these televisions from their less intelligent forerunners. The term 'smart TV' is used consistently throughout this study.

---

[3] Orwell G., "Nineteen Eighty-Four", in Orwell G., *The Complete Novels*, London, Penguin, 2000, pp. 743-744.

[4] The authors are very grateful to Natali Helberger for her valuable comments on a draft version of the study and to Patrick Leerssen for his valuable translation assistance.

[5] Murrow E.R., "Wires and Lights in a Box" Speech, Radio Television News Directors Association Convention, Chicago, 15 October 1958, http://www.rtdna.org/content/edward_r_murrow_s_1958_wires_lights_in_a_box_speech.

If it is not connected to the Internet or its additional functionalities have not been activated, a smart TV remains for all intents and purposes a traditional TV, permitting users to view programmes in linear fashion. That, however, defeats the purpose of having such additional technological capabilities. Smart TV offers access to a range of Internet-based services, such as web browsing, video-on-demand, social networking and the use of apps. In addition to viewing they provide the possibility for the user to engage in transactions.

Ian Walden and Lorna Woods have provided a very useful diagnosis of privacy-related concerns arising from the capabilities of smart TV sets. They point out that "the current broadcasting environment gives rise to two privacy concerns in two key areas":

> *"the enhanced ability to monitor and measure our broadcasting consumption patterns, particularly valuable for profiling and marketing purposes; and the possibility of surveillance over, or interception of, the content we are viewing".*[6]

To these concerns one could readily add similar concerns about the monitoring, measuring and surveillance of our patterns of consumption of information and non-broadcast content through our other online activity via the smart TV set. A further concern has to do with the ability of smart TV sets to collect and process personal data through various features such as voice and facial recognition. The processing of such data typically involves sharing that data with various third parties, which creates additional complexity from a privacy perspective.

More generally, the smart TV 'ecosystem' involves a number of different players which, one way or another, acquire access to information about users' consumption of broadcast content and online activities, as well as users' personal data. The ecosystem comprises the smart TV manufacturer, provider of so-called Hybrid Broadcast Broadband TV (HbbTV) services, portal operator, app store operator, app provider, recommendation services provider.[7] Altogether, the use of smart TVs represent a vastly more complex value chain than traditional television services due to the number of players involved, but also due to complex issues linked to distribution.[8]

The involvement of so many different actors gives rise to fears about "multiveillance" – the phenomenon of "surveillance not just by the state, but by companies, marketers, and those in our social networks".[9] Again, as Walden and Woods put it: "A range of actors in the delivery chain have the potential to monitor viewers' consumption of broadcast content and these relationships may not be transparent, nor the parties' respective commitments clear and understood, not least from the viewer's perspective".[10]

Structure

The structure of this study is built around a number of questions:

- What is smart TV?
- How does smart TV compare with other forms of audiovisual media?

[6] Walden I. and Woods L., "Broadcasting Privacy", *Journal of Media Law,* 2011, 3(1), pp. 117-141, at 121.

[7] Düsseldorfer Kreis, *Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste*, German Guidelines adopted on 15-16 septembre 2015, https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/OH_Smart_TV_v1.0.pdf., p. 9.

[8] Nooren P., Leurdijk A., van Eijk N., "Net neutrality and the value chain for video", *info*, 2012, Vol. 14 ss: 6, pp. 45 – 58, http://www.ivir.nl/publicaties/download/511.

[9] Richards N., *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, New York, Oxford University Press, 2015, p. 5.

[10] Walden I. and Woods L., "Broadcasting Privacy", *op.cit.*, footnote 6, at p. 140.

- What regulatory frameworks govern smart TV?
- What guidance can be found in selected country-specific case studies?
- What are the dangers associated with the collection, storage and processing of private user information by commercial parties?
- How are relevant regulatory frameworks likely to evolve?

Chapter I explores the different terminological and definitional approaches to 'smart TV' and thereby positions it in relation to other forms of (interactive) audiovisual media. It identifies the main distinctive features of smart TV (for privacy-related/data protection purposes) as: speech recognition, motion sensing, facial recognition, interactive capacity (e.g. via apps and social media) and integrated user accounts (e.g. Samsung). These features of smart TV facilitate the collection, storage and processing of personal information by commercial parties. These features then serve as key focuses for the exploration of the regulatory framework and case studies in subsequent chapters.

Chapter II explains how audiovisual media regulation and privacy/data protection regulation have traditionally developed in isolation from one another. Convergence and the emergence and expansion of intelligent technologies are forcing regulators in both sectors to find each other and pursue new regulatory approaches that reflect and address these developments. This chapter examines the lack of relevance of the AVMSD; the limited relevance of the Framework and Access Directives; the growing relevance of the Data Protection and E-Privacy Directives, and the likely implications of the (draft) General Data Protection Regulation. It also explains the relevance of consumer law and human rights law.

Building on the analysis of the complex regulatory framework, **Chapter III** offers an overview of how relevant legal issues are arising and being dealt with in practice at the national level. Four case studies form the core of the chapter, drawing on experiences in Germany, the Netherlands (two case studies) and the United States:

1) Germany: Joint position, technical test of smart TVs and guidance document;
2) The Dutch Data Protection Authority's investigation into the processing of personal data with or through Philips smart TV by TP Vision Netherlands;
3) The Dutch Data Protection Authority's investigation into the processing of personal data by Ziggo relating to of interactive digital services;
4) Electronic Privacy Information Center v. 'Samsung': Complaint to the US Federal Trade Commission about the routine interception and recording by Samsung of private communications of consumers in their homes.

Each of the case studies involves a detailed analysis of the legal issues involved and their broader implications for regulatory approaches to smart TV.

Chapter IV builds on the preceding chapter and, while reflecting on future regulatory developments (in particular the likely implications of the draft General Data Protection Regulation), focuses on the distinctive features of smart TV as identified above, and the (potential) harms that arise from the collection, storage and processing of personal data, as enabled by those technological features.

The study will be completed by a concluding analysis.

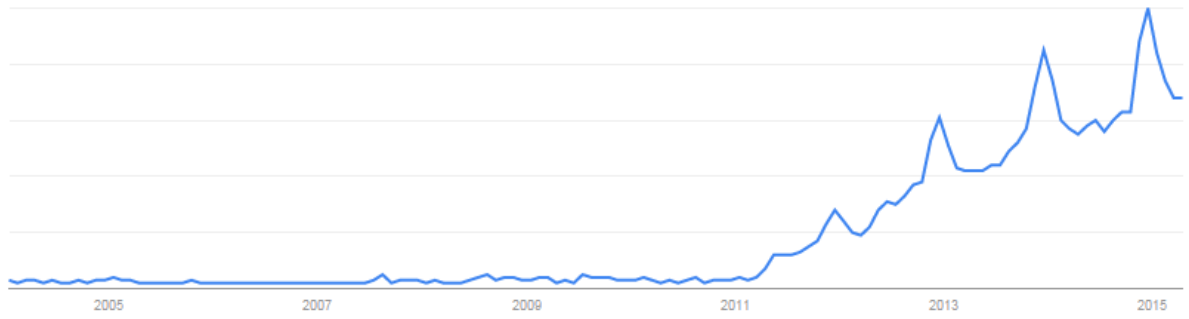
1. Definitions and Features

Smart TVs are becoming an increasingly popular feature of households throughout Europe, which in turn is increasing the public's familiarity with the concept. The term 'smart TV' rightly suggests similarity to the term 'smart phone', but smart TVs have yet to achieve the same level of uptake as their telephonic cousins.

1.1. What is a smart TV?

Use of the term 'smart TV' really started to gain ground in 2011, as can be demonstrated with historical data of Google search terms (see figure 1).[11]

Figure 1: Historical graph of Google searches for the term 'smart TV'



Source: Google trends

The term has not yet been included in the Oxford English Dictionary, but a commonly used definition is 'a television that can connect to the Internet'. Other definitions emphasize the capacity to use certain 'apps', including those provided by third parties.[12]

A basic definition could draw on a comparison with ordinary ('dumb') televisions. These devices are little more than a screen. All the internal parts are aimed at displaying content that is provided through external sources such as antennas, cables, SCART or composite video. The same is true for mobile phones. An ordinary mobile phone has no other function than the transmission of speech via the mobile network. Advanced models were capable of establishing a rudimentary Internet connection via GPRS. However, they were not included under the concept of smart phones.

[11] Online via www.google.nl/trends.

[12] Kovach S., "What is a smart TV?", *Business Insider*, 8 December 2010, http://www.businessinsider.com/what-is-a-smart-tv-2010-12?IR=T.

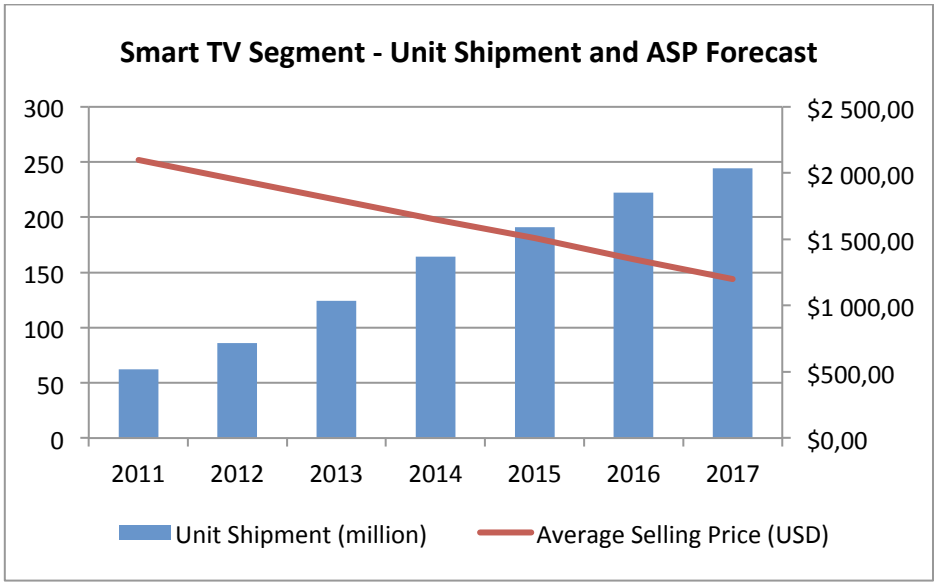
A smart TV, just like an ordinary television, has the capacity to display content via the external sources listed above. Additionally, there are other methods of connecting to such a TV. Thus, most smart TVs are equipped with Ethernet, WIFI, USB and Bluetooth. Again, the comparison with smart phones is readily made. These communication channels bring the possibility of connecting not only to local sources in the TV's immediate surroundings, but also to other peripherals without regard to physical distance. In this manner, TVs are set to become an important element of the Internet of Things (IoT).

Returning to the definition based on the possibility of running apps, it should be noted that ordinary TVs are also capable of running rudimentary programmes. What distinguishes smart TVs, then, is an operating system that is designed to provide a platform for apps from various developers. Furthermore, smart TVs generally possess a degree of computational power, which enables them to execute far more complex programmes than ordinary 'dumb' TVs. One could say that the entire architecture of the smart TV hinges on this function, in addition to displaying images through external sources.

In light of the above, the following description or working definition is proposed for the purposes of this report: 'A smart TV is a TV that possesses a wide variety of connective capabilities, including in any case an Internet connection. In addition, the TV must have an operating system designed to provide content through apps, primarily via the Internet. This makes the smart TV suited to watching non-linear television and enables the user to access personally selected content at a time of his or her choosing.'

Further insights into the current market situation and projected market growth are provided by the following tabular overviews, focusing on different market-related aspects:

Figure 2: Global Smart TV shipment 2011-2017

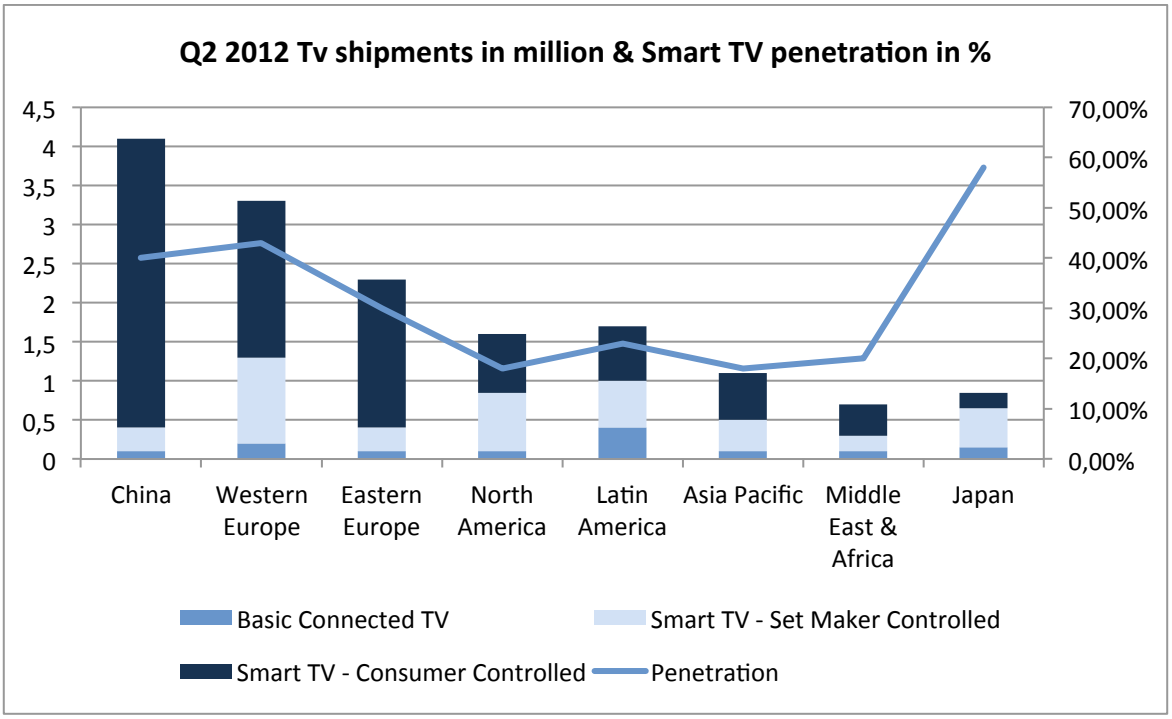


Note: All figures are rounded. The base year is 2012.

Source: Frost & Sullivan

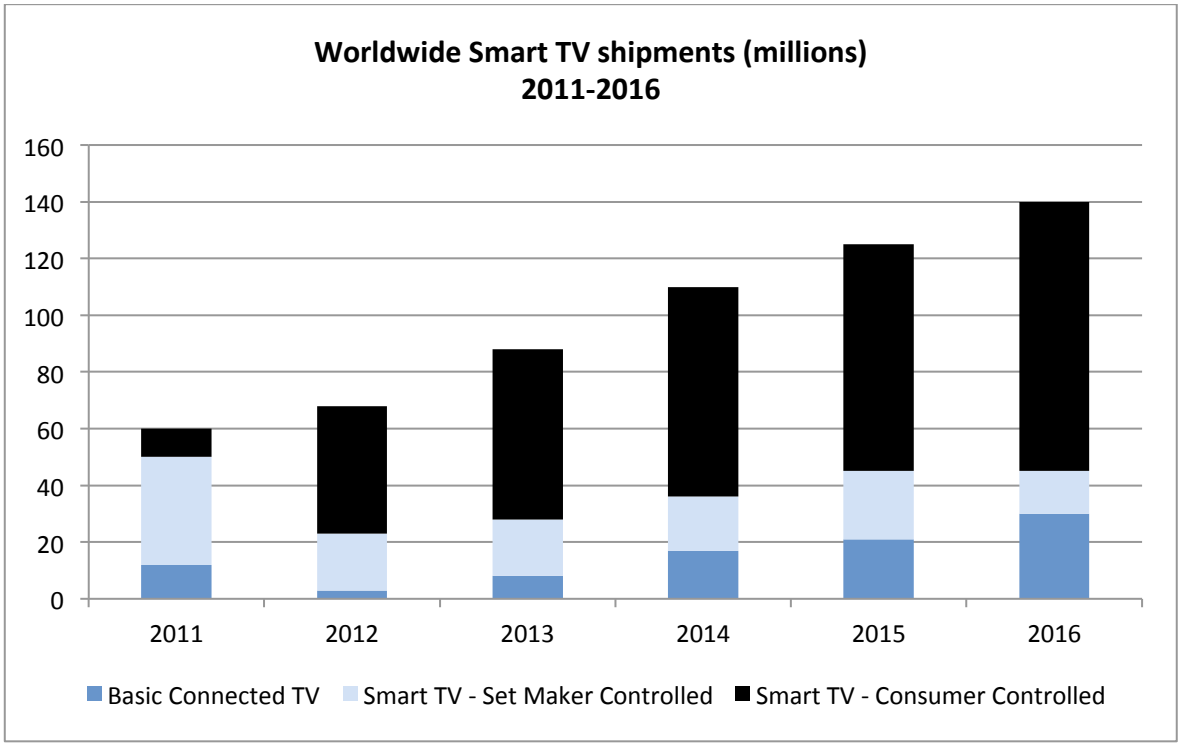
As Figure 2 demonstrates it, from another source (Frost & Sullivan), Smart TV shipment are expected to rise over the coming years and as always with a "new" technology, the average selling price will continuously decrease.

Figure 3: Q2'12 Smart TV Shipments by Region (000s)



Source: NPD DisplaySearch Quarterly Smart TV Shipment and Forecast Report

Figure 4 Smart TV Shipment Forecast 2011-2016



Source: NPD DisplaySearch Quarterly Smart TV Shipment and Forecast Report

Figures 3 and 4 give an overview of how the internet connectivity of Smart TVs is controlled. The clear tendency is towards Smart TVs with user controlled browsers. In fact, consumers want to be able to browse freely the web in order to find content (mainly video content) that suites their tastes. "Consumer Controlled" Smart TVs allow this as opposed to "Set Maker controlled" TV sets where the consumer has to evolve on the platforms designed by the constructor.

Table 1: Global connected TV device installed base (million units)

Q2 14 Rank	Vendor	Q2 14	Q2 13	Q2 14 Share	Q2 14 Installed base growth (YoY)
1	Sony	123.8	96.8	24.8%	27.9%
2	Samsung	62.3	34.4	12.5%	80.9%
3	Nintendo	56.8	67.5	11.4%	-15.8%
4	Microsoft	55.4	53.8	11.1%	2.9%
5	LG	32.2	16.0	6.5%	101.9%
6	Panasonic	29.9	19.6	6.0%	52.4%
7	Apple	18.7	13.0	3.8%	44.7%
8	Sharp	15.0	9.8	3.0%	52.7%
9	Toshiba	10.2	5.1	2.0%	98.8%
10	Philips	9.7	5.7	1.9%	70.0%
11	Roku	8.3	5.5	1.7%	51.9%
12	Google	6.0	0.0	1.2%	na

Note: Connected TV devices include smart TVs, smart Blu-ray players, games consoles and digital media streamers

Source: Gartner, Global Connected TV Device Tracker: Q2 2014

1.2. What data can a smart TV collect?

Having established a working definition for smart TV, it is useful to proceed to describe in greater detail the technical features of (a majority of) smart TVs. The description is based on an average Samsung model.[13] With a global market share of 29%, Samsung is the leading company in the world.[14] This particular television is equipped with a so-called SMART-hub, the 'heart' of the device which provides access to many kinds of apps and other smart-functions.[15]

[13] The Samsung UE40F6320, which exhibits most of the characteristics found in the current market, see: http://www.samsung.com/uk/consumer/tv-audio-video/televisions/hd-tvs/UE40F6320AKXXU.

[14] See https://technology.ihs.com/548718/tv-shipments-post-largest-annual-decline-in-five-years-ihs-says.

[15] See "User's manual for Samsung UE40F6320", 2013, https://www.gebruikershandleiding.com/Samsung-UE40F6320/preview-handleiding-633110.html.

The various functions that this machine offers are outlined in the instruction manual. Under the header 'SMART-interaction' a number of functions are listed, including:

- Voice recognition
- Motion control
- Facial recognition
- Samsung account creation

Apparently, there are numerous ways to control the TV, as well as the possibility of creating an account. Although these functions undoubtedly improve the viewing experience, there are a few caveats to be made. As mentioned earlier, traditional television sets were little more than mere display screens. With smart TVs, it follows from these additional functionalities that the device includes a number of sensors; its 'eyes and ears'.

The following section will discuss these sensors and the data that they can collect. The emphasis will be on technical possibilities. Whether data collection is actually taking place in practice will not be discussed, as it would require entirely separate research. Occasionally, however, real-world examples will be referred to.

1.2.1. Voice recognition

In order to receive voice commands, the smart TV must be equipped with a microphone that can record sound from the surroundings of the device. The term 'voice recognition' indicates that the TV is not merely able to record sound, but also to filter this data and to translate it into commands. In principle, it is therefore possible that the TV stores all words spoken near it, and searches them for possible commands. That this is not merely a hypothetical possibility is evidenced by the commotion surrounding a section of Samsung's smart TV terms and conditions, which made world news with the following clause:

> *"Please 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."*[16]

Samsung quickly changed this clause in response to this negative publicity, but the incident shows the very real possibility that smart TVs record more than one would realise at first instance. From the perspective of advertisers, this ability to literally and figuratively enter into private homes opens up a new world of marketing possibilities. These issues will be examined in more detail in the case study of the complaint of the Electronic Privacy Information Centre to the United States Federal Trade Commission in Chapter 3.

[16] Harris S., "Your Samsung SmartTV Is Spying on You, Basically", *The Daily Beast*, 2 May 2015, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html#.

1.2.2. Motion control and facial recognition

Besides recognising voice commands, the television can also respond to gestures. Additionally, users can log into the SMART-Hub by way of facial recognition.

These features require the television to be equipped with a camera. For the model in question, an external camera has been attached, although there are many models that include a built-in camera. This camera enables the television to record images, for example in order to enable voice-chat. As with voice recognition, further filtering is a possibility, which would allow the software to recognise and distinguish individual users' faces. This could provide insight into not only viewer counts for specific content, but also the identity of the persons involved or at least user profiles based on viewing behaviour.

1.2.3. (Samsung) Account

This category includes other miscellaneous data that technically could be collected, and could lead to the creation of 'profiles' (voluntarily or involuntarily).

One option for smart TV users is the creation of an account to which various data can be linked. These data might include content suggestions or recommendations based on viewing behaviour and advertisements based on viewing behaviour or response to earlier advertising. From the perspective of advertisers, the creation of an account by the user themselves is probably the most attractive option. The reasons for this preference will be discussed below.

In addition, data might also be collected without a user-created account. Quite similar to other interconnected devices, as soon as the TV is connected to the Internet, it is easy to create a profile based on viewing behaviour and to link it to the TV's IP address (which also reveals the TV's location). Viewing behaviour itself can comprise various factors, such as the viewed content and the identity of the viewer, as well as the time and duration of viewing (cf. the German case study in Chapter III). Naturally, the above can be avoided by not connecting the smart TV to the Internet. This effectively reduces the smart TV to a regular screen. This is an unlikely scenario due to the variety of attractive features that smart functions provide. The analogy with smart phones is readily made: without Internet, it is simply a phone with a number of apps that lose their functionality.

In light of the above, it can be concluded that a smart TV is primarily defined by the property that makes it part of the Internet of Things: an Internet connection. Furthermore, a powerful processor enables it to run various apps. Moreover, and in addition to the characteristics described in the definition at the start of this section, the smart TV is equipped with a number of sensors that allow it to observe its surroundings. This makes it capable of collecting all sorts of data and potentially sending them across the globe via the Internet. The fact that this can be done indiscriminately also means that the data of minors and visitors may be recorded.

It is the integration of all these functionalities in one single appliance that makes smart TV such a noteworthy development in the evolution of intelligent and interactive television. These functionalities – if they existed at all – were traditionally distinct and associated with distinct technologies, which in turn were governed by distinct regulatory regimes. One of the historical rationales for media regulation has been the media's ability to influence public opinion. The reach and impact of audiovisual media are often mentioned in this connection, and the US Supreme Court has referred famously to the 'uniquely pervasive presence' of television as a medium, which can be gauged *inter alia* by its ability to penetrate 'the privacy of the home', where the individual's right to

be left alone has pride of place.[17] This pronouncement was made in relation to a case (*F.C.C. v. Pacifica*) concerning the ability of offensive or indecent broadcast images to penetrate that most private of spaces – the family home. The technology that made such penetration possible – a simple 1970s television set - was uni-directional. Smart TVs, however, are of a different technological order. Their bi-directional capacities give a dramatically new meaning to the 'uniquely pervasive presence' of television.

[17] *Federal Communications Commission v. Pacifica Foundation*, 438 U.S. 726, at 748, https://supreme.justia.com/cases/federal/us/438/726/case.html.

2. Regulatory frameworks

As a new generation of converged end-user devices, smart TV's functions and the services it facilitates cut across different sector-specific frameworks at the EU level. The five sets of regulation that are triggered by smart TV are audiovisual media, electronic communications, data protection, consumer protection and human rights law. Each regulatory instrument has its unique aim and addresses different aspects of smart TV's operations. When mapping them out, consideration has to be given to how smart TV can be subsumed under their respective scope of application and to whom legal obligations are addressed from among the actors involved in the smart TV ecosystem.[18]

At the EU level, the regulatory division of labour can be summarised as follows: the AVMS Directive harmonizes a minimum set of provisions for linear audiovisual media services and on-demand audiovisual media services respectively ('graduated regulation').[19] The e-communications framework consisting of five directives covers electronic communications networks and services used for the conveyance of electronic signals, and associated facilities and services, and certain aspects of terminal equipment. In relation to smart TVs certain provisions of the Framework Directive[20] and the Access Directive[21] are of relevance, in particular regarding the technical features of digital television services, such as the application programming interfaces (APIs), the conditional access system, and the electronic programming guide, all of which are relevant for the access to and ultimately findability of content. Access to services is supported by regulation on network neutrality (in the Universal Service Directive).[22] The e-Privacy Directive,[23] which forms also part of the e-communications framework, introduces harmonized rules for the right to privacy with respect to the processing of personal data in the electronic communication sector. It particularizes and

[18] For a broader discussion of these issues, see generally: Hans-Bredow-Institut for Media Research and Institute for Information Law, Hermes: Study on the Future of European Audiovisual Regulation, Hamburg/Amsterdam, October 2015, http://www.ivir.nl/publicaties/download/1643.

[19] Directive 2010/13/EU of the European Parliament and Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32010L0013.

[20] Directive 2002/21/EC of the European Parliament and Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended by Directive 2009/140/EC and Regulation 544/2009, https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/140framework_5.pdf (unofficially consolidated version).

[21] Directive 2002/19/EC of the European Parliament and Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) as amended by Directive 2009/140/EC, http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/140access_1.pdf (unofficially consolidated version).

[22] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) as amended by Directive 2009/136/EC, https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Directive%202002%2022%20EC_0.pdf (unofficially consolidated version).

[23] Directive 2002/58/EC of the European Parliament and Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC, https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/24eprivacy_2.pdf (unofficially consolidated version).

complements the Data Protection Directive,[24] which applies to the processing of personal data in general. Some aspects of the e-Commerce Directive[25] and EU consumer protection law should be highlighted, such as the regulations pertaining to consumer contracts on digital content. Finally, the importance of human rights law should also be underscored.

In spite of the underlying regulatory division of labour this also poses challenges – as it will become apparent in this section - since these regulatory frameworks have traditionally developed in isolation from one another. Although they can apply jointly to smart TVs they are not fully cognizant of each other's aims and thus appear not to reinforce each other in an optimal way. Moreover, the competences for regulatory oversight and enforcement in the EU member states are correspondingly distributed over different authorities, each one in charge of implementing their own sector-specific regulation. With a few notable exceptions, there is little practice of information exchange and coordination between the national authorities across sectoral delineations, which can hamper the effective response to the cross-cutting regulatory challenges posed by smart TVs.

2.1. Audiovisual Media Services Directive

The centrepiece of EU regulation in the audiovisual media sector today is the AVMS Directive.[26] The Directive succeeds the 1989 TVWF Directive precisely as a response to converging media and transformations in media production, formats and distribution. The new notion of 'audiovisual media services' (Article 1(1)(a)) embraces well-known television formats and on-demand offers in edited content libraries. Notwithstanding that smart TVs can facilitate access to audiovisual media services - aside from online services in general - the AVMS Directive does not aim to regulate consumer equipment as such.[27] Manufacturers of smart TV equipment are not within the purview of the definition and fall outside its regulatory scope. Digital platforms operating via smart TVs are not *per se* excluded from the scope of application insofar as they offer audiovisual media services. Vertically-integrated operators which provide hardware and in addition access to audiovisual media services are common in the pay-TV market. They are consequently within the scope of application of the AVMS Directive. Such instances of vertical integration are, however, not yet commonplace in the smart TV market, where equipment manufacturers are traditionally not content producers.

However, the smart TV ecosystem includes the providers of audiovisual media services, such as television channels and on-demand catalogues of edited audiovisual media services who are regulated under the EU member states' laws pursuant to the AVMS Directive. With smart TVs the AVMS Directive may result in different regulatory requirements applying to audiovisual media content that is either linear or non-linear but delivered over the same screen.[28] The European

[24] Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012.

[25] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market,

http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031.

[26] AVMS Directive, *op. cit.*, fn 19.

[27] Technical standards and interoperability are outside the scope of the AVMS Directive.

[28] Cf. Wagner C., "Connected TV: A challenge for market players and regulators", *Global Media & Communications Quarterly,* Spring issue 2012,

http://www.hoganlovells.com/files/Publication/41c5d3e3-0a16-4784-80c0-09193994456c/Presentation/PublicationAttachment/5fc8d47d-18e7-499a-8231-3b61f5067100/GMC_Quarterly_Summer_2012_v2.pdf; European Commission, Green paper - Preparing for a fully converged audiovisual world: Growth, creation and values, COM(2013) 231, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2013:0231:FIN.

Parliament resolution on connected TV observes in this regard that such "graduated regulation, which differentiates between television programmes […] and audiovisual media services on demand, will become less important in its existing form, although differently regulated information and communications services are available on one and the same device…"[29]

In most situations the smart TV is the hardware pillar of a digital platform which connects third parties, such as providers of audiovisual media service and other online content and services with its user base via its application programming interface and affiliated app store. As digital platforms however its providers are presently outside of the scope of application of the AVMS Directive. Layover ads whereby the digital platform provider plays-in his own advertising formats on smart TV's can serve as an illustration of the present limitations of the AVMS Directive.[30] Since the digital platform provider is not offering audiovisual media services itself, this new form of advertisement would presently escape the scope of application of the AVMS Directive even when layover ads are displayed in connection with third providers' audiovisual content. The European Parliament resolution on connected TV concludes that the AVMS Directive's "provisions do not yet reflect ongoing technological convergence" and may necessitate "expanding the concept of platforms" in the upcoming revision of the AVMS Directive and neighboring regulations, in particular the e-communications package.[31]

2.2. E-Communications Framework

The regulatory framework on electronic communications primarily addresses the infrastructure and transmission layer. It does not apply to the provision of content, to the exercise of editorial control over content, or to information society services that do not consist wholly or mainly in the conveyance of signals on electronic communications networks.[32] Since the 2002 reforms, the scope of application of the e-communications framework is technologically neutral and explicitly includes broadcasting networks and transmission services as well as consumer equipment used for digital television.[33] Since then, the Framework Directive and the Access Directive contain new rules on digital television services, which are eminently relevant to smart TVs. This development underscores the growing significance of the technical back-end of digital television services. In the following paragraphs, the focus is on the regulation of digital television services and its auxiliary services in the context of smart TVs.

The central instrument of the e-communications regulatory framework is the Framework Directive, which includes important definitions. Smart TVs would certainly meet the definition of 'enhanced digital television equipment' in Article 2 (o) of the Framework Directive covering inter alia "integrated digital television sets [which are] able to receive digital interactive television services". Digital platforms operating via smart TVs commonly include an application programming interface and electronic programme guides in addition to a conditional access system. Both conditional access systems and electronic programme guides (EPGs) are mentioned in Article 2 (ea) as categories of 'associated services'. Definitions are further provided for the 'conditional access system' (Article 2 (f)) and the 'application program interface (API)' (Article 2 (p)). The Framework Directive itself

[29] European Parliament resolution of 4 July 2013 on connected TV (2012/2300(INI)), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2013-329.

[30] European Commission, supra fn. 288.

[31] European Parliament, supra fn. 299.

[32] Framework Directive, supra fn. 20, Article 2 (c) and Recital (5) and (10).

[33] *Ibid*., Recital (8).

regulates the application programming interfaces (API) whereas the regulatory substance on conditional access systems and electronic program guides is in the Access Directive.

The API is fairly central for the interoperability between applications of broadcasters or service providers and the resources in the enhanced digital television equipment i.e., smart TVs for that matter. Article 18 of the Framework Directive requires member states to encourage open APIs in digital interactive television services and equipment in order to facilitate the interoperability of digital interactive television services. In particular, this is aimed at "providers of all enhanced digital television equipment deployed for the reception of digital interactive television services on interactive digital television platforms" (Article 18 (1)(b) of the Framework Directive). Proprietors shall be encouraged to make the application program interface available "on fair, reasonable and non-discriminatory terms, and against appropriate remuneration, [and make available] all such information as is necessary to enable providers of digital interactive television services to provide all supported services […] in a fully functional form" (Article 18(2) of the Framework Directive). However, as these are duties that are placed on the member states, the regulatory implication is not as strict as an obligation would be.

Article 2 (f) of the Framework Directive defines 'conditional access system' as meaning "any technical measure and/or arrangement whereby access to a protected radio or television broadcasting service in intelligible form is made conditional upon subscription or other form of prior individual authorization". The definition would include smart TVs that provide conditional access to protected television broadcasting services, such as pay-TV, but not if it concerns other protected content, such as non-linear audiovisual media services or other online services. In the context of smart TV's combined functionalities, "the distinction […] can be difficult and impractical".[34] Hence, only in relation to protected television broadcasting services, Article 6 (1) of the Access Directive incorporates the conditions listed in Annex 1 Part I for conditional access systems. The requirements prescribe, among others, that operators of conditional access services have to offer access to broadcasters on a fair, reasonable and non-discriminatory (FRND) basis. Likewise, proprietors of conditional access services when granting licences to manufacturers of consumer equipment, have to observe FRND-terms.

National regulatory authorities are empowered to impose similar access obligations vis-à-vis providers of APIs and EPGs in order to ensure the accessibility of digital radio and television broadcasting services for end-users (Article 5 (1) (b) in connection with Annex 1 Part II of the Access Directive). Moreover, national regulatory authorities can "impose obligations in relation to the presentational aspects of electronic programme guides and similar listing and navigation facilities" (Article 6 (4) of the Access Directive). Yet, manufacturers of smart TVs and associated digital platforms are also under no must-carry obligations for the transmission of specified radio and television broadcast channels and services to the public (Article 31(1) of the Universal Service Directive). The must-carry provision is specifically addressed to undertakings providing electronic communications networks used for the distribution of radio or television broadcast channels to the public.

Outside the limited scope of requirements for conditional access services, APIs and EPGs in connection with digital radio and television broadcasting services, the e-communications framework does not contain a general obligation on neutrality and access to FRND-terms[35] that would apply to smart TVs and their related digital platforms. In its Green Paper on Media Convergence, the European Commission highlighted that the abundance of online content can challenge the discovery of general interest content by users for various reasons e.g., excessive filtering and personalisation

[34] Helberger N., "Access to Technical Facilities in Digital Broadcasting", in: Castendyk O., Dommering E. and Scheuer A., *European media law,* Alphen aan den Rijn: Wolters Kluwer, 2008, pp. 1129-1150, 1135.

[35] FRAND stands for 'Fair, Reasonable and Non Discriminatory'. It is a common benchmark in telecommunications regulation.

mechanisms, business decisions of equipment manufacturers, and so forth.[36] The European Parliament Resolution on connected TV argues for the need to introduce "rules on findability and non-discriminatory access to platforms, for content providers and content developers as well as for users."[37]

The Internet backchannel that enables interactive smart TV-services is also subject to the net neutrality provisions in the E-communications Framework. The Framework Directive stipulates in Article 8(4) that Member States are to promote "the ability of end-users to access and distribute information or run applications and services of their choice." This is laid down in further detail in the Universal Service Directive, in which transparency is prescribed and regulators are given the possibility of intervening. Transparency means that users need to receive information on any procedures put in place by the undertaking to measure and shape traffic so as to avoid filling or overfilling a network link, and information on how those procedures could impact on service quality. Regulators are authorised to set minimum quality of service requirements on an undertaking or undertakings providing public communications networks in order to prevent the degradation of service and to prevent traffic over networks from getting delayed or blocked. This framework for net neutrality is under revision. New provisions are expected to further allow the prioritization of so-called specialised services. Also the provision of free services (zero rating) can be facilitated.[38]

2.3. Provisions on e-privacy and data protection

This section introduces the growing relevance of the EU data protection framework for the smart TV ecosystem. It should be borne in mind that in 2000, the EU institutions officially proclaimed the Charter of Fundamental Rights, which was accorded binding legal value in 2009 with the entry into force of the Lisbon Treaty.[39] The Charter codifies the fundamental rights of EU citizens to the protection of privacy (Article 7 of the Charter) and personal data (Article 8 of the Charter).

In its Green Paper, "Preparing for a fully converged audiovisual world: Growth, creation and values", the European Commission holds that "the processing of personal data is often the prerequisite for the functioning of new services, even though the individual is often not fully aware of the collection and processing of personal data."[40] Where applicable, personalisation of content, for example in the EPG and other portal services, "can benefit consumers and advertisers, but may depend on tools posing challenges for personal data protection."[41] In the smart TV ecosystem, users' personal data flows not just to the respective equipment manufacturer, the digital platform provider, and the audiovisual media service providers, such as TV channels and edited digital content libraries, but also to the online service providers. The processing of personal data, however, has to comply with member states' laws pursuant to the EU data protection framework.

The joint treatment of the e-Privacy Directive,[42] which is actually an instrument of the above described e-communications framework, and the general Data Protection Directive,[43] is justified

[36] European Commission, supra fn. 8.

[37] European Parliament, supra fn. 29.

[38] European Commission, press release, "Commission welcomes agreement to end roaming charges and to guarantee an open Internet", Brussels, IP/15/5265, 30 June 2015, http://europa.eu/rapid/press-release_IP-15-5265_en.htm.

[39] Charter of Fundamental Rights of the European Union, in connection with Article 6(1) of the Treaty on European Union (consolidated version, Lisbon Treaty), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[40] European Commission, supra fn. 40.

[41] *Ibid.*

[42] Supra fn. 23.

[43] Supra fn. 24.

against the background that the former sector-specific instrument particularises and complements the latter (Article 1 (2) of the e-Privacy Directive). Both instruments have as their aim the protection of "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" (Article 1 (1) of the Data Protection Directive and Article 1 (1) of the e-Privacy Directive, albeit confined to the electronic communication sector). At the same time, both are also internal market instruments that aim to ensure the free flow of personal data between Member States.

In the near future, the Data Protection Directive, which dates back to 1995, will be replaced by a modernised instrument. The EU legislator is in the process of adopting a new General Data Protection Regulation (GDPR) this year, which will fully harmonize the rules on the protection on personal data throughout the EU.[44] Hence, an outlook on the GDPR's regulatory impact on the processing of personal data in connection with smart TVs is offered at the end of this section and is used as a frame of reference in Chapter 4.

2.3.1. Scope of application

The Data Protection Directive applies to the processing of personal data by controllers established on the territory of a member state, or, when this is not the case, the controller for purposes of processing personal data makes use of equipment situated on the territory of a member state (Article 4 (1) (a) and (c) of the Data Protection Directive). Even though a fair number of smart TV equipment manufacturers are headquartered outside of the EU, most of them operate via local subsidiaries, which does not pose a problem for the territorial scope of application of the Data Protection Directive.

In the situation of non-EU based online services which users can potentially access via their interconnected smart TVs, there are two avenues to establish the territorial scope. Firstly, the CJEU has interpreted Article 4 (1) (a) of the Data Protection Directive to apply to controllers with an establishment situated in a member state whose activities are inextricably linked to the data processing activities of the controller.[45] Secondly, the Article 29 Working Party interprets installing cookies on end-users' terminal equipment as making use of equipment situated within EU territory.[46] Pursuant to these wide interpretations, the territorial scope of EU data protection law would cover most providers of online services via smart TV who process personal data of EU citizens.

2.3.2. General definitions and principles

The Data Protection Directive provides the definitions of 'personal data' and 'processing' which in turn triggers the material scope of application in Article 3 (1). It is also important to introduce the notion of the 'controller' who is liable to comply with member states' data protection laws pursuant to the directives, and the definition of 'consent'. The E-Privacy Directive incorporates these definitions from the Data Protection Directive (Article 2 of the E-Privacy Directive).

---

[44] The draft versions which are presently discussed in the trialog meetings between the Council, the European Parliament and the European Commission are available at http://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/en/pdf.

[45] CJEU, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD),* judgment of 13 May 2014, Case C-131/12*, paras 56, 60,* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131.

[46] Article 29 Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, adopted on 30 May 2002 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf.

2.3.2.1. Personal data

Pursuant to Article 2 (a) of the Data Protection Directive 'personal data' means "any information relating to an identified or identifiable natural person ('data subject')". The Article 29 Working Party, which assembles the competent data protection authorities of the member states and the EU, has issued guidance in the form of an opinion on the exact interpretation of each element of the definition of personal data.[47] In the context of smart TV, the following categories of personal data are most likely involved: user account information (where applicable), device identification numbers or other unique identifiers (including cookies), static or dynamic IP addresses, viewing and browsing habits (e.g. tracking of TV channel switches), individual user profiles, location data as well as motion control (where enabled).[48] Voice and facial recognition, which can be deployed by manufacturers of smart TVs and can be used for their digital platforms, process biometric data, which also qualifies as personal data.[49]

As long as this data can be linked to an identified or identifiable natural person, this constitutes personal data in the meaning of the definition of the Data Protection Directive. For example, individuals are identifiable by unique identifiers, and pseudonymisation does not destroy the link to an individual data subject. For that reason device identification numbers or other unique identifiers are also within the definition of personal data under EU data protection law. On the contrary, anonymized and anonymous data is no longer personal data and, thus, its processing is not covered by the EU data protection framework, except when the data is again applied to an individual. Still, the anonymisation of personal data has to comply with best practices in order to preclude the residual risk of identification.[50]

2.3.2.2. Processing

'[P]rocessing of personal data' covers "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" (Article 2 (b) of the Data Protection Directive). It is thus a fairly wide concept and any internal processing operation by a controller is likely to meet its definition. For the interference with the right to privacy and data protection and hence for the definition of processing, it does not matter if the information on the private lives concerned is sensitive or the processing of personal data has inconvenienced the individual concerned in any way or produced any harm.[51]

---

[47] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[48] This enumeration is informed by the case law in Chapter III below.

[49] Article 29 Working Party, Working document on biometrics, adopted on 1 August 2003, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf; Opinion 3/2012 on developments in biometric technologies, adopted on 27 April 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

[50] This is often overlooked, cf. Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[51] Cf. CJEU, *Österreichischer Rundfunk and Others* (Cases C‑465/00, C‑138/01 and C‑139/01), para. 75, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CJ0465; *Digital Rights Ireland and Seitlinger v Minister for Communications, Marine and Natural Resources* (C-293/12 and C-594/12) [2014] E.C.R. I-238, para. 33, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1446899221432&uri=CELEX:62012CJ0293.

2.3.2.3. Controller

'Controller' means "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" (Article 2 (d) of the Data Protection Directive). In the smart TV ecosystem there are potentially several controllers of the processing of users' personal data, such as the equipment manufacturer, the digital and app platform provider, audiovisual media service providers, and online content and service providers. In some instances their collaboration may render them joint controllers and in other instances they must be regarded sole controllers. Other service providers can be involved at the backend of a given service, such as a cloud storage provider or a speech recognition service, which are performing duties and "process personal data on behalf of the controller" (Article 2 (e) of the Data Protection Directive). These actors are called 'processors' in the data protection law's own terminology, provided they retain their subordinated function and do not determine by themselves new purposes and means of the processing personal data.

2.3.2.4. Consent

The data subject's consent is a central notion to legitimize the processing of personal data by the controller. 'Consent' is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Article 2 (h) of the Data Protection Directive). The processing of personal data can be based on the unambiguous consent of the data subject (Article 7 (a) of the Data Protection Directive) and in some cases an explicit consent would be prerequisite, e.g. for the processing of special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life (Article 8 (1), (2) (a) of the Data Protection Directive). When personal data is collected from the data subject the consent presupposes that the controller has provided the data subject with clear and comprehensive information as enumerated in Article 10 of the Data Protection Directive.

2.3.3. E-Privacy Directive

As a sector-specific instrument, the scope of the E-Privacy Directive is concerned with the processing of personal data in the electronic communication sector. The obligations flowing from the Directive are addressed to providers of publicly available electronic communications networks and public electronic communications services as defined in the above mentioned Framework Directive thus, excluding providers of content, and exercise of editorial control over content, and information society services. The Directive essentially regulates the rights of users and subscribers of electronic communications services (including legal persons), protects the confidentiality of communications, and lays down rules for the use of traffic and location data. As a result, the E-Privacy Directive addresses only a fraction of the stakeholders at a time, when the economic significance of digital services' personal data processing is steadily increasing.

Most provisions of the E-Privacy Directive do not apply to manufacturers of smart TVs and providers of digital platforms, nor do they apply to TV channels and providers of information society services delivered via smart TVs. By contrast, as operators of publicly available electronic

communications networks the broadcasting network operator, HbbTV-provider[52] (i.e., the back-channel) and TV cable operators would be bound by the E-Privacy Directive. Providers of public electronic communications services via smart TVs such as IP telephony or video chats would also be bound. There are only two exceptions from this rule, which apply in a horizontal fashion to all economic actors, notably the requirement of Article 5 (3) of the E-Privacy Directive on the storing of information and access to information already stored in the terminal equipment of a subscriber or user, which is better known as the cookie-rule, and the rules on unsolicited commercial communications (Article 13 of the E-Privacy Directive). Following Recital 8 of the Framework Directive smart TVs are covered under the e-communications regulatory framework as consumer equipment used for digital television and, hence, Article 5 (3) of the e-Privacy Directive applies:

> *Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*

Essentially, when placing cookies or beacons in smart TVs or accessing information that is already stored on the smart TV, the various actors of the smart TV ecosystem have to obtain the users' consent and comply with the information duties, as regulated in the Data Protection Directive. In other words, equipment manufacturers and other service providers have to display a privacy notice before storing cookies or accessing information stored on smart TVs.[53] In any case users must be offered the right to refuse such processing by the data controller. However, storing information or gaining access to information already stored in the terminal equipment is lawful insofar as it is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

2.3.4. Data Protection Directive

In substance, controllers are liable to process personal data fairly and lawfully and in line with the principles of Article 6 of the Data Protection Directive. These principles essentially circumvent the admissible scope, magnitude, purpose and duration of personal data processing to give effect to the principles of lawful processing, purpose specification and limitation as well as data minimization. Besides, the processing must be based on one of the legal grounds in Article 7 of the Data Protection Directive that render data processing legitimate: among others, the data subject's unambiguous consent to the data processing, as was defined above. In relation to their personal data individuals have the right to access information about the processing activities and the personal data held by the controller which also covers the right to demand rectification, erasure or blocking of personal

[52] Hybrid broadcast broadband TV (HbbTV) is a global initiative aimed at harmonising the broadcast and broadband delivery of entertainment services to consumers through connected TVs, set-top boxes and multiscreen devices. See for more info: https://www.hbbtv.org/.

[53] E.g. concerning earlier allegations that a smart tv read out files of USB keys and communicated this to the manufacturer, cf. Arthur C., "Information commissioner investigates LG snooping smart TV data collection" The Guardian, 21 November 2013, http://www.theguardian.com/technology/2013/nov/21/information-commissioner-investigates-lg-snooping-smart-tv-data-collection.

data (Article 12 (a), (b) of the Data Protection Directive). Moreover, Article 14 of the Data Protection Directive grants data subjects the right to object in certain circumstances, which can also be a opt-out from otherwise legitimate data processing, e.g. in the case of commercial communications according to Article 13 (2) of the E-Privacy Directive.

Data protection law must be applied specifically to each processing operation and in relation to each purpose, as a result of which the interpretation of the principles and the legitimate basis may differ from cause to cause. For argumentative reasons it is common to distinguish between primary and secondary purposes whereas the primary purpose of data processing coincides with a feature of the service requested by the user. A secondary purpose by contrast is more in the controllers' interest, such as placing contextual or behavioural advertisement. For example:

- The purchase of smart TVs is primarily a sales contract, which has little or nothing to do with the processing of personal data outside of technical and perhaps software updates. Additional processing of personal data would require a different legitimate basis than that the processing is necessary for the performance of a contract.
- Personalized services via the electronic programme guide would involve the tracking and processing of individual viewing patterns and behaviour. For a user who specifically subscribes to personalized services, and as long as they are informed about the extent and purpose for which their personal data is processed, this processing may be necessary for the performance of a contract, i.e., the primary purpose (Article 7 (b) of the Data Protection Directive). However, the meaning of the necessicity of the contract has to be interpreted strictly as to only include situations where the processing is genuinely necessary for the performance of a contract.[54]
- When this controller wants to introduce an additional (secondary) purpose for which the same personal data would be used, such as creating individual profiles intended for contextual or behavioural advertisement, this would require the data subject's unambiguous consent.
- Another provider, e.g. a publicly available TV channel (linear audiovisual media service) could not viably establish that the tracking of individual viewing patterns and behaviour is necessary for the performance of a contract simply because this is a one-to-many linear scheduled programme. In order to render the processing of personal data legitimate, the controller has to obtain the unambiguous consent of the data subject concerned.

Above all, default settings have to reflect the situation before the individual user of a smart TV or an online service delivered via a smart TV has given any consent to the processing of his or her personal data. Individual users should be able to control the collection and use of their personal data in the preferences and settings of the smart TV.

From what was said it becomes apparent that the application and compliance with EU data protection law is not a static exercise, but highly case-sensitive to the particular circumstances of a processing activity. It is thus futile to even attempt to enumerate all possible purposes for which personal data could be processed by each actor in the smart TV ecosystem, and explicate how the data protection rules apply *in concreto*.

[54] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014,
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

2.3.4.1. Confidentiality and security of processing

The Data Protection Directive also stipulates requirements on the confidentiality and security of processing. Article 16 of the Data Protection Directive seeks to commit any person who is employed by the controller or assigned to process personal data and who has access to personal data to adhere to the instructions from the controller. According to Article 17 of the Data Protection Directive the "controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing." In the context of the flows of personal data in connection with smart TVs this would likely be interpreted to require encrypted data flows and measures to address the information security triad, i.e., confidentiality, integrity or availability of the data.

2.3.4.2. International data flows

Finally, under EU data protection law the transfer of personal data from the EU to a third country is only permissible if an adequate level of personal data protection is ensured in that third country or if one of the derogations of Article 26 of the Data Protection Directive applies. If, for example, a smart TV collects personal data of EU data subjects and transfers those to an equipment manufacturer headquartered outside of the EU, this transaction involves an international transfer of personal data.[55] Such international transfers of personal data are only allowed where the third country has been found to provide an adequate level of protection of personal data.[56] In the absence of an adequacy finding of the European Commission, such international transfers can be based on binding corporate rules, standard contractual clauses or ultimately the unambiguous consent of the data subject (Article 26 (1), (4) of the Data Protection Directive).

2.3.5. New data protection regulation

The pending legislative proposals for a GDPR, as discussed, would broaden the territorial scope of application to cover, in addition, situations when a controller is not established in the EU, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of such data subjects. Once adopted, the pending proposals would bring clarification and certain regulatory innovations, of which some are relevant to smart TV. For example, if the separation principle is confirmed by the EU legislator, the data subject's consent is only "freely" given when the data subject has choice not to consent. Service providers must also provide an environment in which individuals can abstain from consenting to the processing of their personal data for secondary purposes.

The draft GDPR also introduces new rules on profiling and the principles on data protection by design and by default. The principles on data protection by design and by default create a duty for controllers and processors to implement appropriate and proportionate technical and organisational

[55] *Ibid.*

[56] See CJEU, decision of 6 October 2015 (Maximillian Schrems v Data Protection Commissioner), Case C-362/14, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362.

measures, having regard to the state of the art, current technical knowledge, international best practices and the risks represented by the data processing procedures.

2.4. E-Commerce Directive and EU Consumer Protection Law

The E-Commerce Directive[57] fills in the regulation of online services which are, on the one hand, not public electronic communications services consisting wholly or mainly in the conveyance of electronic signals and, on the other hand, not linear audiovisual media services, i.e., television broadcasting.[58] Pursuant to the terminology of the E-Commerce Directive these services are information society services, which are defined via reference to yet another Directive.[59] Information society services are 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' (Article 2(a) of the E-Commerce Directive in conjunction with Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC).[60] The smart TV environment can potentially host many information society services, such as video on demand, electronic programming guides, app stores and applications, among others.

The E-Commerce Directive does not mount comprehensive regulation of these services but is mainly concerned with establishing an internal market for such services and ensuring that contracts can be concluded via electronic means. However, it places on providers of information society services a fairly elaborate set of information requirements in relation to commercial communications (Arts. 5, 6 of the E-Commerce Directive).

In addition, the E-Commerce Directive provides for a set of liability exceptions for certain intermediary service providers who are providing transit ("mere conduit"), caching and hosting services (Arts. 12 to 14 of the E-Commerce Directive). In the smart TV ecosystem, all of these functionalities are certainly present; however, in order to benefit from the liability exemption, a given provider's service must exactly comply with the relevant definition of the Directive. For example, a digital platform caching and/or hosting third parties' audiovisual media services and online content can qualify for the liability exception as long as "this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored." (Recital 42 of the E-Commerce Directive).

It is important to note that the E-Commerce Directive cannot pre-empt EU data protection regulation. Recital 14 of the E-Commerce Directive clarifies that "the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data."

The Consumer Rights Directive[61] forms part of the EU consumer law aquis and approximates member states' laws on sales of goods and services, including distance and off-premises contracts, concerning contracts concluded between consumers and traders. The Directive in particular

[57] Supra fn. 25.

[58] Recital (18), supra fn. 25.

[59] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards as amended by Directive 98/48/EC and codified by Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015,

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535&from=EN.

[60] *Ibid.*

[61] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0083.

regulates contracts for the supply of digital content.[62] Recital 19 of the Directive defines digital content as "data which are produced and supplied in digital form, such as computer programs, applications, games, music, videos or texts, irrespective of whether they are accessed through downloading or streaming, from a tangible medium or through any other means." Apart from the mainstream consumer protection rules, such as the right to withdrawal, what is remarkable is that at the time of the formation of the contract, in addition to the general information requirements, the consumer must be informed about the functionality and the relevant interoperability of digital content.[63] Functionality, however, is also covering the ways in which digital content can be used for the tracking of consumer behaviour, among other things. This applies to the sale of digital content via on-premise, off-premise, and distance contracts (Arts. 5, 6 of the Consumer Rights Directive). Next to the information requirements flowing from EU data protection law the Directive is yet another legal source requiring prior disclosure of the tracking of consumer behaviour.

2.5. Human Rights Framework

As already mentioned, the European human rights framework contains important focuses on the rights to privacy and data protection. The most salient provisions are Article 8 of the European Convention on Human Rights ('Right to respect for private and family life'), and Articles 7 ('Right to private and family life') and 8 ('Right to protection of personal data') of the Charter of Fundamental Rights of the European Union. The principles set out in these provisions, as further developed in relevant case law, offer valuable guidance as to the substance and scope of the human or fundamental rights to privacy and data protection. The scope of Article 8 ECHR extends to protection of personal data, even though it is not explicitly referenced. The Charter separates the rights to privacy and protection of personal data in a way that acknowledges the evolution of data protection law as a distinct field that is subject to sector-specific legislation. Nevertheless, it is useful to recall the underlying connection between private life and personal data in respect of smart TVs. The voice-recognition features of smart TVs, coupled with their capacity to collect conversations conducted in the privacy of the home, raise obvious concerns for the right to private and family life.

Notwithstanding the importance of these human rights law provisions, their applicability to the actors providing services via smart TVs is complex. The ECHR, after the fashion of international treaties, only creates obligations for State authorities – and not ordinarily for private parties. As explained by leading commentators, the ECHR is not subject to *Drittwirkung*, a doctrine under which "an individual may rely upon a national bill of rights to bring a claim against a private person who has violated his rights under that instrument".[64] However, this is not to say that the ECHR cannot have indirect impact on the conduct of private parties, for instance through the positive obligations it imposes on states.[65] It should also be noted that national legislation could also address these issues.

Article 1, ECHR, obliges States Parties to the Convention to "secure to everyone within their jurisdiction the rights and freedoms" set out in the Convention. The obligation to "secure" these rights is unequivocal, and necessarily involves ensuring that the rights in question are not "theoretical or illusory", but "practical and effective".[66] In order to secure these rights, it is not

[62] *Ibid.*, Recital (19).

[63] *Ibid.*

[64] Harris D.J., O'Boyle M., Bates E.P. & Buckley C., *Law of the European Convention on Human Rights* (3rd ed.) (Oxford, Oxford University Press, 2014), p. 23.

[65] *Ibid*.

[66] *Airey v. Ireland*, 9 October 1979, Series A no. 32, para. 24, http://hudoc.echr.coe.int/eng?i=001-57420#{"itemid":["001-57420"]}.

always enough for the State to simply refrain from interfering with individuals' human rights: positive or affirmative action will often be required as well. Sometimes positive obligations are explicitly provided for in the ECHR, such as Article 6 (right to a fair trial) and Article 13 (right to an effective remedy). Both rights clearly presuppose affirmative action on the part of States, if the rights they guarantee are to be realised in practice. But besides such explicit positive obligations enshrined in the text of the ECHR, the Court has, over the years, identified various positive obligations that are implied by the text.[67]

In its *Airey* judgment, the Court stated that "although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life".[68] In *X. and Y. v. The Netherlands*, it supplemented that statement by admitting that such "obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves".[69] This is an important extension of the principle as articulated in anterior case law; it confirms a degree of horizontal applicability of relevant rights. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data sets out a legislative framework to be implemented by its member countries.[70] The Court frequently takes recourse to this convention in cases involving the automated processing of personal data.[71]

Similarly, it is important to bear in mind the specific applicability of the Charter of Fundamental Rights of the European Union. The Charter's provisions "are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law" (Article 51(1)). "They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties" (*ibid*.). The Charter's provisions "contain principles [that] may be implemented by legislative and executive acts taken by institutions, bodies, offices and agencies of the Union, and by acts of Member States when they are implementing Union law, in the exercise of their respective powers" (Article 52(5)). However, they shall be "judicially cognisable only in the interpretation of such acts and in the ruling on their legality" (*ibid*.).

[67] For detailed analysis, see generally, Mowbray A., *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights*, Oxford, Hart Publishing Ltd., 2004.

[68] *Airey v. Ireland*, supra fn. 66, para. 32.

[69] *X and Y v. the Netherlands*, 26 March 1985, Series A no. 91, para. 23, http://hudoc.echr.coe.int/eng?i=001-57603#{"itemid":["001-57603"]}.

[70] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108) and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (CETS 181),

http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

[71] E.g. *Amann v Switzerland* [2000] ECtHR 27798/95 [65], http://hudoc.echr.coe.int/eng?i=001-58497#{"itemid":["001-58497"]}.

3. Case studies by country

Within the four identified functions of smart TVs – voice recognition, motion control, facial recognition and account creation, the German joint position and technical test of smart TVs discusses all four aspects of smart TVs in general. The Dutch TP Vision and Ziggo cases specifically address the account creation feature and, lastly, the American EPIC complaint to the FTC focuses on voice recognition capabilities.

These country-specific case studies first of all give a comprehensive illustration of how guidelines could possibly be framed or how (data protection) authorities could possibly address the numerous legal implications of smart TVs by creating guidelines similar to the example of the German joint position. Second, the Dutch case studies illustrate specifically what data protection and privacy legal issues are involved. The American example shows the broader implications for regulatory approaches to smart TVs, *inter alia* for telecommunications, child protection and consumer protection law.

3.1. Germany

Against the backdrop of tests by a German consumer test institute (*Stiftung Warentest*) in spring 2014,[72] the issue of privacy and the protection of the personal data of members of the audience and users of the interactive functions of smart-TVs was making headlines. This independent test institute criticized in particular the smart-TV functionality HbbTV, which was found to communicate users' media consumption with television channels and a range of third parties, including Google. Also a smart TV set which uses facial recognition to offer personalized recommendations for television and online content was found to invade users' private sphere, mainly because the privacy policy of the manufacturer reserved the right to tranfer personal data to third parties. Other features, such as the integrated camera and microphone, were at that time considered unproblematic. However, the test institute discouraged the use of speech recognition since this is a biometrical individual characteristic.

Following this, German data protection authorities have given the issue of smart TV priority with regards to their compliance with local laws on data protection. In a coordinated fashion, the competent authorities of the federal states (*Länder*) issued a joint position paper[73] and launched a

[72] Stiftung Warentest, „Ausgespäht: Datenschutz beim Fernsehen", test 5(2014), https://www.test.de/filestore/4697612_t201405040.pdf?path=/protected/46/21/2b850438-9820-4bc1-bcfb-12f9cb905c2f-protectedfile.pdf.

[73] In German: Gemeinsame Position der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, „Smartes Fernsehen nur mit smartem Datenschutz", May 2014, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Beschluss_SmartTV.html.

technical investigation into smart TV's flows of personal data.[74] In September 2015, these activities culminated in the competent German data protection authorities' adoption of a guidance document detailing the data protection requirements on smart TV services.[75]

3.1.1. The joint position

The joint position with the title "Smart TV only with smart data protection" ("*Smartes Fernsehen nur mit smartem Datenschutz*")[76] aligns the data protection authorities in charge of enforcing data protection laws in the private sector (the so-called *Düsseldorfer Kreis*) with the data protection supervisors of the public service media organizations, and is above all supported by the conference of media authorities (*Konferenz der Direktoren der Landesanstalten für Medien*).

The joint position starts off by explaining that audiences and users of smart TV cannot easily tell the difference between watching linear television or accessing content via the Internet or both because the reception of audiovisual signals and interactivity with the Internet via a back-channel are now integrated. Users often cannot recognise which service they are using. Unlike traditional television, the Internet connection creates back-channel from the users to the television provider, the equipment manufacturer or other third parties. Via this back-channel it is possible to track and analyse the individual user's behaviour.

The joint position continues by linking the right to seek information with the tracking and the use of data about user behaviour. It holds that the enjoyment of the right to seek information, which forms an integral part of the right to freedom of expression in the German basic law (*Grundgesetz*) and is a foundation of the free and democratic constitution, would be hampered by this.

The joint position then enumerates the requirements under the relevant German data protection law, i.e., the Telemedia Law (*Telemediengesetz*).[77] In German law, telemedia services are defined similar to information society services under the E-Commerce Directive, thus comprising of electronic information and communications services which are not broadcasting and mere conveyance of electronic signals (Para. 1 (1) Telemedia law). The joint position provides guidance as to how the legal provisions apply to smart-TVs:

1. The anonymous use of television services must be provided for also in the context of smart-TV. The profiling of individual television consumption is not permissible without the informed and explicit consent of the user.
2. Insofar as online or HbbTV services are used via smart-TVs they are regulated as telemedia and have to comply with the data protection requirements of the German Telemedia Law. Equipment manufacturers, television channels and other providers of online services that qualify as telemedia services have to obtain the consent of the users or – as a minimum - comply with the following legal requirements:
    a. Users' personal data can be processed if it is necessary for the purposes of rendering the service and billing.
    b. When the use begins, at the latest, users must recognizably and comprehensively be informed about the collection and use of their personal data.

[74] Bayrisches Landesamt für Datenschutzaufsicht, "Datenschutz und Smart TV", press release of 27 February 2015, https://www.datenschutz-mv.de/presse/2015/pm-SmartTV.pdf.

[75] Supra fn. 7.

[76] Supra fn. 73.

[77] Telemedia law of 26 February 2007, last amended by Article 4 of the Law of 17 July 2015 http://www.gesetze-im-Internet.de/tmg/BJNR017910007.html.

c. Providers of telemedia services are only permitted to create and analyse individual profiles of the usage and consumption if they introduce pseudonyms and the user concerned has not objected. Such objection must be effectively implemented, in particular that information stored in the equipment of a user (e.g., cookies) are deleted. Providers have to inform users about their right to object. IP-addresses and device identification numbers are not pseudonyms in the sense of the German Telemedia Law.
d. Competent internal bodies have to ensure that usage profiles are not re-combined with the individual user behind the pseudonym.

3. Observance of the principle "privacy by default": Manufacturers and providers have to ensure that the default settings of smart-TVs and supported online services conform with the principle of anonymous use of the television set. The access of online services and the corresponding online exchange of data between the device manufacturer, the service provider and other providers can only take place if the user has initiated the request after receiving comprehensive information, e.g. the activation of HbbTV via the red button. Users must be able to control the information that is stored in the equipment. In particular, it must be possible for them to manage cookies.
4. Smart-TVs, HbbTV services of the television channels, and other online services have to maintain technical security measures that protect the devices and the data traffic against unauthorized access by third parties.

3.1.2. The technical test

Early in 2015, led by the Bavarian data protection authority (*Bayerisches Landesamt für Datenschutzaufsicht*), a coordinated countrywide technical test action was conducted of smart TVs of thirteen manufacturers, which together cover circa 90 per cent of the German market.[78] The objective of the technical test was not to attest to the conformity or non-conformity of specific devices or manufacturers with the relevant German data protection laws. Rather, the test aimed to form a technical understanding of the data flows from smart TVs and to obtain a differentiated notion of the actors involved. In detail, the technical test focused on the information duties of the device manufacturers and the analysis of data flows in relation to HbbTV, app stores and personalized recommendation services. Encryption of data flows from the smart TV is essential from an information security point of view, but it also posed a limiting factor for the technical test which could not verify the exact nature of the information transmitted.

The following passage provides a short summary of the test results, based on the presentation delivered at the press conference on 27 February 2015:[79]

- Out of the 13 smart TVs tested, six presented information in relation to privacy and data protection before the device was connected to the Internet.
- Seven out of ten television channels track via the HbbTV-function ("red button") when the user switches between television channels.
- Eight out of ten television channels inform users of the HbbTV-function about the processing of personal data and solicit their consent.

[78] Supra fn. 74.

[79] Bayerisches Landesamt für Datenschutzaufsicht, „Technische Pruefung SmartTV", Press conference of 27 February 2015 https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/SmartTV_Technische%20Pr%C3%BCfung%20Druck.pdf.

- Six out of 13 smart TVs encrypt data when using the app stores that are preinstalled by the device manufacturer; of the seven smart TVs which communicate unencrypted with the app store, five transmit the name of the app the user has started.
- When users receive personalised recommendations via the electronic programme guide (EPG),[80] seven out of the 13 smart TVs sent encrypted communications to the EPG's server. For the remaining six smart TVs, no traffic flows were detected at all.
- When users connect an external storage medium, here a USB key, to the smart TV, four out of 13 devices sent encrypted communications.[81]
- Out of the 12 smart TVs with a recorder function, one communicated the recording back and five others sent encrypted communications.
- When watching linear television, all ten television channels tested received data via the back-channel and so did four out of 13 device manufacturers.

As an outcome of the technical test action the competent data protection authorities of the federal states (*Länder*) have prepared a guidance document manual on smart TV that is intended to butress implementation and enforcement action. In parallel, the competent data protection authorities will follow up with the device manufacturers in order to clarify further and determine what needs to be done in order to achieve data protection conformity of their smart TVs.

3.1.3. Guidance Document on Data Protection Requirements for Smart TV Services

In its session on 15-16 September 2015, the German data protection authorities for the private sector, organized as the *Düsseldorfer Kreis*, adopted a new guidance document on data protection requirements for smart TV services.[82] The guidance is addressed to the providers of smart TV services and products, in particular equipment manufacturers, app portals and app providers, personalized recommendation services, and HbbTV providers. The document provides a substantial overview on how the competent data protection authorities assess their activities under German data protection law (*Bundesdatenschutzgestz*).

The guidelines are careful to explain the services provided by a smart TV that result in personal data flows, and also provide definitions and explanations of key concepts in German data protection law. What is also commendable about the guidelines is the holistic approach to data protection issues in the smart TV ecosystem comprising of various actors and services, but also cognizant of vertical integration in the value chain.[83] Hence, following a modular approach, German data protection requirements are particularised for a range of services via smart TVs that involve personal data flows.

The assessment is based on German data protection law, which derogates in a few important aspects from EU data protection law as described in Chapter 2. In principle, the guidelines set out the circumstances in which the German legal situation provides for a legal basis for the

[80] Under the condition that the consent was given to all processing of personal data.

[81] In connection with earlier allegations that a smart tv read out files of USB keys and communicated this to the manufacturer, cf. Arthur C., "Information commissioner investigates LG snooping smart TV data collection", *op.cit.*

[82] Düsseldorfer Kreis, supra fn. 75.

[83] *Ibid.*

processing of personal data or when an individual user has to give his or her explicit consent to the personal data processing. The relevant German Telemedia Law (*Telemediengesetz*) differentiates between the use of subscriber information (*Bestandsdaten*) and usage data (*Nutzungsdaten*) of individual users, which must adhere to different legal requirements. Notably, under the Telemedia Law, users have the right to use services that qualify as telemedia services anonymously, insofar as this is technically possible. Thus, users should be offered a choice on this matter. This requirement, for example, does not exist in EU data protection law.

Another peculiarity of the Telemedia Law is that service providers are allowed to create usage profiles linked to pseudonyms for the purposes of advertising, market research, and in order to provide the requested services unless the user has objected (i.e., an opt-out requirement).[84] Pseudonymisation, however, requires a separation between pseudonymous usage profile and the individual user of the service, and this is not complied with when linking usage profiles to device identifications numbers or IP addresses.

Much emphasis is placed on the information requirements that are a prerequisite under German data protection law and have to be presented before the personal data processing may take place.[85] Users should also have the possibility to access the information about how their personal data is used at any time. The guidelines clarify that placing the information in the terms and conditions of a service would not suffice in light of the transparency requirement in German data protection law. Moreover, the German data protection law furnishes the data protection principles that are also known in EU law.

Another set of important requirements concern the ability of users to manage the settings and preferences on their device, including cookies, and privacy by default and by design in relation to HbbTV-enabled online services and built-in microphones and cameras.[86]

Finally, it should be highlighted that the guidelines specify the technical and organisational measures necessary to protect the security of the personal data. In particular, equipment manufacturers have to ensure regular security updates, and all personal data flows between the smart TV and service providers should be encrypted during transit, among others.

The joint position described earlier is a policy document whereas the guidelines issued thereafter indicate more precisely how the the competent German data protection authorities will interpret and apply the law in relation to the processing of personal data by the various providers within the smart TV ecosystem. The Guidelines are strictly applying the relevant German provisions on data protection from the Telemedia Law and the Federal Data Protection Act. They are not programmatically going beyond what the law requires, which is, however, rather strict in any case. The main achievement of the guidance document is that the legal assessment is modular in response to the specific activities involving the processing of personal data irrespective of the role of the provider in the smart TV ecosystem.

3.2. The Netherlands

The Dutch Data Protection Authority (*'College bescherming persoonsgegevens'* - CBP) has investigated two commercial companies involved in the processing of personal data in relation to interactive digital TV and online services through smart TVs. The CBP supervises the compliance with

[84] *Ibid.*

[85] *Ibid.*

[86] *Ibid.*

Dutch data protection act[87] ('*Wet bescherming persoonsgegevens'* – WBP) which implements the EU Data Protection Directive, discussed in detail in Chapter 2 on the European regulatory frameworks.[88] In case of a violation of Dutch law, the CBP can use enforcement powers such as conditional fines.[89] The CBP identified the processing of personal data concerning viewing behaviour – in the light of the bigger theme 'tracking and tracing' - as a topic that merits special attention.[90] The first investigation concerned TP Vision:a company offering smart TV services through Phillips equipment. The second investigation concerned the cable TV operator Ziggo,which offers audiovisual media to its subscribers. Because of the detailed analysis of the Dutch Data Protection Act, these examples, besides identifying Dutch legal implications, also raise pertinent questions concerning the European data protection framework applicable to the regulation of smart TVs.

The factual and legal circumstances of the two cases will be analysed separately, and, subsequently, future implications for the regulation of smart TVs will be described in a concluding remark on the Dutch illustrations.

3.2.1. Case study 1 – *CBP v. TP Vision*

On 2 July 2013, the Dutch Data Protection Authority published its findings concerning the Dutch company TP Vision, manufacturer of Philips Smart TVs.[91] The CBP investigated the processing of the personal data of Philips Smart TV users in the Netherlands. The CBP states that TP Vision was in violation of the Dutch Data Protection Act (WBP) for the absence of clear, accessible and comprehensive information about the processing of personal data, the lack of informed consent for placing tracking cookies and the absence of a contract with third parties. The data processed by TP Vision refers to the 'account creation' possibilities and interactive features of smart TVs, as described in detail above.[92]

This case study will first analyse the factual background of CBP's investigation into TP Vision Smart TVs. Secondly, the legal framework underlying CBP's report on TP Vision's Smart TVs will be examined.

3.2.1.1. Factual background

The motive for the CBP to investigate Smart TVs, and TP Vision in particular, has been the rise in the sale of televisions with interactive capabilities and video-on-demand services that collect user information. TP Vision develops and produces Smart TVs for Philips, of which an estimated 1.2 million have been sold in the Netherlands since 2009. TP Vision collects and stores data on online viewer behaviour, the use of apps, and website history - for example by using (tracking) cookies. In addition, the TP Vision Smart TV collects data in relation to user habits such as: favourite

[87] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_26-10-2015.

[88] Chapter 2, under E-privacy and Data Protection Regulation.

[89] https://www.cbpweb.nl/en/node/1930.

[90] Dutch Data Protection Authority, Investigation into the processing of personal data by use of interactive digital television services of Ziggo, Report of 28 April 2015, https://cbpweb.nl/sites/default/files/atoms/files/onderzoek_ziggo.pdf. Dutch Data Protection Authority, Annual Report 2014, https://cbpweb.nl/sites/default/files/atoms/files/annual_report_2014.pdf.

[91] Dutch Data Protection Authority, Investigation into the processing of personal data on Philips Smart TVs by TP Vision Netherlands B.V., Report of 2 July 2013, https://www.cbpweb.nl/sites/default/files/downloads/pb/pb_20130822-persoonsgegevens-smart-tv.pdf.

[92] Chapter 1.

programmes and apps, recorded programmes, rented videos, and shows viewed on-demand. Using this data, TP Vision offers viewers personalised recommendations and intends to offer personalised advertisements in the future.

3.2.1.2. Legal framework

After starting with a substantive overview of TP Vision's practices and other circumstances of the case, the CBP examines these acts and practices in the light of the WBP. Amongst the various obligations in the WBP, this CBP investigation focuses on the primary requirements of the concept of personal data, the legal basis for the processing of personal data, the information requirements and the contracts with third parties.

3.2.1.2.1. Personal data

Personal data is defined in the WBP as *"any information relating to an identified or identifiable natural person".*[93] Since the definition has the same characteristics as the definition used in the EU Data Protection Directive and explained by the Article 29 Working Party, the detailed examination of "personal data" in Chapter 2 is sufficient to give a comprehensive overview of this CBP report. According to the CBP, the collected data is to be categorized as personal data, since the information collected by TP Vision – inter alia, IP addresses, watched TV programmes, used apps and visited websites - gives an extensive account of users' TV habits, behaviour and preferences.[94] Moreover, the CBP qualifies the personal data as sensitive in nature because it reveals a lot about individuals.[95] It can point, for example, to a specific social background, financial profile and/or family situation. Subsequently, this type of data can possibly be used to influence (online) user behaviour, serve direct marketing purposes or the profiling of Smart TV users. This aspect of the finding is noteworthy because it introduces sensitive personal data as a category that is distinct from the otherwise protected special categories of personal data, revealing matters about health, religious beliefs, political opinions, etc.

TP Vision determines the purposes and means of the processing of the personal data. TP Vision therefore is to be seen as the "controller" of the processing of the personal data derived from the smart TVs.[96] Again, the definition of "controller" corresponds with the definition in the European framework as described above.

3.2.1.2.2. Information

According to the WBP, data controllers must communicate specific information to their data subjects: the identity of the controller, the purposes of processing, the recipients of the data, and the existence of their rights of access and right to oppose.[97] This information must be provided in a

[93] Article 1(a) WBP; Article 1(a) Data Protection Directive. For more information see: Article 29 Working Party, WP 136, Opinion 4/2007 on the concept of personal data, 20 June 2007.

[94] For the full list of collected data see: Dutch Data Protection Authority, Investigation into the processing of personal data on Philips Smart TVs by TP Vision Netherlands B.V., Report of 2 July 2013.

[95] *Ibid.*

[96] Article 1(d) WBP; Article 2(d) Data Protection Directive. For more information on the concepts of "controller" and "processor": Opinion 01/2010 on the concepts of controller and processor adopted on 16 February 2010 (WP 169),

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

[97] Articles 33 and 34 WBP; Articles 10 and 11 Data Protection Directive.

clear and comprehensible manner, with the aim to provide the user with more control over the dissemination of personal data.

CBP stated that TP Vision did not comply with these information requirements. Consumers were neither informed on Philip's website, nor by TP Vision's privacy policy, cookie banner, or terms of use. More specifically, users did not receive information on the existence and responsibilities of TP Vision, on the placement of cookies, on the kind of data that was collected, or for how long this data was stored.

Over the course of the investigation TP Vision adjusted their privacy statement, cookie policy, and terms of use to achieve compliance. Nevertheless, according to the CBP, the information is still insufficiently clear, inconsistent, and inaccessible to the public. For example, the information is not presented in Dutch, in short and easily readable texts, and, secondly, the information is not provided in advance but after the Smart TV has already been connected to the Internet.

3.2.1.2.3. Legal basis for processing personal data

In its report, the CBP determines that TP Vision gains access to user information by placing cookies. Because of the use of cookies, the company also has to comply with the Dutch Telecommunications Act.[98]

When a controller stores or gains access to information already stored on a device, the user concerned must consent to such storage or access to information for these actions to be legitimate - unless they are *"strictly necessary in order to provide a service explicitly requested by the subscriber or user".*[99] In accordance with the Dutch Telecommunications Act – and the aforementioned EU E-Privacy Directive - the user's consent must be based on clear and comprehensive information from the controller about, inter alia, the purposes of the processing.

In addition, the cookies placed by TP Vision process personal data. Therefore, the controller needs to have a legal basis for this processing of personal data to be legitimate in the light of the WBP.[100]

In the view of the CBP, TP Vision needs to acquire 'unambiguous consent' before it may collect personal data via cookies. This consent must be based on a free, specific, and informed expression of intent. Initially, TP Vision did not ask for permission at all, although this policy was altered at a later stage. Moreover, the consent is not given freely, since the consent is requested in the process of installing the smart TV. As a result, the user must accept the terms of use. The same is true when TP Vision used 'pop-ups' with opt-out possibilities for receiving consent, since only opt-in possibilities can be seen as free expression of intention.

Secondly, as stated above, TP Vision does not present clear and accessible information about the use of cookies and the specifics of the processing taking place. This absence of transparency is not considered to be valid consent for the processing of data, due to the absence of 'specific' and 'informed' consent.

3.2.1.2.4. Processing agreement

For the processing of personal data, TP Vision uses the services of five different companies. As these companies can be seen as "processors" under the Dutch Data Protection Act, TP Vision is obliged to

[98] Dutch Telecommunications Act of 19 October 1998 (*'Telecommunicatiewet'*), http://www.wetboek-online.nl/wet/Telecommunicatiewet.html.

[99] Article 11.7a(3)(b) Tw.

[100] Article 8 WBP; Article 7 Data Protection Directive.

enter into a processing agreement or other legal act with the processors to address the responsibilities of both parties, with the aim of ensuring the fair processing of personal data.[101]

The CBP stated that TP Vision is in violation of this requirement, since no processing agreement was signed with Google for the use of the Google Analytics services. Google, however, refused to sign the contract, so the issue was resolved by ending the cooperation with Google entirely. In regard to the other processors, TP Vision already signed contracts that, in the view of the CBP, merely needed small adjustments in order to comply with the WBP.

In reaction to the CBP investigation, TP Vision amended its privacy statement, cookie policy and terms of use agreement to bring its practices in accordance with the WBP. Information on the collection of cookies for monitoring viewer behaviour is more clearly presented when the smart TV is installed and, in addition, clear and comprehensive information concerning the processing of data for advertising purposes is available. As stated above, CBP is of the opinion that TP Vision is still in violation of Dutch data protection law. However, CBP announced that because of the partial ending of the breach, CBP would not proceed with formal enforcement actions.[102] The CBP will nevertheless continue to monitor TP Vision's compliance with the WBP.

3.2.2. Case study 2 - *CBP v. Ziggo*

On 28 April 2015, the Dutch Data Protection Authority published the report on its investigation of cable TV operator Ziggo. The report explains how Ziggo infringed the Dutch Data Protection Act by monitoring viewing behaviour of users of interactive digital television services. This personal data, corresponding to the findings in the TP Vision case, refers to the 'account creation' possibilities and interactive features of smart TVs, as described in detail in Chapter 1. According to the CBP, Ziggo violated the WBP by not providing users with sufficient information on the processing of personal data. Furthermore, the investigation concluded that Ziggo did not obtain the requisite unambiguous consent for the processing of personal data.

This case study will first analyse the factual background of the CBP report. Secondly, the legal framework underlying the CBP's research of Ziggo's interactive services will be examined.

3.2.2.1. Factual background

Ziggo B.V. is a Dutch cable TV operator providing interactive digital television services. Although Ziggo recently merged with UPC Nederland, the CBP's research took place before this merger and therefore only takes into account the acts and activities of Ziggo. The reason for the CBP to investigate Ziggo is that Ziggo was, with 2.3 million users, the biggest provider of digital television services in the Netherlands. Today Ziggo services 4.2 million customers.

In its report, the CBP discusses three different forms of monitoring of viewer behaviour to determine how Ziggo uses this data for profiling and marketing ends. The CBP focuses on 'regular' (i.e., linear) TV viewing, (video) on-demand viewing, and pay-per-event viewing. By use of the first category, linear TV viewing, Ziggo was able to determine the viewing behaviour of specific individuals, and, consequently, to determine viewing ratings on a larger scale. The CBP report explains that Ziggo was processing this personal data with the use of an activated interactive television decoder.

[101] Article 14 WBP; article 17(4) Data Protection Directive.

[102] See https://www.cbpweb.nl/nl/nieuws/tp-vision-past-privacybeleid-aan-na-onderzoek-cbp.

In the case of on-demand services, Ziggo, also with the use of interactive decoders, was capable of monitoring the viewing history of users. By profiling the behaviour of video-on-demand users, Ziggo personalized viewing recommendations for specific users and, secondly, could provide viewing recommendations in general.

Thirdly, the CBP distinguished 'pay-per-view' or 'pay-per-event' monitoring. Pay-per-view is the interactive service by which users can buy certain programmes or films online, primarily in the category of sports and erotica. Ziggo used this viewer information on a once-off basis for the purposes of direct marketing.

3.2.2.2. Legal framework

The CBP starts its report with a substantive overview of procedural aspects and factual circumstances of Ziggo's processing of personal data. Afterwards, the CBP examines the acts and practices of Ziggo in the light of the WBP. Comparable to the CBP's analysis in the case of TP Vision, this CBP investigation focuses – amongst the various requirements of the WBP - on the concept of personal data, the information requirement and the legal basis for the processing of this data. These obligations will be discussed in the light of the distinction made by the CBP between the linear, on-demand and pay-per-event viewing. The CBP identifies breaches of data protection law in each of these areas.

3.2.2.2.1. Personal data

According to the CBP, Ziggo collects personal data by monitoring viewer behaviour. By subsequently analysing and/or combing this data, Ziggo is able to label users according to specific profiles and treat them differently or approach them in a more targeted manner.

Notably the CBP made a remark regarding the sensitive nature of the personal data involved in Ziggo's data processing activities. Following its assessment in the TV Vision case, the personal data should be regarded as sensitive, since the monitoring of digital television consumption – notably the pay-per-view history of erotic content – intrusively reveals the habits and preferences of users. This can point to a specific social background, financial profile and/or family situation. Subsequently, this type of data can possibly be used to influence (online) user behaviour, or serve direct marketing purposes and the profiling of Ziggo users.[103]

3.2.2.2.2. Information

As previously stated, according to the WBP, controllers must communicate specific information to the data subjects, such as the identity of the controller, the purposes of processing, the recipients of the data, the existence of their rights of access in relation to the processing of their personal data.[104] This information must be provided in a clear and comprehensible manner, with the aim to provide the user with more control over the dissemination of personal data.

In the first category, linear TV services, Ziggo was able to determine the viewing behaviour of specific individuals, although insufficient information was provided to the data subject. In the view of the CBP, Ziggo does not sufficiently clarify which personal data is collected and processed for what specific purposes.

---

[103] *Ibid.*

[104] Articles 33 and 34 WBP; articles 10 and 11 Data Protection Directive.

Ziggo addressed this infringement by adjusting the decoders in such a way that information on viewing behaviour was no longer traceable to specific persons. By the implementation of these anonymisation methods, the processed data can no longer be regarded as personal data. As a result of these adjustments the Dutch data protection law is no longer relevant, which also resolved inter alia the earlier violations of the law, the CBP stated.

With regard to the category of on-demand TV, Ziggo failed to provide sufficient information on multiple aspects. Firstly, Ziggo's privacy policy stated that all information was processed anonymously, which the CBP identified to be false. Moreover, users are unaware of the kind of behavioural data that is processed. Thirdly, Ziggo is in violation of the information duty for not clarifying the purposes of the processing. The purpose of *"adapting services to customers'"* needs is not specific enough. In addition, users do not know their viewing behaviour is used to create user profiles. Finally, in general, Ziggo's privacy policy was inaccessible to most customers, as it was difficult to find access to the privacy statement on Ziggo's website.

In the final category, pay-per-event viewing, Ziggo also failed to observe its informational duties. The monitoring of (sensitive) digital consumption took place without Ziggo informing its users about any aspect of the processing. In general, users were ignorant of the fact that Ziggo profiled their personal viewing behaviour for marketing purposes.

3.2.2.2.3. Legal basis for processing personal data

The WBP requires the controller to have a legal basis for the processing of personal data to be legitimate.[105] The CBP states that Ziggo is in violation of this requirement due to the monitoring of linear viewing, on-demand viewing, and pay-per-event viewing, in the absence of valid consent. The CBP clarified that Ziggo could not rely on any legal basis other than 'unambiguous consent' for its processing, since it concerned sensitive data.

In the first category, linear TV, the CBP reported that Ziggo did not acquire the requisite unambiguous consent before processing the users' personal data. At the time, Ziggo did not provide users with the ability to express their consent at any time in the process of the collection of data. As stated above, by anonymising the processed data, the breach of the WBP provision was resolved since the information about viewing behaviour was no longer traceable to specific individuals.

In the view of the CBP, the use of personal data from on-demand viewing constituted a violation of the WBP. Ziggo did not obtain a valid informed consent; users did not have an effective way of refusing permission for this act of processing.

Initially, Ziggo did not request consent at all. Thereafter, Ziggo introduced the so-called "I do not agree" button. Attempts were made to formulate the request for consent more specifically, but this could not remedy the fact that insufficient information was being provided concerning the types of personal data being collected. According to the CBP, Ziggo does not inform users about the specific categories of personal data that is being used to order to personalise content. In addition, as stated above, Ziggo does not inform users about the creation of profiles. Furthermore, this request was only displayed to new customers, and not to Ziggo's earlier users. Since consent was a strict necessity according to the CBP, its absence rendered Ziggo's activities unlawful. Ziggo once more adapted its on-demand activities, and consumers are now prompted to give valid consent for the processing of their personal data or not.[106]

In the final category, pay-per-event viewing, viewer information was used on a one-time basis for the purposes of direct marketing. The same as noted under linear TV and on-demand TV is

[105] Article 8 WBP; article 7 Data Protection Directive.

[106] CBP Persbericht, *'Ziggo beëindigt privacy overtredingen digitale tv na onderzoek CBP'*, 9 June 2015, https://cbpweb.nl/nl/nieuws/ziggo-beeindigt-privacyovertredingen-digitale-tv-na-onderzoek-cbp.

true for this category. Especially since the information is identified by the CBP as being sensitive personal data, Ziggo failed to comply with the WBP for not having required a valid consent.

In response to the CBP report, Ziggo ended the violations of the WBP with multiple adaptions of their privacy policy. The CBP states that Ziggo now complies with the requirements of the WBP by correctly informing subscribers and requesting their unambiguous consent for the processing of their personal data.[107]

3.2.2.3. Future implications

In general, the CBP acknowledges that, since smart TVs are relatively new on the television market, there is still little awareness among consumers of the risks that are present when using them. It is therefore likely that the CBP will continue to focus on this new phenomenon, with a view to protecting the rights of subscribers and users of interactive smart TV services. CBP's enforcement focus underscores the awareness of the privacy and data protection implications of interactive devices, like Smart TVs, that easily connect multiple aspects of an individual's private life.[108] In the Netherlands, an alliance of data protection supervisors and public media organizations – or other cross-sectoral coordination – like the German alliance has not (yet) been constructed.

3.2.2.3.1. Interactive televisions

Both investigations are representative of the Dutch Data Protection Authority's approach to launch selective enforcement actions that are exemplary for the processing of personal data in the context of interactive smart TV services. The Ziggo investigation highlights interesting characteristics of monitoring and profiling of interactive television users. The widespread possibilities of Smart TVs are discussed by specifically addressing the differences between linear TV viewing, on-demand viewing, and pay-per-event viewing. By contrast, in the TP Vision case other services in relation to smart TVs were concerned, such as the monitoring of online viewer behaviour, the use of apps, and website history more in general[109]. Moreover, the CBP confirms that information on user viewing history, whether in the form of on-demand viewing or pay-per event viewing, can be categorized as sensitive personal data. This could implicitly be applicable to other interactive consumer devices that profile individual behaviour.

3.2.2.3.2. The role of information and transparency

In both of the Dutch examples, it becomes clear that the primary aspect of the violation is the absence of sufficient information to the data subject. The information duty is a specific requirement in Dutch (and EU) data protection law. It also influences the validity of a consent, since it needs to be based on 'an informed' expression of intention. One could conclude that this information aspect of data protection plays an important role.

Both of the Dutch CBP reports demonstrate the importance of transparency in the field of interconnected consumer devices. The increase of transparency concerning the specifics of the

[107] *Ibid.*

[108] Article 29 Working Party has published a report on the importance of transparency in the area of interconnected devices, see: Article 29 Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things', WP 223 16 September 2014.

[109] Dutch Data Protection Authority, Investigation into the processing of personal data on Philips Smart TVs by TP Vision Netherlands B.V., Report of 2 July 2013.

processing of personal data and processor agreements is likely to improve decision-making and the possibility for users to effectively control their personal data.

In combination with media regulation that aims to empower the individual (media literacy), data protection regulation aims at the same empowerment and transparency objective. Other requirements in the WBP, such as the data subject's right to access, should empower individuals vis-à-vis controllers of personal data.

Thus, the violations that the CBP addressed in these two case studies primarily aim at empowerment of the individual. The Dutch cases do not mention consumer protection laws. However, the empowerment of the individual can be seen as having the same objective as consumer protection regulation, as will be described below.

In addition, the German joint position also explains the lack of information, primarily because of the reception of audiovisual signals and interactivity with the Internet via a back-channel are now integrated. The technical test of smart TVs revealed that out of 13 smart TVs tested, six presented information in relation to privacy and data protection before the device was connected to the Internet.[110]

3.3. An American Example

What is interesting about the following case study from the United States of America is that EPIC describes different regulatory options for the Federal Trade Commission to take action against Samsung. As set out in Chapter 2, (at least) five sets of regulation are applicable to smart TVs. In contrast to the Dutch examples, this case study shows the possibility of acting against the allegedly prohibited act of processing (voice recording) data, by referring to consumer protection - and specifically to the protection of children – and privacy and telecommunications law. Although it is not certain whether the FTC will press charges based on these acts, it is interesting to see the different options for regulating smart TVs in the United States.

3.3.1. *Electronic Privacy Information Center v. Samsung*

On 24 February 2015, the Electronic Privacy Information Center (EPIC)[111] filed a complaint with the United States Federal Trade Commission (FTC) concerning Samsung's smart TVs.[112] In this complaint, EPIC states that Samsung's business practices adversely impact consumer privacy in the United States, since Samsung routinely intercepts and records the private communications of consumers in their homes by the use of voice recording features of smart TVs. For this reason, EPIC asks the FTC to take action in this matter.

This case study will first analyse the factual background of EPIC's complaint. Secondly, the legal framework underlying EPIC's complaint of Samsung's alleged privacy invasive Smart TVs will be examined. The last section will study possible implications of EPIC request to the FTC.

---

[110] Bayrisches Landesamt für Datenschutzaufsicht, „Technische Pruefung SmartTV", Press conference of 27 February 2015, https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/SmartTV_Technische%20Pr%C3%BCfung%20Druck.pdf.

[111] EPIC is a public interest research centre located in Washington DC.

[112] EPIC, *In the matter of Samsung Electronics Co., Ltd., EPIC Complaint, Request for Investigation, Injunction and Other Relief*, 24 February 2015, https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf.

3.3.1.1. Factual background

EPIC's complaint concerns the voice recognition abilities in Samsung's smart TVs. Samsung's "Smart Touch" remote control has a built-in microphone for voice recording. As explained above,[113] Samsung's smart TVs are capable of more than the voice recognition feature that was studied by EPIC. The motion control, facial recognition and account creation functions, therefore, will not be dealt with in this case study.

The foundation of EPIC's statement that Samsung routinely intercepts and record private conversations in the home is to be found in Samsung's previous[114] and current[115] privacy policies. EPIC cites three sections of these privacy policies to highlight the alleged violations of consumer privacy.

The first and primary section that EPIC cites is the text following the heading 'Voice Recognition' under the previous Privacy Policy: *"Please 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."*[116] According to EPIC, as soon as this speech recognition feature of the smart TV is enabled, everything a user says in front of the Samsung Smart TV is recorded and transmitted over the Internet to a third party – regardless of whether it is related to the provision of the service. The 'third party' mentioned in the Privacy Policy was not yet identified in the previous version of the Policy.[117] Samsung later – after negatively being reported in the media – explained that the 'third party' is the voice-to-text recognition company Nuance Communications, Inc.[118]

In addition, EPIC cites a section of Samsung's current Privacy Policy: "*Please note that when you watch a video or access applications or content provided by a third-party, that provider may collect or receive information about your Smart TV (e.g., its IP address and device identifiers), the requested transaction (e.g., your request to buy or rent the video), and your use of the application or service. Samsung is not responsible for these providers' privacy or security practices. You should exercise caution and review the privacy statements applicable to the third-party websites and services you use."*[119] Based on this section, EPIC states that Samsung attempts to disclaim liability for any third party data privacy or security practices, including Nuance's data privacy and security practices.[120]

Thirdly, EPIC mentioned that Samsung stated it encrypts the voice communications it transmits to Nuance.[121] However, computer researchers Ken Munro and David Lodge found out that Samsung does not encrypt all the voice recordings it records and transmits to Nuance.[122] According to EPIC, in response to its research, Samsung later conceded that the company does not encrypt all the conversations it transmits, and subsequently that it has not deployed the software necessary to encrypt plaintext transmissions.[123]

---

[113] Para. 1.2.

[114] See http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/.

[115] See http://www.samsung.com/uk/info/privacy-SmartTV.html.

[116] Supra fn. 114.

[117] Supra fn. 114.

[118] *Ibid.*

[119] Supra fn. 112, para. 24; Samsung Global Privacy Policy http://www.samsung.com/us/common/privacy.html.

[120] Supra fn. 112, para. 23.

[121] *Ibid,* para. 25; *"Samsung takes consumer privacy very seriously and our products are designed with privacy in mind. We employ industry-standard security safeguards and practices, including data encryption, to secure consumers' personal information and prevent unauthorized collection or use."* http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/.

[122] *Ibid.*, para. 27; https://www.pentestpartners.com/blog/is-your-samsung-tv-listening-to-you/.

[123] Supra fn. 112, paras. 28 and 29; http://www.bbc.com/news/technology-31523497.

EPIC substantiates its complaint by quoting privacy experts and collecting consumer experiences. According to EPIC, privacy experts warn that Samsung's "always-on" voice recording practice is misleading to consumers and those who have learned of this practice described it as both unfair and deceptive.[124]

3.3.1.2. Legal framework

EPIC demonstrates the alleged unlawfulness of Samsung's Smart TV - the aforementioned widespread intercepting and recording of private conversations, the (partial) absence of encryption and the attempt to disclaim liability - by citing the Cable Act, the Electronic Communications Privacy Act, the Children's Online Privacy Protection Act and the FTC Act. The core of the complaint is based around the FTC Act and the corresponding FTC Policy Statements on Deception and Unfairness.

3.3.1.2.1. The Cable Communications Policy Act

Firstly, EPIC cites the Cable Communications Policy Act (CCPA),[125] which aims to protect the personal information of customers of cable service providers.

Provision 47 U.S.C. 551 §631(b) CCPA prohibits the collection of personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned. Moreover, 47 U.S.C. 551 § 631(c) prohibits the disclosure of personally identifiable information of a subscriber[126] and demands that the cable providers take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator- i.e. the voice-to-text recognition company Nuance.

In reaction to these requirements, EPIC states that *"Samsung does not obtain written or electronic consent to recording the private conversations of people in their homes and transmitting those voice recordings to Nuance".*[127] EPIC furthermore states that *"Samsung does not take such actions as are necessary to prevent unauthorized access to subscriber information"* and subsequently, that "*Samsung deliberately over collects information provided by cable subscribers".*[128] EPIC does not specifically address in what manner this over-collecting takes place.

3.3.1.2.2. The Electronic Communications Privacy Act

The second Act that is cited by EPIC is the Electronic Communications Privacy Act (ECPA).[129] The ECPA protects wire, oral and electronic communications and applies to email, telephone conversations and electronic stored data.

18 U.S.C. § 2511(1) EPCA provides that any person[130] who *"intentionally intercepts, endeavours to intercept, or procures any other person to intercept, any wire, oral, or electronic communication"*[131] or *"intentionally discloses, or endeavours to disclose, to any other person the*

[124] Supra fn. 112, para. 30-57.

[125] Cable Communications Policy Act of 1984 (CCPA), 47 U.S.C. §521-573.

[126] Exceptions to the prohibition of disclosure as stated in 47 U.S.C. 551 § 631(2), government requests pursuant to court order, or disclosures necessary for the fulfilment of cable services, are not applicable in the underlying case.

[127] Supra fn. 112, para. 60.

[128] *Ibid.*, para. 61.

[129] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-2522.

[130] The definition of 'person' includes corporations; 18 U.S.C. § 2510(6).

[131] 18 U.S.C. § 2511(1)(a).

contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection"[132], violates the EPCA.

EPIC states that Samsung is violating the ECPA by intercepting and recording private communications in the home,[133] since Samsung intentionally intercepts conversations and discloses these voice recordings to Nuance and *"no exception permits a company to surreptitiously record private communications in the home".*[134]

3.3.1.2.3. The Children's Online Privacy Protection Act

In addition, EPIC refers to the Children's Online Privacy Protection Act (COPPA)[135] to demonstrate the legitimacy of the FTC to take action. Similar to the FTC Act, the FTC is empowered to enforce COPPA.

This Act aims to protect the privacy of children less than thirteen years of age by regulating the collection of children's personal information by operators of websites or online services.

The requirements of COPPA apply to operators of online services, websites, and apps directed to children less than thirteen years of age[136] - as well as to operators of online services, websites and apps serving a general audience that have actual knowledge that they collect or maintain personal information from a child.[137] For operators falling within this spectrum not to violate the Act, they must:

a) Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information;[138]
b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information of children;[139]
c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance;[140]
d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity;[141]
e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.[142]

EPIC first aims to prove that Samsung can be seen as an online service provider that needs to comply with the above requirements, by citing Samsung's supplemental Smart TV Privacy Policy – the privacy policy specifically addressed to Samsung's smart TVs. In this supplemental Privacy Policy it is written: *"Smart TV services may make available educational videos and other content appropriate for children, but we do not knowingly collect any personal information from children under the age of*

[132] 18 U.S.C. § 2511(1)(c).
[133] Supra fn. 112, para. 71.
[134] *Ibid.*, para. 70.
[135] The Children's Online Privacy Act of 1998 (COPPA), 15 U.S.C. § 6501-6505.
[136] Title 16 of the Code of Federal Regulation (16 C.F.R.) §312.3
[137] *Ibid.*
[138] 16 C.F.R. §312.4(b).
[139] 16 C.F.R. §312.5.
[140] 16 C.F.R. §312.6.
[141] 16 C.F.R. §312.7.
[142] 16 C.F.R. §312.8.

thirteen without parental consent, unless permitted by law."[143] In EPIC's view, Samsung therefore presents itself as an online service operator with a general audience and being compliant with COPPA.

However, EPIC states, Samsung specifically targets some features of the Smart TV to young children; Samsung encourages parents to have their children interact with Samsung's Smart TV and the company has acknowledged that Smart TVs are commonly purchased by families with children under the age of thirteen.[144] Based on this information, EPIC concludes that Samsung violates COPPA by not fulfilling the requirement under 16 C.F.R. §312.3 – failing to ask parents' permission to record, store and transmit children's voices to a third party.

3.3.1.2.4. The Federal Trade Commission Act

Under section 5 of the Federal Trade Commission Act, the FTC is empowered to prevent unfair and deceptive acts and practices.[145] Although this law does not grant the FTC specific authority to protect privacy, it has been construed to prevent certain privacy invasions based on unfair and deceptive acts and practices.[146]

EPIC describes both the deception and unfairness of Samsung's Smart TVs, and thereby analyses the FTC Act in combination with the FTC Policy Statements on Deception[147] and Unfairness.[148]

Unfairness

A trade practice is deemed unfair if it *"causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."*[149]

Firstly, 'substantial' in this context typically involves monetary harm, but may also include unwarranted health and safety risks. Emotional harm and other "more subjective types of harm" generally do not make a practice unfair.[150]

In the view of the second element, that the injury must not be outweighed by any offsetting consumer or competitive benefits, the FTC analyses whether a practice is "injurious in its net effects".[151]

Thirdly, the FTC will examine if the injury is one that consumers could not reasonably have avoided.

EPIC states that the 'substantial injury' element is present because of Samsung's failure to take responsibility for the privacy and safety of users' recorded conversations, by which Samsung *"unreasonably creates or takes advantage of an obstacle to free exercise of consumer decision-*

---

[143] Supra fn. 112, para. 87; Samsung Global Privacy Policy SmartTV Supplement, https://www.samsung.com/uk/info/privacy-SmartTV.html?CID=AFL-hq-mul-0813-11000170.

[144] Supra fn. 112, paras. 89-91.

[145] 15 U.S.C. § 45(a)(2).

[146] Electronic Privacy Information Center, *'Federal Trade Commission: Overview of Statutory Authority to Remedy Privacy Infringements'*, https://epic.org/privacy/internet/ftc/Authority.html.

[147] Federal Trade Commission, FTC Policy Statement on Deception, 1983, https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[148] Federal Trade Commission, FTC Policy Statement on Unfairness, 1980, https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[149] 15 U.S.C. § 45 (n).

[150] Supra fn. 148.

[151] *Ibid.*

making."[152] To establish this injury, EPIC recapitulates Samsung's attempts to disclaim liability for the data privacy and security practices of companies to whom it transfers user data it has acquired from consumers, and subsequently, the fact that Samsung transmits the private conversations of Smart TV users to third-party company Nuance.[153] Moreover, EPIC points at Samsung's Privacy Policy, which did not reveal to consumers the name of the third-party company. Samsung proceeded to mislead consumers about their use of encryption to transmit recorded conversations, as to EPIC.

Secondly, EPIC writes that the inadequate protections are not outweighed by countervailing benefits to consumers or competition.[154]

Lastly, EPIC states that users of Samsung's Smart TVs could not reasonably have anticipated that by using the smart TV, their private conversations would be transmitted, sometimes unencrypted, to Nuance.[155] EPIC therefore states that Samsung's inadequate disclosures constitute unfair acts or practices.[156]

Deception

Under the FTC Deception Policy, an act is deceptive if it "*involves a representation, omission or practice that is likely to mislead the consumer acting reasonably under the circumstances, to the consumer's detriment*.[157] Deception therefore consists of three elements.

First, there must be the representation, omission, or practice that is likely to mislead the consumer. Practices that are found misleading include false written representations, misleading price claims and failure to perform promised services.[158] The threshold to determine the misleading character of the act or practice is whether the act or practice is likely to mislead, not whether the act or practice actually misled.[159]

Second, the act or practice must be considered deceptive from the perspective of the consumer acting reasonably in the circumstances. The FTC examines the totality of the act or practice.[160]

Third, the act or practice must be a "material" one, meaning that the act or practice must be likely to affect the consumer's conduct or decision with regard to a product or service.[161] The FTC will thus examine whether consumers would have chosen another product if the deception had not occurred.

EPIC explained that Samsung deceptively failed to disclose that it records and transmits private conversations through its smart TV. According to EPIC, consumers have been misled, as they were unaware of the fact that their personal conversations are recorded and transmitted to a third party. Furthermore, Samsung assured them that all recorded transmissions were encrypted, while in fact some voice recordings were transmitted unencrypted. When users did find out about this collection and transfer of data, they objected and believed it was an illegal practice, indicating that this misrepresentation was "material" to consumers. EPIC concludes that Samsung's inadequate disclosures constitute deceptive acts or practices as prohibited in 15 U.S.C. § 45(a).[162]

---

[152] Supra fn. 112, para. 107.

[153] *Ibid*., para. 103.

[154] *Ibid.*, para. 109.

[155] *Ibid*., para. 108.

[156] *Ibid.*, para. 110.

[157] Supra fn. 147.

[158] *Ibid.*

[159] *Ibid.*

[160] *Ibid.*

[161] *Ibid.*

[162] Supra fn. 112, para. 102.

3.3.1.3. Likely implications

The FTC has, up until today, not taken formal action against Samsung. The reaction of the FTC in this case could possibly have great impact because of fast emergence of interactive consumer devices in general, and the absence of subsequent case law on smart TVs both in the United States and in Europe. Whatever the outcome may be, this case study highlights interesting choices that can be made in regulating privacy implications of smart TVs. The legal provisions on which EPIC's complaint is based show possible responses on the emergence of smart TVs; by means of increasing consumer protection by enhancing transparency in privacy policies, or subsequently by enforcing specific state law like the CCPA and the ECPA that more specifically address unlawful transfers of personal data.

While it is hard to anticipate a certain outcome, the FTC Chairwoman Edith Ramirez recently addressed the specific problem of consumer devices that spy on consumers, where specific reference was made to smart TVs. Ramirez stated that "*reasonable limits on data collection and data retention is the first line of defence for consumer privacy*".[163] Based on this statement, one could state that it is likely the FTC will address the privacy implications of smart TVs.

EPIC more recently urged the FTC and the Department of Justice to conduct a comprehensive investigation to determine whether 'Always-On' consumer devices violate the Wiretap Act, state privacy laws, or the FTC Act.[164] EPIC again turned to the FTC with the aim of protecting consumers' privacy in the light of interactive consumer devices.

[163] Privacy and the Internet of Things: Navigating Policy Issues - *Opening Remarks of FTC Chairwoman Edith Ramirez,* International Consumer Electronics Show, Las Vegas, 6 January 2015.

[164] See https://epic.org/2015/07/epic-urges-investigation-of-al.html.

4. The General Data Protection Regulation

This Chapter is primarily a preview of the forthcoming General Data Protection Regulation ("GDPR" or "the Regulation"). The legislative process leading to the adoption of the new GDPR is not yet concluded but in its final phase. On 24 June 2015, the European Parliament, the Council, and the European Commission entered co-decision negotiations on the proposed GDPR. The foundation of these negotiations is the Commission's proposal of January 2012, the Parliament legislative resolution of 12 March 2014 and the General Approach of the Council adopted on 15 June 2015.[165] This section will analyse the main differences between the applicability of the current DPD and the GDPR to smart TVs.[166] The final version of the GDPR is expected by December 2015, which could lead to its formal adoption in early 2016.[167]

4.1. Smart TVs and the General Data Protection Regulation

Having described in Chapter 1 what smart TVs are and what data these devices can collect, the present chapter will consider whether these data can be seen as personal data for the purposes of the (draft) GDPR.

4.1.1. Definitions

The definitions and scope of the Regulation are closely related to the DPD. The latter is detailed in Article 2 (*material scope*), which provides that the Regulation is solely applicable to the processing of personal data. It thereby establishes the two key concepts of data protection: *processing* and *personal data*. Article 4 of the Regulation (*definitions*) provides the definition of these terms.

The first term, *processing*, has been broadly defined, such that almost any action may constitute an act of processing. Despite the European Parliament's proposed amendment of the

[165] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012)11 final, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf; European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//en; Preparation of a general approach, Council document 9565/15, 11 June 2015, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

[166] By referring to Council document 10391/15, 8 July 2015: http://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/en/pdf.

[167] European Data Protection Supervisor, 'EDPS recommendations on the EU's options for data protection reform', 2015/C301/01, 12 September 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_summary_EN.pdf.

definition of processing,[168] Article 2 GDPR is not broadened to also include "any method of processing" and, therefore, the Regulation still applies to the processing of personal data wholly or partly by automated means.[169]

The broad scope of both the DPD and the Regulation is apparent in inter alia the *Bodil Lindqvist* judgment,[170] where the concept of processing for the purposes of Directive 95/46 was examined. The reasoning applied to this provision can be transferred to the Regulation, since their definitions are identical. In this case, the CJEU ruled that displaying the phone numbers and hobbies of various people on a website qualifies as an act of processing. Also relevant is the fact that this processing was not entirely automated. It has thus been accepted that partially automated processing falls within the scope of the Regulation.

The concept of 'personal data' also has remained unchanged in relation to the DPD. Personal data is defined as all information relating to an identified or identifiable natural person.[171] Consequently, four elements can be distinguished which are relevant for the application of this concept. According to the Article 29 Working Party, these factors are: (1) it must be any information; (2) which relates to; (3) an identified or identifiable; (4) natural person.[172]

4.1.1.1. Any information

The use of the words 'any information' reflects the EU legislator's intention to afford the concept of personal data a broad scope. In the opinions of the Article 29 Working Party it is assumed that both objective and subjective data fall under the scope of 'any information'. It is not relevant whether this information is necessarily true.[173] Nor is it relevant whether the information is relevant to a person's professional or private life. In the case of *Volker und Markus Schecke GbR und Hartmut Eifert v. Land Hessen*,[174] the CJEU ruled that professional activities may also fall under the scope of private life. This finding is also reflected in the case law of the ECHR, which opted for a similar approach in the *Amann* ruling.[175] The way in which data is stored can also be a distinguishing factor. Digital files, film, printed documents, and audiotapes can all contain personal data.

4.1.1.2. Relating to

This element might seem obvious at first glance. After all, the data must somehow concern a specific person in order to qualify as personal data. However, the reality is slightly more nuanced than that. The Article 29 Working Party applies the 'relating to' test based on three factors: content, purpose and result. These factors are non-cumulative.

---

[168] Article 2 GDPR, see Council document 10391/15 under EP Position/First Reading, *Ibid.* fn. 166.

[169] *"This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing of other than automated means of personal data which form part of a filing system or are intended to form part of a filing system"* Article 2(1) GDPR.

[170] CJEU 06-09-2003 C-101/01, (Bodil Lindqvist),
http://curia.europa.eu/juris/celex.jsf?celex=62001CJ0101&lang1=en&type=TXT&ancre=.

[171] Article 4(1) GDPD, see Council document 10391/15 under Council General Approach (15/06/2015), supra fn. 166.

[172] WP29, Opinion 4/2007 on the concept of personal data, 2007, supra fn. 47.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[173] *Ibid.*

[174] CJEU 09-11-2010, C-92/09 en C-93/09, (Volker und Markus Schecke GbR und Hartmut Eifert v. Land Hessen), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62009CJ0092.

[175] ECHR 16-02-2000, Nr. 27798/95, (Amann v. Switzerland), supra fn. 71,
http://hudoc.echr.coe.int/eng?i=001-58497#{"itemid":["001-58497"]}.

In short, data of which the *content* has consequences for a person therefore *relates to* that person. Furthermore, data relate to a person when they can be used for a *purpose* that can, for example, influence an individual's behaviour. Finally, data that can be used to achieve a certain *result* for specific people can be said to relate to that person.

4.1.1.3. Identified or identifiable person

The key difference between 'identified' and 'identifiable' is that an identifiable individual has *not yet* been identified.[176] Article 4(1) of the Regulation refers to the possibilities of direct and indirect identification.[177] Direct identification can be achieved, for example, by acquiring someone's name. Identification through personal numbers such as passport numbers or social security numbers is a form of indirect identification, since additional data or means are needed to determine the subject's identity. Naturally, whether identification based on various 'identifiers' is a possibility depends on the circumstances. Indirect identification can be seen as a process of identification through a series of elements that allow one person to be singled out from a larger group. This raises the question of when the point of indirect identification is reached. In other words, this is the point when a party has sufficient reasons or possibilities to identify the subject. The Regulation addresses this question in Recital 23, which provides that it must be assessed based on all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly.[178] This test of reasonableness must take account of all relevant factors, such as the time and effort involved in the identification process. It should also take into account the most recent technological developments and advances.

The Recital also draws the line between personal and non-personal data.[179] When data are anonymous and the data cannot be traced back to a specific person (for example by aggregating the data), these anonymous data no longer qualify as personal data. After all, the data can no longer be linked to individual data persons.

4.1.1.4. Natural person

The final element entails that the rules of data protection apply, in principle, to all living people.[180] A few exceptions can be detailed, but they are of limited interest for this study.

4.1.1.5. Special categories of data

Read in conjunction, the above elements provide a framework for the determination of whether certain information constitutes personal data. Just like the DPD, the Regulation then makes a further distinction between 'ordinary' data and special categories of data. Article 9 (Processing of special categories of personal data) provides that the following data fall within a special category: data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, tradeunion

[176] Supra fn. 47.

[177] Article 4(1) GDPD, see Council document 10391/15 under Council General Approach (15/06/2015), supra fn. 166.

[178] *Ibid.*

[179] *Ibid*.

[180] Supra fn. 47.

membership, and the processing of genetic data or data concerning health or sex life..[181] In the text of the first reading Position of the European Parliament, biometric data, data concerning administrative sanctions, judgments, criminal or suspected offences, and convictions are also included.[182] Clearly, this sub-category is also of a broad nature. For these special categories of data, a stricter regime is in place, which will be discussed further below. For now, it suffices to mention the existence of this separate category.

4.1.1.6. Territorial scope

Besides the Regulation's material scope, described above, Article 3 (*Territorial scope*) establishes its (extra-) territorial applicability.[183] The first paragraph indicates that the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, whether or not the processing takes place in the Union. Paragraph 2 is one of the Regulation's new additions, stating that the Regulation also applies when a processor is not established in the EU, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of such data subjects as far as their behaviour takes place within the EU. This reflects the legislator's intention to broaden the Regulation's scope in comparison to the Directive.

4.1.2. Application

The above description of the Regulation's scope can be applied to the case of smart TVs, as set out in Chapter I. Insofar as data does not constitute personal data for the purposes of the Regulation, all its further provisions lose relevance. The various practices described in Chapter I will now be considered in terms of their legal implications.

4.1.2.1. Voice recognition

It was established above that a smart TV is able to record sounds from its surroundings and to recognise speech patterns, which in turn can be registered as commands. One might ask whether personal data are being processed through this function. The outcome may differ in various scenarios.

Firstly, it is worth considering the content of the conversations that could possibly be recorded. Given that the TV usually takes up a central location in households, it is likely to pick up a considerable amount of vocal interaction. Of course, the content of these conversations is never the same, and they might contain an infinite number of word combinations. Undoubtedly, these words will include names, places and other identifying information. It will also include a degree of 'snow', i.e., information that does not contain any germane or identifying information.

Returning to the criteria put forth in the Regulation, one must keep in mind that the definition of personal data speaks of *any* information relating to natural person. By analogy, one

[181] Council document 10391/15 under Council General Approach (15/06/2015), Ibid. fn. 166.

[182] The exact wording of this article is still controversial. See Council document 10391/15 under EP Position/First Reading, Ibid. fn. 166.

[183] Council document 10391/15, Ibid. fn. 166.

could refer to the Dutch Supreme Court's decision in *Dexia*,[184] in which it was ruled that recorded phone conversations could under certain circumstances qualify as personal data. Furthermore, it has been shown above that it is relatively straightforward to indirectly identify an individual, so long as enough identifiers can be collected. Since smart TVs do not distinguish which sounds are recorded, and which are not - after all, all sounds must be filtered in order to recognise voice commands - it appears warranted to conclude that sound recordings from living spaces qualify as personal data. The question remains whether this recording also constitutes an act of processing. Article 4(3) of the Regulation shows that the processing of personal data includes the collecting, recording, storing, use and transmission of information. It is not relevant whether these actions are automated or not. In conclusion, it can be stated that the recording of conversational content is a form of personal data processing for the purposes of the Regulation. This processing could also include personal data listed in the special category of Article 9.

4.1.2.2. Motion control and facial recognition

It was established in Chapter I that smart TVs are capable of recording images and recognising faces. Having determined that sound recordings fall within the Regulation's scope, the same question can be asked with regard to these visual recordings.

Images require a more nuanced analysis than sound. Photographs may allow for the direct identification of individuals. Portrait images are generally treated as sensitive data, since they allow for the determination of traits such as ethnicity.

The Regulation does not yield a different outcome. After all, images of persons are information relating to an identified or identifiable natural person. What was not considered in the above section regarding sound recordings is the possibility that *everyone* near the device can be recorded. Furthermore, it is possible that the recorded images and sounds are of minors or visitors to the household and not the ordinary/registered users. In such cases, specific legal scenarios would arise due to the particular status of the minors or visitors.

As with sound, the recording of this information constitutes an act of processing. Consequently, it can be concluded that motion control and facial recognition fall within the scope of the Regulation.

4.1.2.3. Account creation

This category of data is meant as a residual category for all data other than visual or audio recordings. However, that should not raise the impression that this category is of lesser importance. On the contrary, for the purposes of this report, the following is of great significance.

Firstly, the information that can be linked to a user account will be discussed, even though it should be acknowledged that many users will not use such an account. To a lesser extent, the same may apply to voice and motion commands. However, this residual category also includes data which are relevant for every user and are therefore of great consequence for this research.

Account creation requires the entry of information such as one's name, e-mail address, date of birth and postal code. Evidently, one's name constitutes personal data. Although the other data may not qualify as personal data in and of itself, they can be used to identify an individual when read in conjunction. The account information is therefore without question a form of personal data.

---

[184] HR 29-06-2007, ECLI:NL:HR:2007:AZ4664 (Dexia), para. 3.8 f.f. http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2007:AZ4664.

The discussion will now turn to the scenario where users choose not to register an account. After the fracas surrounding Samsung smart TVs' terms and conditions, the tech-giant has not been granted a moment's peace. The initial controversy was soon followed by a news report that accused Samsung of injecting advertisements into content that users played from their home networks.[185] This content was not streamed or downloaded, but acquired independently by the user. Samsung soon responded with an official apology, stating that this incident was the result of an error. In any case, it shows that the interjection of advertisements in local content is at least technically possible. Furthermore, one of the smart TV's features is the capacity to display content based on the user's viewing history. With this in mind, it is not unthinkable that viewing history would also be used to offer targeted advertising and personalised content, as is the case on many websites.[186]

Analysing viewing behaviour is an obvious application of the collected data. This is evidenced by the developments in online marketing that occurred throughout the last decade. The rise of tracking cookies, browser fingerprinting, and behavioural targeting shows that an enormous demand exists for information on the interests and preferences of Internet users.[187] It may then be no surprise that the same is being attempted with smart TVs.

Before returning to the definition of personal data, it is worth considering which data are actually being collected. In order to suggest additional content, smart TVs must be able to register the user's viewing behaviour. From a technical perspective, it is not unthinkable that the duration of viewing, the time of viewing and the identity of viewing are also registered, and whether the viewed programme is received through a broadcast, online streaming, or from local network sources. The TV's IP-address can provide an estimate of its location. It is also imaginable that the TV registers the app that is used to provide content, such as a Netflix app, for example. In this case, Samsung *and* Netflix might have an interest in registering this information. As an aside, the interesting question is raised of how these apps are presented on screen and how their rank or order is determined. However, questions of prominence and findability fall outside the scope of this report.

Do these categories all contain information relating to an identified or identifiable natural person? Given that no account has been registered, there is no reason to assume that it concerns an identified person. Thus, it comes down to a question of identifiableness. As established above, this criterion depends on the means by which one can reasonably expect the person in question to be identified. In any case, the processor in question possesses information as to the content, time and duration of viewing as well as app usage. The user's location can be approximated through the IP-address used.[188] Naturally, the answer will differ on a case-by-case basis, but due to the diversity of available TV programmes, streams and other content, relatively quickly there would be enough information to render the user identifiable. In the words of the Regulation, it allows conclusions to be drawn regarding the social, mental and cultural identity of that person. It can be concluded that even when smart TVs are not equipped with a camera and microphone, and the user does not register an account, personal data might be processed. As discussed in Chapter III, research conducted by the Dutch Data Protection Authority concluded that information on one's viewing

[185] Roettgers J., *Samsung TVs start inserting ads into your movies*, 10 February 2015, https://gigaom.com/2015/02/10/samsung-tvs-start-inserting-ads-into-your-movies/.

[186] Titlow J.P., *How Yahoo's homepage delivers personalized news to 700 million people*, 2012, http://readwrite.com/2012/02/10/how_yahoos_homepage_delivers_personalized_news_to.

[187] Zuiderveen Borgesius, "Behavioural Sciences and the Regulation of Privacy on the Internet", ALSLS 2014/54, p. 3 f.f. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2513771.

[188] Whether an IP-address constitutes personal data itself, is currently the subject of a prejudicial question to the CJEU in the case C-582/14 Breyer v Bundesrepublik Deutschland, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CN0582. The Article 29 Working Party already considers IP addresses a form of personal data, see: Opinion 01/2012 on the data protection reform proposals. The Regulation itself merely makes an ambiguous reference to IP addresses in Recital 24, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

history could have a significant impact on the right to private life, such that it could be considered sensitive data.[189] The increasing ability to select our own content through on-demand television makes it more interesting and more straightforward to determine personal preferences based on viewing behaviour.

4.2. The Regulation's level of protection

Having considered in the previous section the question of whether smart TVs are covered by the Regulation's scope in most cases, and having answered this question affirmatively, the present section will consider the safeguards offered by the Regulation, based on the same scenarios. It is not intended to provide a comprehensive overview of the Regulation's provisions. Instead, the focus will be on the provisions that relate to the legal questions that arose in Chapter 3, thereby providing insights into the level of protection afforded by the Regulation so that it may be evaluated further below.

4.2.1. Key provisions

In the second section of the Regulation, Article 5 lays down the same principles as can be found in Article 6 of Directive 95/46/EC, albeit in a more specific form and with certain additions.[190] As will be discussed below in more detail, the concept of consent is specified in a more detailed manner. As discussed in Chapter II, these principles indicate the limits of what constitutes legitimate processing. As such, they provide a general framework for the other provisions and are essential for an understanding of the Regulation's system.

Applied to our by-now-familiar scenario, these principles reflect how Samsung should treat the collected personal data. A more specific analysis is not possible since we lack further information regarding the exact act of processing. Its treatment here serves an illustrative purpose and paves the way for discussion in the following sections.

Article 6 of the Regulation sets out the grounds on which legitimate processing must be based. This method, also recognisable from the Directive, entails that every act of processing must fulfil one of the following conditions:

> *(a) the data subject has given unambiguous consent to the processing of their personal data for one or more specific purposes;*
> *(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
> *(c) processing is necessary for compliance with a legal obligation to which the controller is subject;*
> *(d) processing is necessary in order to protect the vital interests of the data subject or of another person;*
> *(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*

[189] Dutch Data Protection Authority, supra fn. 109.

[190] Council document 10391/15, supra fn. 166.

> *(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. […].*[191]

Of the above grounds, three are of particular importance for our scenario, as is apparent from the TP-Vision decision:[192] (a) consent, (b) contractual obligations, and (f) the legitimate interest of the controller.[193] Consideration will now be given of whether these conditions can form a basis for the acts of processing described in Chapter 3.

4.2.1.1. Contractual duties

On the face of it, this ground seems an obvious method to legitimise data processing. After all, Samsung could simply request processing permission in their sales contracts, as in article 7(b) DPD. However, the interpretation given to this provision by the Article 29 Working Party is highly restrictive:

> *"The provision must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller."*[194]

In short, the processing must be *essential* to the fulfillment of the contract. Furthermore, the CBP stated in the TP-Vision case that 'a justification for the processing must be present in relation to the specific, individual data subject involved'.[195] The purchase of smart TVs is primarily a sales contract, which has little or nothing to do with the processing of visual or audial personal data. This provision is therefore less suitable than one might initially expect.

4.2.1.2. Legitimate interests of the controller

When this ground is invoked, the controller's interest must be weighed against the fundamental rights of the data subject. According to Article 29 Working Party, the 'legitimate interests of the controller' can include a wide variety of different interests.[196] Ultimately, the weighing of controllers' and subjects' interests must determine whose claim prevails. Recital 38 of the Regulation elaborates on this matter. It stipulates that, besides the fundamental rights and freedoms of the data subject, his or her reasonable expectations must also be taken into account. However, as described above, article 7(f) DPD has significantly changed in regard to the protection of minors. When the data subject is a child, it is not likely that the legitimate interests of the controller will override the interests of the child.[197]

---

[191] Article 6(1) GDPR, see Council document 10391/15 under Council General Approach (15/06/2015), supra fn. 166.

[192] Dutch Data Protection Authority, *op. cit.* fn. 109; Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[193] Of these conditions, consent is the most commonly claimed in practice. See WP29, Opinion 06/2014, supra fn. 54.

[194] *Ibid.*

[195] Dutch Data Protection Authority, supra fn. 109.

[196] WP29, Opinion 06/2014 supra fn. 54.

[197] Article 6(f) GDPR, see Council document 10391/15 under Council General Approach (15/06/2015), supra fn. 166.

This provision has been the subject of frequent criticism under the DPD, since it is open to diverse interpretations. Again, this proves to be the case. Part of this criticism was the complaint that the weighing of interests can only be conducted once the processing has already taken place, i.e., when unreasonable processing practices are discovered and a court is seized upon to conduct such a test.[198]

In the case of smart TVs, Samsung's interest is primarily related to providing an advertising platform for services and content (including that of third parties). This is especially the case when viewing behaviour is analysed. The reasonable expectations of the buyer will for the most part be based on the technical specifications of the smart TV itself. Of course, smart functions can also affect expectations, although it is unlikely that users will expect or desire advertisements based on viewing behaviour.

The balancing of fundamental rights and freedoms of the data subject against the interests of Samsung is not straightforward. An important factor is the fact that smart TVs tend to take up a central position in the household, where one is especially justified in objecting to surveillance and incursions on private life. The use of television and the selection of content are also relevant here. When weighing these interests in the case of TP-Vision, the CBP decided in favour of protecting the data subject.

4.2.1.3. Consent

*A*s discussed previously, consent is the most commonly-used ground and, according to the CBP, the only ground which is suitable for data processing by smart TVs.[199] This might also explain why the European legislator decided to introduce additional safeguards in the Regulation. Article 4(8) defines consent as follows:

> *the data subject's consent means any freely given, specific and informed* ***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*[200] (emphasis added).

Under the DPD, explicit consent is only required for the processing of the special categories of personal data. This test was introduced in the GDPR draft as a general requirement for the granting of consent, but is not taken over by the Council.[201]

Secondly, this formulation shows that consent cannot be given implicitly, as it refers to a 'statement' or 'a clear affirmative action'.

Article 7 GDPR, in addition to the Directive, details conditions for consent. It prescribes that the controller must carry the burden of proof for the data subject's consent.[202] In addition, when consent is given in the context of a written declaration that also concerns another matter, the requirement to give consent must be presented as clearly distinguishable in its appearance from this other matter.[203] It also allows data subjects to retract their consent at all times, in a manner which should be as easy as the act of giving it. In such cases, the data subject must then also be informed

---

[198] Bits of Freedom*, A loophole in data processing,* 2012, p. 10, https://www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf.

[199] *Ibid.*; Dutch Data Protection Authority, supra fn. 109.

[200] Council document 10391/15 under Council General Approach (15/06/2015), supra fn. 164.

[201] *Ibid.*

[202] Article 7(1) GDPR, see Council document 10391/15 under Council General Approach (15/06/2015), supra fn. 166.

[203] Article 7(2) GDPR, *Ibid.*

whether this retraction would lead to a termination of services provided by the controller.[204] Finally, as described in Chapter II, Article 7 stipulates that consent is 'purpose-limited', and loses its validity when its purpose ceases to exist or as soon as the processing of personal data is no longer necessary for the purpose for which they were originally collected.[205] Significantly, the final sentence of this paragraph states that the execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision.

Samsung must fulfil these conditions if it wishes to process personal data based on consent. Data subjects must be asked for their consent and in such a way that it is clear what they are consenting to. Samsung must also clarify which data are being processed. A 2014 study shows that this is not always the case;[206] it concludes that the privacy policies of various smart TVs do not cover all processing purposes and that the request for consent is formulated in overly ambiguous terms.

4.2.2. Other relevant provisions

This section will explore other provisions that might be relevant for the users' level of protection. In Article 8 (Conditions applicable to child's consent in relation to information society services) additional safeguards are set out for the processing of data of children younger than 13 years.[207] Such processing shall only be lawful if and to the extent that consent is given or authorised by the child's parent or legal guardian. Moreover, the controller has to make reasonable efforts to verify in such cases that consent is in fact given or authorised by the holder of parental responsibility over the child, taking into consideration the current state of technology.[208] For Samsung, this means that they may have to request permission during installation, because (as established in section 2), the possibility exists that the personal data of children could be processed. This was also clearly argued in EPIC's complaints to the FTC.[209]

In light of the fact that personal data falling under the 'special categories' may also be processed with facial recognition features, it is worth considering Article 9 (Special Categories of Data).[210] These categories are subject to additional safeguards, as they are in Article 8 DPD. According to paragraph 2, they may only be processed with the subject's consent. This consent must fulfil the same definition as described above. By way of exception, certain additional grounds are listed, although these are of limited relevance for this report. For our case study, it could mean that consent is required for the activation of facial recognition applications.

Article 14 (Information to be provided where the data are collected from the data subject) requires the controller to inform the data subject of various matters.[211] It lists information that must be made clear to the data subject, and can be seen as a set of demands for the privacy policies of the future. Most importantly, the controller's identity must be communicated, as well as the purpose of processing, the period of retention, and the rights of the data subject. This is not a recent

[204] Article 7(3) GDPR, *Ibid.*

[205] Article 7(4) GDPR, Council document 10391/15 under EP Position/First Reading, *Ibid.*

[206] Schermer B.V. and Falot N., *Analyse privacy voorwaarden Smart TV*, 2014, p. 29, http://www.considerati.com/wp-content/uploads/2014/09/201400820Onderzoek_privacyvoorwaarden_smarttv.pdf.

[207] Council document 10391/15 under Council General Approach (15/06/2015), Ibid. fn. 166.

[208] Article 8 GDPR, *Ibid.*

[209] EPIC, supra. fn. 112.

[210] Council document 10391/15 under Council General Approach (15/06/2015), supra fn. 166.

[211] *Ibid.*

development, although the findings from the second section show that it is not always observed in practice.

The 'right to be forgotten', as established in the case of Google/Spain,[212] has also found its way into the Regulation. It is mentioned here because it is closely related to the granting of consent and the subsequent right of retraction. It is laid down in Article 17 (right to erasure and "to be forgotten") and grants the data subject the right to obtain from the controller the erasure of personal data relating to them.[213] This right can be invoked, inter alia, when the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, or when the data subject withdraws consent.

As such, smart TV owners can request the removal of collected data once they decide to stop using the device. This grants them a certain degree of control over the information relating to them.

Two articles of particular relevance for our scenario are Articles 19 (right to object) and Article 20 (Profiling).[214] These provisions allow users to object to 'profiling' practices, defined as follows in Article 4(3) bis:

> *Profiling means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.*

The analysis of viewing history by smart TV providers would appear to fit this definition, since it involves the evaluation of personal preferences and behaviour. This is supported by the CBP's findings in the *Ziggo* case. This provision is directed at the 'behavioural targeting' techniques that are applied by some market participants. In accordance with Article 19, data subjects can object to such profiling. Furthermore, pursuant to Article 20(1a), these techniques may only be applied in order to perform a contract, under authorisation by a Union or Member State law, or based on the subject's consent. Should Samsung, or Netflix, wish to analyse viewing behaviour, the company will have to qualify for one of these grounds. Two possibilities would be obtaining consent, and the use of contracts where Samsung or Netflix commits itself to provide content suggestions based on the user's viewing behaviour.

Another noteworthy provision is found in Article 23 (privacy by design and by default).[215] It creates a duty for controllers and processors to implement appropriate and proportionate technical and organisational measures, having regard to the state of the art, current technical knowledge, international best practices, and the risks represented by the data processing procedures. In relation to the findings in Chapter II, this means that controllers must take additional measures in order to ensure that their products meet the relevant specifications and must develop a compatible visual design. That being said, privacy by design and by default are listed in 79(2a)(e) as criteria to decide on the imposure of administrative fines and the amount of these fines. Moreover, these fines can rise up to 1,000,000 euro or 2% of global revenue, a measure that could facilitate enforcement efforts.[216] This rise of the maximum of administrative fines may provide multinationals a powerful incentive towards compliance.

---

[212] CJEU, C-131/12, supra fn. 45.

[213] Council document 10391/15 under Council General Approach (15/06/2015), supra fn. 166.

[214] *Ibid.*

[215] *Ibid.*

[216] See Articles 79a(3), see Council document 10391/15 under Council General Approach (15/06/2015), supra fn. 166.

A final point of interest is the legality of international data transfers. In the case of TP Vision, data were stored locally in the Netherlands, but it is of course possible that other providers would choose to transfer it elsewhere. This matter is regulated by Articles 41 to 45 bis.[217] Article 41 permits transfers to third countries insofar as they have been approved through a formal 'adequacy decision'. Under Article 42, such transfers are also permitted when it can be established that the country of destination offers appropriate safeguards. Finally, under Article 43, controllers may legitimise transfer to third countries by subscribing to so-called 'Binding Corporate Rules', or BCRs.

It appears that the Directive's system for the regulation of third country transfers was too restrictive and exacting, since large-scale international transfers often took place within the companies themselves. One article described the Regulation's revised approach as follows: 'Regarding the problem of structural transfer of personal data within multinationals, the proposal at least offers clarification by way of a codification of specific rules for BCR which were developed in practice. The starting point that processors also make use of BCRs lends feasibility to third countries for the purposes of offshoring and cloud computing. However, it is not yet clear how processors are expected to use BCRs.

Finally, the proposal does not offer a solution to the problem of data requests by government authorities in third countries. In light of the on-going globalisation process, the intensification of international data flows, and the associated risks for the protection of personal data, it is essential that the new rules for transfers are reconsidered and improved, such that they can provide a workable, future-proof framework for international data processing and the protection of data subjects.'[218]

It can be concluded that the rules regarding international transfers have been clarified in certain areas. Although the Regulation might provide more legal certainty regarding cross border personal data transfers, the recent CJEU decision in the *Max Schrems* case might provide the opposite.[219]

4.3. What is an adequate level of protection, and is it offered by the Regulation?

So far, this report has considered the definition of smart TVs and the data they can collect, as well as its scope and safeguards it provides. This section will consider the requirements of adequate protection of smart TV users and critically evaluate the Regulation on this basis.

4.3.1. What requires protection and why?

An adequate level of protection assumes that there is an object in need of protection. Only once it is clarified *what* is being protected can we consider reasons as to *why* such protection is needed. Without this step, any further reasoning would be baseless.

---

[217] Council document 10391/15, supra fn. 166.

[218] Wisman N. and de Vries H.H., *Doorgifte van persoonsgegevens onder de nieuwe Verordening*, P&I 2012, p. 117, http://www.recht.nl/vakliteratuur/staatsrecht/artikel/358929/doorgifte-van-persoonsgegevens-onder-de-nieuwe-verordening/.

[219] In this case, the Court declared the Safe Harbor Decision invalid. For more information see:

http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre=; CJEU, 6 October 2015, C-362/14 (*Max Schrems*), supra fn. 56.

Ultimately, the rights to private and family life (Article 7 of the Charter of Fundamental Rights of the European Union) and to protection of personal data (Article 8 of the Charter) are the objects of protection. However, it is instructive to explore why the physical space that smart TVs 'occupy' is worthy of protection, as the object of protection is the free space created in one's own home. This view is related to the scope of Article 7 of the Charter, which covers "private and family life, home and communications". This free space is used to pursue numerous activities. Television viewing, which is taking place on a great scale across the globe, is one of these activities. It is done for many reasons, mostly importantly entertainment and the acquisition of knowledge. Traditionally this was achieved through 'dumb' TVs, which could only display images. As described above, this has changed dramatically with the introduction of smart TVs. Suddenly, the viewer may also be observed in his own home. As a consequence, people may start to adapt their behaviour, consciously or subconsciously. This should not happen in a space that ought to be free and where one can view content and consider information based on their personal preferences. The object of protection should be the space where, in a word, you can be yourself. Julie Cohen more precisely articulated this sentiment:

> *A fundamental assumption underlying our discourse about the activities of reading, thinking, and speech is that individuals in our society are guaranteed the freedom to form their thoughts and opinions in privacy, free from intrusive oversight by governmental or private entities.*[220]

While Cohen is concerned with reading, the same reasoning can be applied to viewing. These two methods of registering information do not differ fundamentally. Cohen also partially answers the question of *why* protection is needed, with reference to the U.S. Constitution's First Amendment, which enshrines the U.S.'s conception of the freedom of speech. Neil Richards also supports an argument for privacy of the home based on freedom of speech:

> *We often think of privacy rules as being in tension with the First Amendment, but protection of intellectual privacy is different. Intellectual privacy is vital to a robust culture of free expression, as it safeguards the integrity of our intellectual activities by shielding them from the unwanted gaze or interference of others. If we want to have something interesting to say in public, we need to pay attention to the freedom to develop new ideas in private, either alone or with trusted confidants. Free speech thus depends upon a meaningful level of intellectual privacy, one that is threatened by the widespread distribution of electronic records of our intellectual activities.*

In this work, titled 'Intellectual Privacy',[221] Richards makes the argument that an effective enjoyment of the right to freedom of expression requires a space in which one can explore and develop ideas without interference. Without such a space, the protection of free speech risks becoming meaningless, as there would be no opportunity to develop ideas worth protecting. This reasoning is relevant for the use of television in a home environment. The space referred to by Richards comprises physical locations, or 'spatial privacy',[222] as well as 'intellectual space' - also referred to as 'freedom of private intellectual exploration'.[223] Together with the basic principle of 'freedom of

[220] Cohen J.E., *A Right to Read Anonymously*, CLR 1996, p. 2, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=17990.

[221] Richards N., *Intellectual Privacy*, TLR 2008, p. 387, http://ukcatalogue.oup.com/product/9780199946143.do. See further, Richards N., *Intellectual Privacy*, 2015, supra fn. 9.

[222] *Ibid.*

[223] *Ibid.*

thought and belief' and 'freedom of confidential communications',[224] these concepts form the building blocks of 'intellectual privacy'.

The European Court of Human Rights has taken a similar approach in its jurisprudence, and raised concerns that echo those raised by Richards. It has observed, for instance, that "thought and opinions on public matters are of a vulnerable nature", and:

> *Therefore the very possibility of interference by the authorities* ***or by private parties acting without proper control*** *or even with the support of the authorities may impose* ***a serious burden on the free formation of ideas*** *and democratic debate and have a chilling effect*[225] (emphasis added).

The type of chilling effect on freedom of expression that is envisaged here concerns the right to seek or access information and ideas without interference. The chilling effect comes in no small measure from the "multiveillance" of users' consumption of broadcasting as well as their other online activities carried out via smart TVs (see the Introduction, above, for further details).

4.3.2. What is adequate protection?

Having determined the object and reasons for protection, it is now possible to investigate how this space can be protected in an adequate manner. The concept of personal data is highly suitable for the realisation of this protection. Fried's view of privacy is relevant in this regard: '*Privacy is the control we have over information about ourselves*'.[226] Even more famous, perhaps, is Westin's definition of privacy: '*the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others*.'[227]

These statements share two common elements: (1) control over information; and (2) the information relates to ourselves. The second element might sound familiar, given that it appears in the definition of personal data from section 2. As we saw with Articles 7 and 8 of the Charter, it can be said that these rights are closely connected. The protection of private life cannot exist without individual control over one's own personal data.

The key concept for assessing 'adequacy' of protection is *control*. Control describes the autonomy of individuals to counteract interferences with their private life. In the words of Rössler:

> *The reason why people consider these types of violation of "informational privacy" as damaging and alienating, is not only the fact that they perceive them purely and simply as unpleasant, embarrassing and hurtful and therefore reject them – this is of course true; but also and above all it is the fact that those violations of "informational privacy" result simultaneously in violations of the conditions of autonomy: individual autonomy depends on "informational privacy".* (Quotation marks added).[228]

---

[224] *Ibid.*

[225] *Altuğ Taner Akçam v. Turkey*, no. 27520/07, § 81, 25 October 2011, http://hudoc.echr.coe.int/eng?i=001-107206#{"itemid":["001-107206"]}.

[226] Fried, *Privacy*, YLJ 1968, p. 482.

[227] Westin A.F., *Privacy and Freedom*, New York: Atheneum 1967, p. 7.

[228] Rössler B., *Der Wert des Privaten*, 2001, p. 203, http://www.suhrkamp.de/buecher/der_wert_des_privaten-beate_roessler_29130.html. Translated into English by the editor.

The need for control of information is central to the position of the Dutch and German privacy watchdogs regarding the level of protection needed for smart TVs. As seen in the investigation of TP Vision,[229] the Dutch DPA listed a number of requirements for compliance with data protection law. This does not necessarily show the adequacy of this legislation, but it illustrates an emphasis on means that enhance the individual's autonomy. The requirements included a clear description of the aims of processing, such that the data subject is capable of granting informed consent. Thus, information duties play an important role in the views of the Dutch Data Protection Authority. The aforementioned four general rules that must be observed in relation to smart TVs, as formulated by the German authorities, need to be taken into account too. [230]

It is worth nothing that this statement also calls for the possibility to make anonymous use of the TV, a sentiment echoing Cohen's 'right to read anonymously' at the start of this section.

Accordingly, one could start with the following principles in order to determine what constitutes adequate protection. Adequate protection entails that the user of a smart TV is offered the possibility to make entirely anonymous use of the device. Only then can the safe space needed for 'intellectual privacy' be enjoyed effectively. Firstly, this necessitates that all information used for the processing of personal data is displayed clearly and in descending order according to their 'impact'. In order to grant the user effective control over his or her personal data, an adequate level of protection demands that processing is based on the user's consent. There should be no other option available but to process personal data on the basis of this condition. If refusal should mean that the user is no longer able to receive certain services, an assessment should be made whether this consequence is reasonable. For example, it is difficult to make content suggestions without user profiles. If the user does not grant permission for the creation of a profile, this could mean that the service remains unavailable. For many users, this could be seen a reasonable option, so long as they are clearly informed beforehand.

An adequate level of protection also requires the provider of smart TVs to apply the principles of 'privacy by design' and/or 'privacy by default'. This affords less technically informed users to make a conscious choice before using the device.

The degree of control for users should apply to the entire 'life cycle' of the processing, from controller to processor to sub-processor. This entails that the user must have control over the storage or deletion of his or her personal data.

4.3.3. Does the Regulation provide an adequate level of protection?

Now that the concept of adequate protection has been defined, it can be investigated whether the Regulation meets this requirement. This will be done though a discussion of relevant provisions.

4.3.3.1. Anonymity

The Regulation only bears one mention of the word 'anonymous', in Recital 23, which expressly excludes anonymous data from the concept of personal data since identification is no longer possible.[231] Anonymity is not treated further as it is not included in the Regulation's objectives, which focuses instead on principles and processing conditions. This approach acknowledges and

[229] Dutch Data Protection Authority, supra fn. 109.

[230] Supra fn. 73.

[231] Council document 10391/15, supra fn. 166.

accepts that the processing of personal data takes place, and attempts to create safeguards for this practice. It may be possible to recognise a type of anonymity in the consent requirement.

4.3.3.2. Consent

As discussed previously, the lawful processing of personal data is only possible on the basis of the conditions set out in Article 6. One of these conditions is consent. As already pointed out above, processing of personal data from smart TVs should *only* be possible on the basis of consent, because the other conditions provide insufficient control for the data subject. However, the Regulation provides five other grounds besides consent, of which two are likely to be suitable for smart TV data processing. In this regard, the level of protection appears inadequate. There is no clause that would force Samsung or other providers to obtain the data subject's consent. This could be achieved by creating a separate category of 'essential services', with a regime similar to that for special categories of personal data in the Directive, where consent is the only possible ground for processing. Essential services (or facilities) should be services that play an important role in the day-to-day reality of users and are crucial for receiving knowledge and gathering information. Examples include television and Internet but also libraries. A comparable step was already made when the Dutch Protection Authority prohibited public broadcasters from operating a so-called 'cookie wall'.[232] The further ramifications of such an approach would be difficult to predict, but it would answer to the need for the protection of 'intellectual privacy'.

The consent requirement laid down in the Regulation involves a detailed definition which precludes implied or default consent. This is a positive development, since this affords the data subject a greater degree of control. A tension exists between consent and anonymity, in that refusal of permission must also be registered as a form of preference. A similar discussion is taking place regarding cookies; a cookie is required to register the very fact that a user does not wish to make use of cookies. However, this need not form a great cause for concern, as the impact of this singular processing is limited. 'Privacy by default' could also provide an outcome by making anonymous use the default setting. A certain degree of anonymity is therefore achievable by refusing to grant consent. However, it is no silver bullet, as Borgesius argues in '*Privacy protection can be done better: the myth of informed consent* ('Privacybescherming online kan beter: De mythe van geïnformeerde toestemming').[233] He bases his position on the observation that many people tend to click 'yes' wherever necessary, such that the protection granted by data protection laws is largely illusory. He proposes an emphasis on *empowerment* - which is comparable to the previously discussed principle of control - and *protection*. This protection must be afforded through legislation. As we saw, the EU legislator has attempted to improve consent requirements in the Regulation. One could state that shortcomings in the consent requirement have been adequately amended by the Regulation and that it grants data subjects a sufficient degree of control. A point of improvement would be to make the consent requirement mandatory for essential services and facilities.

It deserves consideration that certain services, e.g. Facebook, are not available without the user's consent for data processing. Currently, the only option is not to use this service. However, this choice is complicated by the strong network effects displayed by many online services. One might choose a service that does not systematically infringe her/his rights, but it is unlikely that her/his friends are also registered there. The current consent requirement does nothing to change this. Access to services is not a given; users must pay with their personal data, rather than with currency.

---

[232] CBP, *Brief aan de staatssecretaris van Onderwijs, Cultuur en Wetenschap, inzake cookiebeleid NPO*, 2013, https://cbpweb.nl/sites/default/files/atoms/files/med_20130205-cookies-npo.pdf.

[233] Zuiderveen Borgesius, *Privacybescherming online kan beter*, NJB 2015/14, p. 878 f.f., http://www.ivir.nl/publicaties/download/1536.

One solution would be to provide for a remunerated option, or to offer a stripped-down version of the service that only provides basic functionalities. An important provision in this regard is Article 7(4) of the Regulation, which prescribes that execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of personal data that is not necessary for the execution of the contract or the provision of the service.[234]

4.3.3.3. Other requirements

The other requirements for an adequate level of protection, such as 'privacy by design', control over personal data removal, and clear information duties, can be found in the Regulation. The above has shown that controllers and processors, on the basis of Article 23, must observe 'privacy by design'. Furthermore, the 'right to be forgotten', the informational duties, and retraction of consent are all included. Additional safeguards such as the 'right to object' and rules on profiling and international data transfers further strengthen the overall framework and thus the subject's level of protection.

It can be concluded that the Regulation comes close to a level of adequate protection. Insofar as smart TV providers and third parties such as Netflix comply with its prescriptions, smart TV users will be able to exercise effective control over their personal data. Of central importance is the consent requirement, which ought to be mandatory in this scenario. Here the Regulation could still be improved. Only insistence on this condition can ensure users have the choice to view content anonymously.

[234] Supra fn. 205.

Concluding Analysis

It's undeniable: big data have entered the audiovisual domain. Traditional broadcasting is quickly complemented – and more importantly – substituted by non-linear services. But both are no longer "disconnected" from the user. Through interconnectivity providers and users can interact. Based on the exchange of personal data - the new currency – providers can optimize their offer and users get recommendations and selections based on their personal profile. These benefits are one side of the coin. On the other side we see concerns about manipulation, cherry-picking, reduction of consumer choice, and information isolation.

One of the clearest examples of these developments is smart TVs. These devices are connected to the Internet offering the aforementioned possibilities. The growth of smart TVs is unstoppable. Within one or two years the majority of European households will have one. But if one were to include other devices with similar functionality (tablets, smartphones and set-top boxes), we have already reached the point of no return.

In this *IRIS Special* we describe the functionality of smart TVs in more detail and discuss the most relevant aspects of the regulatory and policy context. We also give background information on the first cases where concern was expressed about the privacy implications of smart TVs. From this we can at least draw the following conclusions:

1. The privacy issues related to smart TVs are multifaceted, because the smart TV ecosystem comprises of many providers with varying processing activities involving users' personal data. Information is gathered through traditional interaction such as the remote controls and/or in combination with platforms for selections (i.e. electronic programming guides). But devices are even smarter and include voice recognition, motion control, and facial recognition, and collect/use data from the user as part of his/her account. This is not an exhaustive list but we should be aware that technological developments will introduce other options. Apps make it possible to combine physical and medical data with the use of audiovisual content.
2. The analysis of the existing legal and policy environment depicts a highly fragmented situation consisting of special media regulation (such as the audiovisual media services directive, other sector-specific regulation (telecommunications, ecommerce, e-privacy) and general privacy regulation applicable to smart TVs (Data Protection Directive and GDPR). An umbrella of fundamental rights – first of all freedom of expression and privacy/data protection - complements this landscape.
3. Traditional media regulation, such as the Audiovisual Media Services Directive, has a long historical basis dating back to the 1970s. Interactivity and privacy were not seen as topics that needed to be included. Even the latest revisions were merely focused on including new developments from this traditional perspective: non-linear services became part of it, but only as something that delivers audiovisual content in a different way. However, the key actors – both providers of audiovisual services and the users – are at the core of this traditional framework. Possibilities and limitations, for example rules on youth protection, therefore directly affect the possibilities of the smart TV environment.

4. The functionality and applicability of smart TV is impacted more directly by other sector-specific instruments, which are of a more generic nature and are not meant to specifically address the audiovisual sector. This is the case with communications regulation impacting the underlying infrastructure such as the Internet, and thereby providing safeguards for the exchange of information. In the EU directives for the communications sector special attention is given to conditional access, electronic program guides, and interfaces. As these mechanisms are more and more linked to consumer choice and findability of content, their relevance is growing steadily. The transactional aspects of smart TV mean that traditional concepts about jurisdiction become more complicated. Whereas in the audiovisual sector jurisdiction is mainly linked to the country of origin, in consumer-related regulation consumers can claim their rights in their home country.
5. The issues around new phenomena such as smart TVs illustrate the importance of generic instruments applicable to it. General data protection regulation is directly impacting the collection, processing and storage of personal data gathered via smart TVs. For the scope of application of data protection law, it is not definitions of the categories of regulated services that are relevant but merely whether personal data is processed and who is the controller who is liable to regulation. At the same time, data protection law is agnostic to the special role and function of audiovisual media services for society and democracy and does also not vest any special protection to the users of audiovisual media services via smart TV.
6. Fundamental rights are also shaping the evolving regulatory and policy environments, by providing guidance on how States can ensure effective protection of individuals' rights to freedom of expression, privacy, and data protection. Effective protection of these rights necessarily entails a range of negative and positive obligations for States. Relevant positive obligations could have implications for the activities of the range of actors involved in the smart TV ecosystem, insofar as those activities interfere with fundamental rights.
7. In the near future smart TVs – as a *totum pro parte* – offer great challenges. Not only from a service perspective affecting the industry and users, but also from a regulatory and policy perspective. The scattered regulatory landscape needs to be assessed from a more integrated point of view. This will help to determine whether all relevant aspects are covered in a consistent way. Such an analysis might show that certain instruments are outdated and can be abolished or modified. As smart TVs show how quickly the landscape can change, a more normative approach could be needed, because carving rules into stone might not match the dynamics of the sector. General instruments often provide a more normative approach, but often require more commitment on the application and enforcement level. This creates challenges for regulators: media, privacy and consumer authorities need to work together and coordinate their actions. Coordination seems the most likely step in many respects: building one policy and regulatory framework taking all aspects into account is too utopian, too time-consuming, and not in line with the interests of both service providers and users.

Set up in December 1992, the European Audiovisual Observatory's mission is to gather and distribute information on the audiovisual industry in Europe.
The Observatory is a European public service body comprised of 41 member states and the European Union, represented by the European Commission. It operates within the legal framework of the Council of Europe and works alongside a number of partners and professional organisations from within the industry and with a network of correspondents.

Major activities of the Observatory are

- the Yearbook online service
  www.yearbook.obs.coe.int
- the publication of newsletters and reports
  www.obs.coe.int/publications
- the provision of information through the Observatory's Internet site
  www.obs.coe.int
- contributions to conferences
  www.obs.coe.int/events

The Observatory also makes available free-access databases, including:

IRIS Merlin
Database on legal information relevant to the audiovisual sector in Europe
www.merlin.obs.coe.int

MAVISE
Database on TV and on-demand audiovisual services and companies in Europe
www.mavise.obs.coe.int

AVMSDatabase
Database on the transposition of the AVMS Directive into national legislation
www.avmsd.obs.coe.int

LUMIERE
Database on admissions to films released in Europe
www.lumiere.obs.coe.int

European Audiovisual Observatory
76 Allée de la Robertsau – 67000 Strasbourg – France
Tel: +33 (0) 3 90 21 60 00 – Fax: +33 (0) 3 90 21 60 19
www.obs.coe.int – E-mail: info.obs@coe.int

IRIS Special

Smart TV and data protection

Samsung have warned owners of their smart TVs that the system's voice recognition could actually be recording and sharing their private conversations. This "bad buzz" comes at a time when Brussels is in the process of adopting new legislation – the General Data Protection Regulation (GDPR) - aimed at protecting us from abuse and misuse of our private data and consumer behaviour big data collected by smart equipment such as television sets. The European Audiovisual Observatory, part of the Council of Europe in Strasbourg, is keeping track of these developments and has published this IRIS *Special* report entitled "Smart TV and data protection".

This is a joint publication by the Strasbourg-based Observatory and partner institution, the Dutch Institute for Information Law (IViR in Amsterdam). It inspired an expert workshop organised in Strasbourg in December 2015, which looked at "the grey areas between media regulation and data protection".

EUROPEAN AUDIOVISUAL OBSERVATORY

EUR 49 - ISBN 978-92-871-8239-5