Pre-publication version of Irion, K., & Helberger, N. (2017). 'Smart TV and the online media sector: User privacy in view of changing market realities.' *Telecommunications Policy*, 41(3), 170-184. DOI: 10.1016/j.telpol.2016.12.013

Smart TV and the online media sector: User privacy in view of changing market realities

Kristina Irion* and Natali Helberger

Institute for Information Law (IViR) at the University of Amsterdam, PO Box 1030, 1000 BA Amsterdam, The Netherlands

1. Introduction

Television sets used to be standalone device with the main purpose of receiving TV channels. Convergence, i.e. "the progressive merger of traditional broadcast services and the internet" (European Commission, 2013), has overhauled this situation dramatically. According to Ofcom, connected TVs or "smart TVs" are rapidly diffusing in Western-European countries with market shares above or close to 40 per cent (Ofcom, 2015a).

One fundamental difference between watching traditional TV and today's consumption of television and other audiovisual content via smart TVs but also mobile phones and tablets (Nielson, 2015) is that these devices are connected to the internet. Connected devices enable the collection of very detailed information about media consumption and behavior of individual users. Such information can be used to create detailed user profiles, which in turn can feed into personalized services, personalised recommendations but also behaviorally targeted advertising.

In so doing, smart TVs, like other connected devices, trigger privacy and data protection issues (Walden & Woods, 2011). Unlike other connected devices, we will show that the collection of information about the viewing behavior of users can provide very detailed and sensitive insights into what users think, know, and believe. Therefore, we argue, special attention to the issue of privacy is needed, not only from the perspective of data protection law, but also media law and policy. Studying the examples of cases from Germany and the Netherlands, in which regulatory authorities have started to develop the contours of a special privacy regime for media users, we will develop suggestions for better accommodating the specific privacy concerns in the audiovisual media sector.

At present, these issues sit squarely in EU law, which provides for distinct regulatory regimes for audiovisual media services, electronic communications and data protection. The traditional focus of the EU's media policy is on the supply of television and television-like content, i.e. what used to be broadcasting. Walden and Woods (2011) observed that "broadcasting was diffuse, with no identifiable pathways to individual viewers, whose consumption of particular programming was therefore effectively anonymous." For that matter, there is currently very little recognition in EU policy of particular privacy concerns about the monitoring of users' consumption of media content.

This article sets out to challenge the isolation of media policy from specific concerns about citizens' and users' privacy and data protection, in audiovisual and online content, at EU level. On the one hand, the objective of the EU's data protection law is to protect individuals' fundamental rights to privacy and the protection of their personal data. It is not concerned with upholding the values of an

* Tel.: +31(0)205253649.
Email address k.irion@uva.nl, n. helberger@uva.nl

EU media policy, such as ensuring the freedom of EU citizens to freely receive information, including from audiovisual and online media, while not being exposed to monitoring and tracking. The EU's media policy, on the other hand, strangely avoids the emerging issues of monitoring and tracking users' media consumption, the role of targeted advertising and how media personalisation strategies could affect media pluralism for better or worse.[1] This seems wholly inadequate considering the important role of television and online media in pluralistic and democratic societies in member states and the EU.

The policy issues surrounding privacy, data protection and personalisation with smart TVs and in the online media sector are still relatively young and have thus been only sporadically addressed in the literature. German legal literature flagged legal challenges with connected TV, however, primarily concerned with application of German law (Ladeur & Gostomzyk, 2014) and discusses associated privacy risks in light of German legal requirements (Ghiglieri, Hansen, Nebel, Pörschke, & Fhom, 2016; Schmidtmann & Schwiering, 2014). The European Audiovisual Observatory's (2016) recently published report on "Smart TV and data protection" applies EU sectoral regulation to the smart TV ecosystem.[2] The article of Walden and Woods (2011) is one of the first that have taken up the topic of broadcasting privacy more explicitly. The authors argue for a more cognizant policy on broadcasting privacy, albeit from the perspective of the challenges that convergence poses for upholding the traditional legal distinction between 'broadcasting' and 'communications services' in relation to the privacy safeguards pertaining to electronic communications. Besides, there are a number of more technical contributions discussing facets of personal data-intensive content services and threats to privacy and security (Ghiglieri, Oswald, & Tews, 2013; Michéle & Karpow, 2014), however, these are mostly focused on the technology, and less concerned with the legal and policy aspects.

Building on Walden and Woods' (2011) critique, the article argues that the monitoring and tracking of users of interactive audiovisual media services should be a concern of EU and national media policy in view of changing market realities. This article's specific contribution lies in presenting facts from implementation and enforcement actions in two Member States, Germany and the Netherlands, and demonstrating how here a new approach of acknowledging and protecting the specific privacy interests of media users is emerging. It places these initiatives within the broader context of an emerging body of literature that argues in favour of the important contribution of protecting privacy for the freedom to receive information and hold opinions (Cohen, 1996; Krotoszynski, 2016; Richards, 2008; Rössler, 2005; Solove, 2010). It is also the first article to draw possible lessons for an adequate approach in media policy to protecting users' privacy in relation to smart TV and media content, also at the EU level.

The reason for covering in particular Germany and the Netherlands is that in both countries the protection of users' privacy and personal data in relation to smart TV and interactive television services has become enforcement priorities. Germany provides a good case study on turning a sectoral investigation into concrete policy guidance for stakeholders of the smart TV and interconnected television services' ecosystem. The Netherlands have seen three enforcement actions by the Dutch Data Protection Authority against leading providers of interactive television services. Thus, it is not about offering a complete comparative review across member states but to focus on Germany and the

[1] For example, Netflix claims it is investing $150 m (approx. €120 m) in improving personalised recommendation services per year (Roettgers, 2014).
[2] Please note that Kristina Irion is a contributing author to this report.

Netherlands, where local data protection authorities have advanced their legal assessment the furthest.

This article is structured as follows: it starts by fact-finding, to provide the necessary background on smart and connected TV, audiovisual and online media, and the collection and use of personal data in this field. The second section offers a brief overview of EU data protection law, hereby already incorporating the new General Data Protection Directive (GDPR), and the challenges of monitoring and tracking users' viewing habits and other new purposes for which personal data is being processed. The third section presents implementation activities in Germany and enforcement actions in the Netherlands in relation to smart TV and interactive media services. The fourth section explores the missing link between users' viewing privacy and media policy and offers some arguments as to why the latter could be falling short given the central role of the media in democracies and users' rights to freely receive information. This is followed by the conclusions, in which we will also reflect about lessons to be learned from the initiatives in the Netherlands and Germany for EU and national law and policy.

2. Personal data processing via smart TVs: A fact-finding mission

Recently, the connective capabilities of smart TVs made headlines in several European countries for divulging users' privacy in a variety of ways. In 2013, the media reported that a smart TV was found to transfer information about what users are viewing and the filenames on an external storage device to the equipment manufacturer (Arthur, 2013). In 2015, the voice control of a smart TV made headlines for incidentally eavesdropping on private conversations which were transmitted online to a specialised voice recognition provider in yet another country (Crossley, 2015). This incident raised the question of whether words spoken inside the home are still private. In both cases the equipment manufacturers concerned took measures to address certain technical and legal shortcomings and to bring their activities in line with the relevant data protection laws.

Besides anecdotal evidence in the media, two technical tests have informed our understanding of personal data flows via smart TVs. In 2014, a German consumer test institute published a report about its investigation into data flows from the smart TVs of nine equipment manufacturers (Stiftung Warentest, 2014). The test covered the interactive return channel via HbbTV,[3] when the smart TV is connected to the internet and the user has activated the function via the red button on the remote control. The report criticised the fact that apart from the TV channels which receive the request of the user to access their online services via HbbTV, this information was in some cases also sent to a third party web analytics provider (Ghiglieri et al., 2013; Stiftung Warentest, 2014). Three smart TVs were found to transmit their device identification number which is a unique identifier that can be used to single out an individual user (Stiftung Warentest, 2014).[4] German media covered this report widely, which prompted the competent German data protection authorities to launch a coordinated investigation into smart TVs.

In 2015, the Bavarian Data Protection Authority (*Bayerisches Landesamt für Datenschutzaufsicht*) took the lead and conducted a test on the smart TVs of 13 manufacturers,

[3] Hybrid Broadcast Broadband TV (HbbTV) is an industry standard by the European Telecommunications Standards Institute (ETSI), which enables the delivery of a wide range of services, such as catch-up TV, video-on-demand, electronic programming guides, interactive advertising and personalised services, among other things.
[4] Ibid. (Fn. 5).

covering ca. 90 per cent of the German market (BayLDA, 2015). This test was not part of an enforcement action but a sectoral investigation into data flows from smart TVs. It followed a technical protocol to test, in relation to certain functions and events, which data flowed from the TV and to which destination. However, whenever data flows from the smart TV were encrypted (which is best practice from an information security point of view) that could conceal whether personal data was being transmitted. The test results proved that users' personal data was already being widely collected via the smart TV by all kinds of providers (cf. Table 1). However, the discovered data flows cannot be regarded as evidence of an infringement by certain providers because they have yet to be appraised under German data protection law.

Table 1. Data flows from smart TVs of 13 equipment manufacturers

Function of the smart TV/ event	Data flows		Destination server
	Unencrypted	Encrypted	
- Watching linear television	4	-	Equipment manufacturer
	10	-	TV channels
- Switching between TV channels	7	-	TV channels
- Use of recorder function	1	5	Equipment manufacturer
- Connect external storage	-	4	Equipment manufacturer
- Using apps	5	6	App store
- Using EPG (personalisation)	-	7	EPG

Source: Based on Annex 1 (Bayerische Landesamt für Datenschutzaufsicht, 2015.

There are a number of important lessons to be learned from this information. At its most basic, the smart TV is a connected device through which, in addition to the equipment manufacturer, an entire ecosystem of providers is offering its services to the user. TV channels now tend to offer two types of service: television programmes and on-demand audiovisual media services, often via their own app.[5] The electronic programming guide (EPG) can be an affiliated or independent provider, who -- in either case – is increasingly embarking on personalised recommendation services. Apart from this, smart TVs link to an app store, the provider of which is often the equipment manufacturer but not always.[6] Via the app store numerous third party apps are made available to the user, such as the apps of TV channels, games, etc. Additional third parties are involved in offering numerous auxiliary services, such as voice recognition and analytics to name but a few. Services delivering advertising in connection with online content of TV channels, the EPG and apps are also becoming increasingly involved. Ultimately, connectivity via HbbTV and internet protocol is provided by an electronic network operator.

Secondly, while the smart TV ecosystem is rapidly taking shape, there is clearly a trend on the part of the equipment manufacturer and service providers to take full advantage of users' personal data. Personal data is used for a variety of purposes, such as measurement and analytics, tracking viewing behaviour and profiling, personalised content recommendations, and targeted or behavioural advertising. Considerations of privacy, data protection and security are legal requirements which, arguably, are still in the process of being fully asserted in the smart TV ecosystem. At different speeds, equipment manufacturers and service providers are catching-up with legal requirements, for example by providing compulsory information and asking for users' consent to the processing of

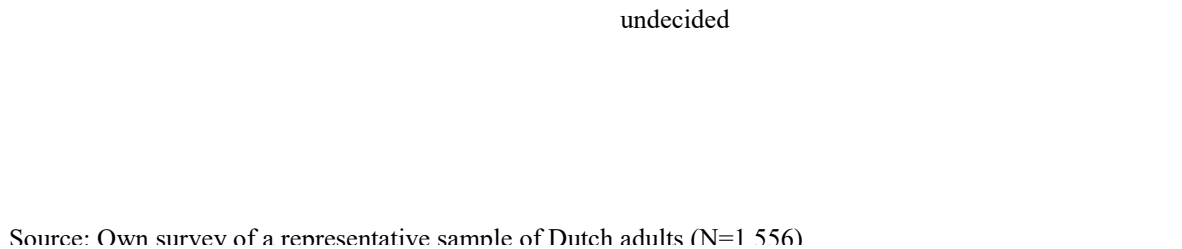
[5] The apps of certain public service broadcasters are very popular and in total 32 apps from 17 member states were in the top-ten most downloaded apps in Google Play and Apple App Store (Visionary Analytics, SQW, & Ramboll, 2016).

[6] E.g. in the Netherlands the app store accessible via the Philips smart TV is TP Vision, a joint venture (CBP, 2013).

personal data. Apart from this, the diversification of personal data flows in the smart TV ecosystem poses new challenges for oversight and enforcement as will be discussed below. In addition, audiovisual media policy at EU and member states levels is facing new challenges from the fading anonymity of media consumption and the prospect of an increasingly personalised media environment, neither of which are properly understood yet.

Finally, the TV set remains a highly important device for individuals' private and family lives and home, something which renders smart TV's appetite for personal data quite a concern. This is reflected by the outcome of a user survey that was conducted in the context of the Personalised Communications research project.[7] In the survey we asked a representative sample of Dutch adults (N=1.556) about their attitudes to a TV that (now or in the future) could collect their personal data. It was explained that this personal data would be used to customise information, for example in order to deliver advertising or recommendations based on their personal preferences. Almost two thirds of the participants (66.5%) found this unacceptable. While users enjoy the benefits of video-on-demand and personalised recommendation services, for example, in their attitudes towards monitoring users are not differentiating between desirable and perhaps undesirable personal data use. Such broad rejection levels are in line with findings elsewhere that EU citizens' are concerned about their everyday activities being monitored (European Commission, 2015). It is of course impossible to infer any direct conclusions for regulatory action from findings as these, however, it should be taken at least as a signal that this is an issue that should be on the radar screen of regulatory authorities, seeing the fast proliferation of smart TVs in Europe.

Figure 1: Attitudes towards TV collecting personal data



Source: Own survey of a representative sample of Dutch adults (N=1.556)

Nevertheless, it is known from the literature that there is a discrepancy between individuals' attitudes and actions in the context of privacy and data protection. What has become known as the privacy paradox can be attributed to different possible causes. Acquisti, Brandimarte, & Loewenstein (2015) explain the often counter-intuitive dynamics of individual decision-making with uncertainty about the consequences of privacy-related behaviours and their own preferences over those

[7] Via a cross-sectional survey, the data was collected from among a representative sample of Dutch adults (N=1.556). The data was collected through Computer Assisted Web Interviewing (CAWI) in the period from 05 October 2015 to 14 November 2015. The survey was administered by the Dutch polling company CentERdata and drawn from the Dutch academic household panel LISS.

consequences; the context dependence of people's concern, or lack thereof, about privacy; and the degree to which privacy concerns are malleable in the service of commercial interests. This article would actually support an additional cause: that users' agency is significantly reduced because information duties have not been complied with and default settings were not conducive to preserving users' and viewers' privacy.

3. The EU data protection framework applying to interactive audiovisual media services

In the EU, the rights to the protection of privacy and personal data are fundamental rights guaranteed in Articles 7 and 8 of the Charter of Fundamental Rights of the EU. EU data protection law aims at ensuring "effective and complete protection of the fundamental rights and freedoms of natural persons" (CJEU, 2014). Based on its exclusive competence in Article 16(2) TFEU, the EU legislator recently accomplished its reform of EU data protection law. The General Data Protection Regulation (GDPR) (European Parliament and the Council, 2016) will enter into force in May 2018 and will repeal the 1995 Data Protection Directive (European Parliament and the Council, 1995). The Regulation will set directly applicable law in all EU Member States. This article already incorporates the legal situation under the GDPR.

3.1 The new General Data Protection Regulation (GDPR)

The GDPR defines the scope of application, key concepts and the legal framework for the lawful processing of personal data in EU law. The following encompasses the essentials of data protection as provided for under EU law and relevant to the consumption of audiovisual media and online content.

Personal data is defined as "any information relating to an identified or an identifiable natural person" (European Parliament and the Council, 2016). The definition is satisfied if an individual can be identified directly or indirectly by reference to an identifier, such as an online identifier. As emerged in the section above, smart TVs and online media are collecting and processing a range of personal data from users, notably subscriber information and - as long as it is linked to a particular user via the subscription or another unique identifier -- a user's viewing habits relating to television programmes and switching between channels, the use of apps and location data, among other things. For example, collecting and linking information to device identification numbers, unique cookies and even dynamic IP addresses falls under the scope of data protection law (CJEU, 2011, 2016; Kuner, 2007; F. Zuiderveen Borgesius, 2016). Voice and facial recognition techniques, which make use of biometric data unique to an individual, also meet the definition of personal data (Article 29 Working Party, 2003, 2012). Only anonymous or truly anonymised data would fall outside the material scope of the GDPR (Article 29 Working Party, 2014; F. Zuiderveen Borgesius, 2016).

In order for the processing of personal data to be legitimate, it has to have a justifiable legal basis and it has to meet the principles of data quality. Personal data flows from smart TVs and when using online content can be necessary for the performance of a contract, to which the user is a party (Article 6(1)(b) GDPR). Processing subscriber information is, for example, necessary to give access to audiovisual content and for billing purposes. Personalised recommendation services at the request of a user would also require some information about the user's preferences. However, the service provider is obliged to provide the user with detailed information about the processing of her personal data in advance (Article 13 GDPR). In order to satisfy the information obligation, that information must include the identity of the provider, the purposes for which the data is intended and used, whether the data is to be transferred to any third party or recipient, and it must explain the user's rights in relation to his data.

The processing of personal data can also be legitimately based on the consent of the user (Article 6(1)(a) GDPR). In the absence of another legal basis for the processing of personal data consent is often the only viable legal basis for rendering data processing lawful. For example, monitoring users' consumption of audiovisual media for the purpose of building individual profiles and targeting advertising to a user's preferences are two distinct purposes to which the user has to consent. By virtue of the law, 'consent' is "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she […] signifies agreement to the processing of personal data relating to him or her" " (Article 4(11) GDPR). For any consent to be informed, information about the processing of personal data has to be provided upfront, containing the details listed in Article 13 of the GDPR.

The GDPR also defines 'special categories of personal data' as "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 9(1) GDPR). From the consumption of audiovisual media and online content it is certainly possible to make inferences about individual users, for example that viewers of minority or diaspora television may belong to this ethnic group or that viewers of certain adult content share a similar sexual orientation. Pursuant to the GDPR the processing of these special categories of personal data for ordinary commercial purposes is prohibited, unless the user has given his explicit consent (Article 9(2)(a) GDPR).

Those equipment manufacturers and service providers who are in control of the data processing activities have obligations to ensure the confidentiality and security of the processing. To this end, they have to take appropriate technical and organisational measures to secure personal data, "in particular where the processing involves the transmission of data over a network" (Article 24(1) GDPR). The involvement of third parties, who for example provide auxiliary services, must be governed by a contract or another binding legal act, which instructs and limits how the personal data can be used (Article 28(3) GDPR). Finally, the Data Protection Directive prohibits the transfer of personal data to third countries outside the EU and the European Economic Area, except where this meets certain legal requirements or can be derogated from (Articles 44f. GDPR).

3.2 The discrete but disparate contribution of the e-Privacy Directive

A second relevant instrument at EU level is the e-Privacy Directive (European Parliament and the Council, 2002b), which regulates various aspects of privacy and the processing of personal data in the electronic communications sector. The e-Privacy Directive complements general data protection law and, where it applies, supersedes the general rules. As part of the EU's regulatory package on e-communications, the obligations under the e-Privacy Directive are addressed to providers of public electronic communications networks and services as defined in yet another legal instrument, the so-called Framework Directive (European Parliament and the Council, 2002a).

In their contribution, Walden and Woods (2011) already observed that the regulatory division of labour, which traditionally distinguishes between electronic communications and content regulation, fails to offer technologically neutral legal protection. For example, the HbbTV-provider, i.e. the provider of the interactive return-channel, would be bound by the e-Privacy Directive in its entirety. The scope of application, however, excludes by definition equipment manufacturers because they are not provider of electronic networks and services. But also content service providers are excluded, which – albeit electronically transmitted - are broadcasting content ("intended for a potentially unlimited audience", Recital (16) e-Privacy Directive),[8] services involving editorial

[8] "Intended for a potentially unlimited audience", Recital 16 e-Privacy Directive, ibid. (fn. 29).

control (Article 2(c) Framework Directive),[9] information society services (Recital (10) and Article 2(c) Framework Directive),[10] and other over-the-top (OTT) services (Jakobsen, 2014). Their personal data processing activities are regulated by the GDPR instead. This is also the reason why the e-Privacy Directive is currently in the process of being reviewed for internal consistency and relevance for today's personal data-rich economy (European Commission, 2015).

There is one important exception in which the e-Privacy Directive applies indiscriminately to all players and "worldwide" (Article 29 Working Party, 2013): the requirement 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' (Article 5(3) e-Privacy Directive). Apart from computers and other connected devices, also storing cookies and beacons on consumer equipment used for digital television is within the scope of the regulation, which explicitly covers "consumer equipment used for digital television" (Recital (8) Framework Directive). Henceforth, storing cookies and using them as identifiers "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" (Article 5(3) e-Privacy Directive). This translates into a duty on equipment manufacturers and service providers to display a privacy notice and obtain users' consent before storing cookies or accessing information stored on smart TVs. Alternatively, such measures are permitted under EU law when they are strictly necessary to provide an information society service upon the explicit request of the subscriber or user (Article 5(3) e-Privacy Directive). For instance, the authentication of a subscriber or user may mean accessing information previously stored for that purpose on the TV set.

4. Emerging case law carving out heightened privacy protection for media users in Germany and the Netherlands

This section offers a brief overview of implementation and enforcement actions at the member states level. It is, after all, national regulators that implement and enforce EU data protection law and national laws pursuant to the e-Privacy Directive. Member States do have some level of discretion as to how they achieve the desired ends of an EU directive (Craig & De Burca, 2015). Moreover, the EU has only marginal competences in the field of culture that is subsidiary to Member States' cultural policy (Irion & Valcke, 2015). In that sense, national variations can also inform policy on data protection in the audiovisual and online media sector. This has to be borne in mind when looking at implementation activities in Germany and enforcement actions in the Netherlands that are summarised below.

4.1 Smart TVs and data protection in Germany

Germany has a federal Data Protection Act (*Bundesdatenschutzgesetz*) and, in addition, data protection rules dedicated to broadcasting services and on-demand audiovisual media services. The law on broadcasting services takes the form of a federal treaty (*Rundfunkstaatsvertrag*) which, by reference, incorporates the data protection rules on so-called telemedia (*Telemediengesetz*). The definition of telemedia services covers, inter alia, on-demand audiovisual media and online content

[9] Article 2(c) of Directive 2002/21/EC of the European Parliament and of the 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, available at <https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/140framework_5.pdf> (unofficially consolidated version, accessed 28.02.2016).

[10] Information society services "are not covered by the scope of this Directive because they do not consist wholly or mainly in the conveyance of signals on electronic communications networks." Recital 10 and Article 2(c) of Directive 2002/21/EC, ibid.

services. As a result, broadcasting services and on-demand audiovisual media services and online content services adhere to the same set of rules on data protection, which underscore the high level of protection afforded to personal data generated in the course of media consumption.

As a German peculiarity, which does not find expression in EU law, Germany has specific privacy safeguards in its media law (Schmidtmann & Schwiering, 2014). Remarkable is that users have the right to use services anonymously, insofar as this is technically feasible.[11] The Telemedia Act treats the use of subscriber information (*Bestandsdaten*) and usage data (*Nutzungsdaten*) of individual users differently. Another deviation from EU law allows service providers to create usage profiles linked to pseudonyms for enumerated purposes, such as advertising and market research, unless the user has objected. To that end, the Telemedia Act requires a clear separation between the usage profile and the individual user of the service, and pseudonyms should not simply reproduce unique identifiers generated by the service. German law moreover prohibits the sharing of personal data on the use of television and on-demand audiovisual media services with third parties. Only anonymised usage data can be shared with third parties for market research and analytical purposes.

German authorities have taken successive measures that aim to implement local data protection law in the context of smart TV. The efforts launched with a policy document entitled "Smart TV only with smart data protection" (*Smartes Fernsehen nur mit smartem Datenschutz*) which was released in 2014 (Düsseldorfer Kreis & der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, 2014). This was followed by the smart TV test action, conducted under the lead of the Bavarian Data Protection Authority (*Bayerisches Landesamt für Datenschutzaufsicht*), which was introduced as part of a fact-finding exercise above (Section 2) (BayLDA, 2015). Based on the legal assessment of the sectoral investigation, the competent data protection authorities of the federal states prepared a guidance document on smart TV (Düsseldorfer Kreis, 2015). This guidance document serves to inform the stakeholders in the smart TV ecosystem and aligns the interpretation of data protection requirements among German data protection authorities.

The first policy document "Smart TV only with smart data protection" (*Smartes Fernsehen nur mit smartem Datenschutz*) was issued as a joint position by the data protection authorities competent to enforce data protection laws in the private sector which were leading coordination efforts via the so-called *Düsseldorfer Kreis* (2015). The policy document received the support of the conference of media authorities (*Konferenz der Direktoren der Landesanstalten für Medien*) and the data protection officers of the public service media organisations in Germany (ARD and ZDF). This is a remarkable alliance of data protection authorities and independent public service media and it has the very symbolic support of the media regulators for audiovisual services in the private sector.

The document introduces the connected capabilities of smart TVs and states that it is not so clear to users anymore whether they are watching television or accessing on-demand services. It recognises that the interactive return-channel can be used to track users and analyse users' individual media consumption. It continues with a principled statement that television is an important medium for the dissemination of information and the free formation of opinions; the right to access information is a fundamental right and the foundation of a free and democratic society. It then concludes that the enjoyment of this right would be seriously impaired by the collection, analysis and use of data on media consumption.

[11] Art. 13 (4) No. 6 of the German Telemedia Law (*Telemediendienste-Gesetz*).

The policy document sets out four requirements for smart TV ensuing from German data protection law. Firstly, the anonymous use of television services must be guaranteed for both normal and smart TVs. The profiling of individual television consumption is not permissible without the informed and explicit consent of the user. Secondly, equipment manufacturers, television channels and other providers of online services, within the scope of the Telemedia Act, must either obtain users' consent or confine themselves to processing personal data as it is provided for by law. It provides details about the use of subscriber data, information obligations and the legal possibility of creating pseudonymized profiles under the Telemedia Act. Thirdly, it calls for the observance of the principle of "privacy by default" meaning that factory settings should comply with legal requirements and allow anonymous viewing of television. Information obligations are stressed again along with the fact that users must have the possibility to manage settings and cookies. The fourth requirement relates to technical security and calls for the protection of devices and data traffic against unauthorised access by third parties.

The guidance document, which was issued after the policy document and the sectoral investigation, offers a much more detailed assessment of what is required under German data protection law in relation to various purposes and what is required of the various players (Düsseldorfer Kreis, 2015).It strictly applies the relevant provisions from the Telemedia Act and the federal Data Protection Act while dealing mainly with the data flows from smart TV and its ecosystem. The legal assessment is modular, in response to the specific activities involved in the processing of personal data and almost reads like a manual for compliance. At the same time, the guidance document sets the legal benchmarks against which the processing of personal data through smart TV and content services will be assessed. There has been no public enforcement action so far[12] and a more recent consumer test finds no significant improvement in the upfront compliance with German data protection law (Stiftung Warentest, 2016).

4.2 Enforcement priority on tracking in the Netherlands

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*)[13] supervises compliance with the Dutch Personal Data Protection Act[14]. In 2014, the Authority identified the theme 'tracking and tracing' as one of its enforcement priorities and with this the tracking of viewing behaviour (Autoriteit Persoonsgegevens, 2014). To date it investigated three companies processing personal data in interactive digital TV and online services through smart TVs – this will be summarised below.

4.2.1 Enforcement against TP Vision

The first enforcement action took place in 2013 against the Dutch company TP Vision (CBP, 2013), which is a joint venture with the equipment manufacturer of Philips smart TVs.[15] TP Vision, who collected and processed the personal data of Philips Smart TV users in the Netherlands, was found to be in violation of Dutch data protection law on three grounds: firstly, the services did not provide information about the processing of personal data and the purposes for which the data was processed when the smart TV was first deployed. Secondly, TP Vision did not obtain users' valid consent for placing tracking cookies on the smart TV. For consent to be valid it has to be an opt-in

[12] A German consumer protection organisations won a civil law case against a Samsung smart TV because the terms of service and the privacy notice were incomprehensible and the TV transferred personal data without a legal basis, Landgericht Frankfurt am Main, judgment of 10 Juni 2016, case 2-03 O 364/15 (in German).
[13] Formerly *College bescherming persoonsgegevens* (CBP).
[14] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), available at <http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_26-10-2015> (accessed 28.02.2016).
[15] An estimated 1.2 million Philips Smart TVs have been sold in the Netherlands since 2009, ibid.

decision as well as being free, in the sense that it must be possible not to consent. Thirdly, TP Vision transferred the personal data of its users to third parties without the requisite contractual agreement.

What is remarkable about the enforcement action against TP Vision is that the authority classified the collected personal data as sensitive because it can reveal very individual patterns which could potentially disclose the specific social background, financial or family situation. This is a creative interpretation of the law which, under EU law, only recognises the dichotomy of personal data and special categories of personal data. This new middle category of sensitive personal data sort of raises the stakes with its need for protection under Dutch law. As a result of the enforcement action TP Vision brought its operations into line with Dutch law, however, the Dutch Authority is not yet satisfied about how information is provided to the users.

4.2.2 Enforcement against cable TV operator Ziggo

In its second enforcement action, the Dutch Data Protection Authority investigated the Dutch cable TV operator Ziggo,[16] which since early 2014 has been a subsidiary of the UK listed company Liberty Global (Daalen, 2014). Analogously with the TP Vision enforcement action, Ziggo infringed Dutch data protection law when monitoring its users' viewing of interactive digital television services (Autoriteit Persoonsgegevens, 2015). The company failed to provide clear information about the processing of personal data and the purpose for which it was used and did not obtain the users' unambiguous consent to the data processing. Ziggo made successive concessions to comply with Dutch data protection law, such as introducing information for users and obtaining users' consent.

In its reasoning, the authority distinguished between three content services offered by Ziggo, being: linear television, video on-demand and pay-per-view. Via interactive television decoders, the company monitored users' content viewing in all three categories of content services, for purposes such as audience measurement, personalised recommendations, but also direct marketing. Again, the authority invoked its notion of sensitive personal data, with the argument that from monitoring media consumption a precise impression about someone's behaviour and preferences can be formed. Again this raises the stakes for Ziggo to use this personal data for other purposes, then delivering its services to its users, unless the individuals have given their explicit consent to additional purposes.

The processing of such sensitive personal data beyond what is necessary for the performance of the contract would necessitate the explicit consent of the user. The Dutch Data Protection Authority underscored that in order to obtain an explicit consent, users must also be given the opportunity not to agree to the processing. In the course of the investigation, Ziggo improved the option for users to agree or disagree to personalised recommendation services. Another consequence of attributing media consumption as sensitive personal data is that Ziggo's interest in processing such data cannot weight heavier than individuals' interest in them not being used. As a result of the investigation, Ziggo stopped using personal data about the consumption of video-on-demand and asks for users' explicit consent for the collection of pay-per-view data from its users, which mainly pertains to sports and adult content.

4.2.3 Enforcement against XS4ALL and KPN

The third enforcement action in relation to digital interactive television was directed against XS4ALL who is another provider of interactive television services (Autoriteit Persoonsgegevens, 2016b). The Dutch Data Protection Authority concluded that XS4ALL, and its mother company KPN

[16] With 2.3 million users Ziggo is the biggest provider of digital television services in the Netherlands. The investigation had have some ramifications with cable TV qualifying as electronic communications network operator, which are further discussed in Section 5.2 below.

jointly control the processing of customers' personal data about their viewing behaviour (Autoriteit Persoonsgegevens, 2016a). The authority repeated that such personal data is of a sensitive nature because it can reveal someone's behaviour and interest. Similar to the other two cases, the companies failed to provide essential information about the purposes for the processing of personal data to its customers. Even after XS4ALL furnished a privacy notice it reserved the right to introduce changes to its policy without notifying customers, which contradicts Dutch law.

A new aspect of this enforcement action was that customers' viewing behaviour was used for producing TV ratings, which is a form of market analysis which the companies used for several other purposes. The personal data was not effectively anonymised because the original log files were still available for up to six months. Absent of customers' explicit consent to the use of their personal data for TV ratings XS4ALL and KPN did not have a legal basis in data protection law. The companies discontinued producing TV ratings in order to bring their activities in line with the findings of the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, 2016a).

4.2.4. Dutch enforcement actions confirming sensitive nature of individuals' media consumption

With these three enforcement actions the Dutch Data Protection Authority created precedents for the application of data protection law with respect to the processing of personal data when users viewed audiovisual and online media via smart TV and interactive television services. It was asserted that unambiguous consent is required by law for any purpose other than that which is strictly necessary for the performance of the contract. This in turn necessitates clear and complete information about the collection of personal data and its uses. The legal assessment is fairly similar to what would be required under EU data protection law.

What can be considered a specific Dutch interpretation of the law is applying the notion of sensitive personal data to the consumption of audiovisual content. In view of the particularly precise inferences that can be drawn from such data about individuals' behaviour and preferences, the Dutch data protection authority underscored in its enforcement actions that it will not tolerate the use of media consumption data without an informed express consent by the concerned user. EU data protection law, which is at the root of the Dutch legislation, does neither foresee this explicitly nor would it preclude *de lege lata* attributing special sensitivity to personal data about media consumption.

5. The missing link: Users' viewing privacy and media policy

One of the particularities of the discussion on smart TV and interconnected media services in relation to individuals' privacy is that it seems to take place in relative isolation from the media law and policy debate about convergence and connected devices, or the re-visitation of the Audiovisual Media Services Directive (AVMSD) (European Parliament and of the Council, 2010). In its 2013 Green Paper on Convergence, for example, the European Commission does acknowledge the fact 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" (European Commission, 2013). Having said that, the consultation document makes it very clear that - in the view of the European Commission - these matters should, in the first place, be a matter for EU data protection regulation. Similarly, both, the Audiovisual Media Service Directive, and the draft proposal for its amendment do not include provisions on data protection and privacy, but refer to EU data protection law.

This clear division of tasks between audiovisual media law and data protection law is also reflected in the current debate about smart TVs and interactive audiovisual media services. The

objective of the following section is to challenge this division of labour and to make the argument that the issue of users' viewing privacy is also a matter for media law and policy at EU and Member States' level, taking its embedded values and objectives into account. So far, we have demonstrated that smart TVs, like other connected devices, have to adhere to the principles of data protection to ensure that the way information about users is collected and processed is fair and lawful. Another question is to which ends this information is being used, and how the tracking and profiling of viewers relates to other fundamental rights and freedoms than privacy and data protection, for example individuals' freedom of expression.

It is important to realize the critical difference between the consumption of online content via smart TV and other connected devices and similar monitoring and tracking of usage in the context of other online services via computers, smart phones or wearables: smart TVs and interactive television services collect, as the Dutch Data Protection Authority already hinted at, 'sensitive personal data', ie. information that can give a pertinent picture of someone's interests or social background, habits and preferences and that can be used to influence users in a way that impacts on their rights and interests.

Even more explicit on the possible tension between freedom of expression and the monitoring of viewers' behavior via smart TVs has been the German data protection authorities in the Düsseldorfer Kreis. As the Düsseldorfer Kreis observed:

> "*Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt*." (Television is an central medium to inform and an essential conditions for the freedom of expression. The right to unhindered information access is constitutionally protected and necessary for the democratic order. The comprehensive collection, processing and using of information about user behavior will critically affect the exercise of that right. *Translation by the authors*). (Düsseldorfer Kreis & der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, 2014)

This warning from the *Düsseldorfer Kreis* echoes earlier concerns expressed by the Council of Europe in Strasbourg – an institution that has a long tradition in issuing guidance on matters of media law and policy, and that has influenced large parts of national media laws. The Council of Europe noted explicitly for the context of tracking users online, "[t]hese capabilities and practices can have a chilling effect on citizen participation in social, cultural and political life and, in the longer term, could have damaging effects on democracy. … More generally, they can endanger the exercise of freedom of expression and the right to receive and impart information protected under Article 10 of the European Convention on Human Rights" (Council of Europe, 2013). Chilling effects is an important concern in both the recommendations of the Council of Europe as well as the case law of the European Court of Human Rights (Townend, 2017).

Empirical evidence of potential chilling effects of monitoring the television and audiovisual media consumption is still scant. And yet, these are warnings that merit further attention and also research because today's technical capabilities revert the previous default position of anonymous consumption that was implied with broadcasting technology. This is the broader context in which the right to watch media content anonymously in the German Telemedia Law and also the warning from

the Dutch Data Protection Authority about the particular sensitivity of tracking viewing behavior have to be seen.

The right to watch media content anonymously seems to be a direct response to Julie Cohen's reflections about the importance of a 'right to read anonymously' (albeit in the context of digital rights management (DRM) technology) (Cohen, 1996). Basing her argument on US constitutional freedom of speech theory and the threat of chilling effects, Cohen (1996) suggests that the legislator should introduce "a right of anonymous access to reading material that are otherwise made available by willing distributors." In a similar vein, the US scholar Neil Richards (2014) speaks out in favor of "intellectual privacy". According to Richards, "a meaningful measure of privacy is critical to the most basic operations of expression, because it gives new ideas the room they need to grow." Put differently, the protection of privacy is more than a value that merits protection on its own right but instrumental for other rights and values (Krotoszynski, 2016; Rössler, 2005; Solove, 2010).

Especially in the European constitutional tradition, the right to privacy and the attendant protection of personal data has been conceived as an enabling right to broadly further individuals' fundamental rights and freedoms that would be conducive of human dignity and personal autonomy (Oostveen & Irion, 2017). In the context of the media, the right to privacy has to render a particular functional component: to create the necessary individual and - as the sum of its elements - democratic breathing space for intellectual development and for the participation in a public sphere of diverse media exposure. It is obvious why these are relevant considerations, also and especially in the context of smart TVs and interconnected media services, which – for the time being - remain one of the dominant sources citizens use to inform themselves (Newman, Fletcher, Levy, & Kleis Nielsen, 2016).

Having said so, protecting the intellectual privacy of users and their right to view anonymously can only be part of the response to monitoring, profiling and targeting users when watching TV and comparable non-linear formats. This is because there will be many instances in which watching *not* anonymously, and sharing preferences and reading habits with the media can be very useful for users if that means that the media can assist them through personalized recommendations and viewing suggestions. Insofar, it is important, but not enough to afford users some privacy to receive information unmonitored. Equally important is it to ensure that to the extent data collections, profiling and targeting is taking place, this is done in a way that is compatible with the democratic mission of the media, and other fundamental rights and freedoms of users, such as access to a plural and diverse media landscape. This is a discussion that goes beyond television channels and TV apps collecting users' personal data but extends to many more service providers that take part in the media value chain and collect and use viewer's data. In the following, four aspects in particular shall be highlighted.

5.1 Personalised recommendations and media pluralism

Probably the most salient issue, and one that *has* made its way also into the media law and policy discourse is the use of data to provide personalized recommendations, and how that relates to media law and privacy. As we have shown earlier, one of the objectives of data collections is for the use in EPGs, and to give personalized viewing recommendations. As such, learning about the user, his preferences and information needs, can be an important step in making the media more responsive to the needs of its user. Personalisation can be a means of bringing people into contact with content and information which they otherwise might not have looked for, or may not even have been aware that it existed (and is relevant to them) (Natali Helberger, 2011; Resnick, Garrett, Kriplean, Munson, & Stroud, 2013). But it also could have the opposite effect. The concerns that 'filter-bubbles' and 'echo

chambers' could have implications for the way people choose and engage with media content already demonstrate that the collection and use of personal information of viewers could potentially conflict with established values in media regulation.

The European Commission (2013a), in its Convergence Green Paper, tried to capture the difficult balance between reaping the benefits of personalized recommendations, and the demands of a plural and diverse choice for media users. The European Commission (2013) stressed, on the one hand, the potential of filtering and personalization mechanisms to allow citizens "to navigate efficiently through the information overload that characterizes the digital environment." It also acknowledged, however, that so doing, can influence traditional value chains and the role of media providers as editors, but also "the de facto choice for citizens to access media offerings representing a plurality of opinions and can lead to a situation where citizens potentially find themselves in a vulnerable situation without realising it." (ibid.).

While it is too early to draw any conclusions if, and under which conditions personalised recommendations can affect media diversity (Resnick et al., 2013; F. J. Zuiderveen Borgesius et al., 2016), it is clear that this is an issue that merits the attention of the regulatory authorities for the media sector (in this sense also Ofcom, 2015b). As we will show further below, the division of powers between media and data protection authorities renders this task more difficult, and is hence reason for concern. Similar is true for the aforementioned division of labour between media and electronic communications law. For the time being, recommendation services in the form of electronic service guides are regulated under electronic communications law, and only few services have taken the opportunity of adopting further-reaching obligations for recommendation services to promote media political goals, such as media diversity (van der Sloot, 2012).

5.2 Confidentiality and data security

The security and confidentiality of viewers' data is an aspect that Walden and Woods (2011) treat prominently in their analysis. The authors make a clear point about the importance of securing viewing data against interception and surveillance, and the results from our fact finding mission earlier in this article seem to confirm their concerns. Walden & Woods (2011), however, also point out the vulnerability of that data, not at least because of the way how the current EU framework on electronic communications law is organised. The aforementioned e-Privacy Directive provides explicit safeguards for the confidentiality of communications and the related traffic, and listening, tapping, storage or other kinds of interception or surveillance (Art. 5 (1) e-Privacy Directive; European Parliament and the Council, 2002b). Having said that, the scope of that provision is restricted to providers of public communications networks and publicly available electronic communications services. It does not extend to providers of broadcasting services, interactive apps, personalised recommenders or smart TVs.

In a similar vein qualified the Dutch Data Protection Authority' viewing data as sensitive data, the processing of which can have "a major impact on those concerned" (CBP, 2013). In so doing, the authority also highlights the particular vulnerability of such data, and the need to protect them effectively. In the enforcement action against Ziggo, the authority also makes an explicit link to communications freedom, and the fact that viewing data can also reveal the content of communications. Ziggo, the regulatee, is a vertically integrated providers of interactive television services with its own content delivery network, which is the reason why they have the obligation to ensure the confidentiality of communications, including when delivering interactive television services. This particular aspect underscores that the legal distinction between distribution and content

services can lead to asymmetric regulation where the confidentiality of some providers' interactive television services are regulated while others are not.

The German Telemedia Act makes the protection of the usage data on media consumption an obligation for the providers too, as does general data protection law. In this light, the specific provisions in the German Telemedia Service Act are exemplary as they do acknowledge, and specifically address the particular sensitivity of viewers data for interception and uauthorised access by third parties. Parts of the German provisions about media services specifically relate to the security of viewing data, and users have a right to use online media services unobserved by third parties (Ghiglieri et al., 2016). The relevant Guidelines on Smart TV prescribe the use of state-of-the art encryption technology and a range of other measures on technical security (Düsseldorfer Kreis, 2015). In addition, German law prohibits the sharing of personal data on the use of covered media services with third parties, even if pseudonymised; a provision which could only be overridden with the explicit consent of the user. Only anonymised usage data can be shared with third parties for market research and analytical purposes (Düsseldorfer Kreis, 2015).

Although general data protection law would apply in all situations, in light of the above said an argument in favour of protecting the confidentiality and security of interconnected television and content services can be made. The added value of a confidentiality and security duty would be that collecting and using viewing behaviour, including sharing it with third parties, would only be possible with the explicit consent of the individuals concerned. It is important to note that this would not prevent the provisions of personalised recommendations and other value-added services for which there is a demand. But it would limit more effectively the use of data on viewing behaviour for purposes unrelated to rendering the service and limit substantially the ability to share individual profiles with third parties. The outcome would be similar to the creative solution adopted by the Dutch Data Protection Authority to ascribe sensitivity to personal data on viewing behaviour in order to limit its use, without explicit consent, for purposes other than providing the service.

5.3 Personalised advertising and media consumer protection

Moreover, to the extent that viewers' data is being used to offer new personalised services, or to target the audience with behavioural advertising, the values and objectives behind media law can throw new light on these practices, too. The European Commission (2013), in its Green Paper on Convergence, did, for example, refer explicitly to new forms of personalised advertising, but, once again, reference was only made to data protection law. Behavioural targeting, however, could also challenge the application of the existing rules on advertising and fair commercial practices in media law. Media law has a long tradition of seeking the right balance between the interests of media consumers to be informed and entertained, and the amount of, and form in which advertising is used to finance media content.

To this end, EU media law set limits to the amount of advertising that the audience can be required to watch.[17] Needless to say, comparable rules about how much personal information users can reasonably be required to share in exchange for programming and (value-added) services are still lacking. Then there are media law-specific requirements about the permissibility of targeting advertising at minors.[18] And the protection of editorial independence and the trust of the audience in

[17] See e.g. Article 23 of the Audiovisual Media Service Directive: "The proportion of television advertising spots and teleshopping spots within a given clock hour shall not exceed 20 %." (European Parliament and of the Council, 2010).

[18] See e.g. Art. 9(1)(e) and (g) of the Audiovisual Media Service Directive (European Parliament and of the Council, 2010).

that independence are important values in media regulation – values that may also become highly relevant in a situation in which the media move steadily towards new, more behavioural forms of advertising (see for more in-depth explanation Helberger, 2016). At this point in time, there is very little debate about and research into how these values translate to the trend to personalised services and targeted advertisements, and whether the existing media law framework lives up to the requirements of a connected and smart television world.

5.4 Competencies and the need for collaboration between data protection and media supervisory authorities

We have argued that key values in media law but also electronic communications law, such as freedom of expression, confidentiality of communications but also concerns about pluralism and diversity can be important considerations in the context of smart TVs and interconnected audiovisual media services. As already the European Commission (2013) in its Convergence Green Paper has indicated, in the EU legal system, matters related to the collection and processing of personal data fall commonly under data protection law. As we have demonstrated, the collection and processing of personal data can also touch upon important interests and principles that are not directly related to data protection law, but that are subject matter to media and communications law.

The current division of competencies between data protection authorities, communications and media supervisory authorities renders the realisation of these values in the smart TV context more difficult. How far this division of labour between data protection and media authorities goes, and how problematic it can be may be demonstrated by the following example from the Netherlands. This example does not relate directly to smart TVs, but to the collection and processing of personal data by the media, and more specifically the use of so-called cookie-walls to make users agree to the media's data collection and processing strategies.

In response to discussions about the implementation of the cookie provisions in the e-Privacy Directive, a large number of media companies, including the public service broadcasters, started presenting users with take-it-or-leave-it choices in the form of so called cookie-walls. These cookie-walls were essentially pop-ups that gave users the choice to either grant the media permission to use cookies, or not access the website. It were the cookie-walls by the Dutch public service media that were considered the most problematic, and caused most public resistance. By the end of 2012, the Dutch Parliament decided, in light of the controversies and ongoing protests, that there was a need for action, which eventually led to an amendment of the Dutch rules.[19] Maybe the most remarkable aspect of the parliamentary debate was the absence of any consideration of media law and policy, and the question of how making access to the websites of the public service media conditional upon the acceptance of all sorts of tracking and profiling correlates to the mission of the public service media. And maybe even more remarkable was that, in the end, it was not the regulatory authority for the broadcasting sector, but the Dutch Data Protection Authority, that criticised the use of cookie-walls by the public service media:

> The main objective in financing the NPO (Dutch Public Broadcasting Organisation) from the public budget is that the NPO offers a public service, which is essential for everyone in our society. There is no alternative available to users of online services to access the information and emissions of the public service media. It can therefore be said that NPO has a factual monopoly. Through forcing the acceptance of cookies users are paying for their visit with

[19] Article11.7a, 3b of the Dutch Telecommunications Act (*Telecommunicatiewet*).

their personal data. This cannot be regarded as free and valid consent (Autoriteit Persoonsgegevens, 2013).

In doing this, the Authority made a remarkable effort of stretching the interpretation of data protection law, with arguments that relate rather to the public mission of the public service media. Later the Dutch Data Protection Authority opened an investigation into the use of cookies by public service media, but this again was confined to the application of data protection law (CBP, 2014).

By contrast, the Dutch Media Authority, the competent authority for the media sector, took no part in the debate, because matters of data protection law do not fall under its competency, and media law does not make any explicit reference to the placing of cookie walls in the (public service) media. Arguably, a closer investigation of Dutch media law might have provided additional arguments for the Media Authority to assess the cookie walls. According to Article 2(f) of the Dutch Media Act, for example, programmes of the public service media need to be accessible for everyone. The question is: to what extent are they fulfilling this requirement by indiscriminately tracking users' activities on the websites of the public service media? The lack of choice for accessing public service information anonymously could potentially affect at least the more privacy-conscious members of the Dutch population. And Article 3 of the Dutch Media Act requires the public service media to make programmes available to all households at no additional cost - other than the purchase of the necessary hardware (e.g. TV set). It could be argued that the requirement to give personal data in exchange for a programme could be considered to be such a prohibited, additional cost. And yet, the media authorities remained silent in this important debate, because it concerned matters of data collection and processing, and as such fall under the competencies of data protection authorities.

While the Dutch data protection authority did a remarkable effort in advancing the public interest argument, it was equally clear that it had neither the competencies nor the experience to decide in matters related to media law and policy. Remarkably and rather ironically, this division of tasks has its origins in a provision that was originally meant to protect freedom of expression interests of the media and users, namely data protection law's media exception. The cookie-wall example has also made clear that under today's conditions of data-driven media markets, the division of tasks that is the result of this exception can be also an obstacle, rather than a guarantee for freedom of expression, and the legitimate interests of media users.

6. Conclusions: Users' viewing privacy in the light of changing market realities

After its investigation into personal data flows from smart TVs, the German consumer test institute recommended that users should disable the HbbTV functionality or not connect the smart TV to the Internet at all (Stiftung Warentest, 2014). This cannot be the right way forward but should be a wake-up call to the EU and national policy makers to assess the new risks to users' viewing privacy in the light of changing market realities. In this article, we argued that collecting information about users' media consumption does not raise issues about privacy and data protection alone, but also about (audiovisual) media law and policy in the EU and in Member States.

Over the past few years we have seen some important initiatives by regulatory authorities in the Netherlands and Germany on how to reconcile the growing demand for users' personal data with the interests of media users. These initiatives confirmed that the user of media services, and public media services in particular, may require a higher, or at least different level of protection when consuming media content than, for example, when buying shoes online. This is because, as the Dutch Data Protection Authority has put it, this is information that can give a pertinent picture of someone's interests or social background, habits and preferences and that can be used to influence users in a way

that impacts on their rights and interests. In case of media users, in addition to privacy these are also interests that flow from the right to freedom of expression, unhindered information access and media pluralism.

As such, media user privacy is not only a matter for data protection law and data protection authorities. It is also a matter for media law, and media authorities. And yet, apart from the usual provision on balancing the Charter's fundamental rights, in the reform proposal of the Audiovisual Media Service Directive there is not one single reference to matters of privacy or data protection.[20] This lack of any clear references to media user privacy in media law is in line with the division of tasks that EU and Member States' laws handle between matters of privacy and the media, with the notable exception of Germany. This division of tasks has also been confirmed in the European Commission's Green Paper on Convergence (2013). Here, the Green Paper acknowledges that the processing of personal is in many cases part of the functioning of new media services, to then directly refer to data protection law, without any considerations of any possible further implications for media law.[21]

As this article has shown: In view of the changing market realities media law and data protection law no longer co-exist in clinical isolation but tie in when the tracking and monitoring of users' media consumption touch very traditional values and objectives of media policy. Hence, leaving the matter to data protection law alone would not recognise the intrinsic link between media consumption and the freedom to receive information that is a tenet of the fundamental right to freedom of expression. Instead media policy should recognise the specific role of audiovisual and online media for individuals' formation of opinions, which, to our mind, calls for additional safeguards from incessant tracking and monitoring by a host of providers.

Very concretely, we developed four recommendations for future media policy, both, at EU Member States' levels: First, and inspired by innovative approaches in the Germany, EU law should protect the confidentiality and security of data about users media behaviour. Granting users a right to watch anonymously should be part of that protection, as much as the obligation to protect the data from unauthorised access, and apply restraint in sharing the data with third parties. As the technical tests in the beginning of this article have demonstrated, the confidentiality of that data is not a given in the current smart TV environment.

Second, granting users a right to anonymity is a useful first step towards acknowledging their heightened interest in privacy, and yet, it is not enough. This is the more as data collection and processing will often come with the promise of more functionality and value added services, a promise that more privacy-sensitive users should not be forced to forgo. Instead, there is a need to ensure that the way personal data is collected and processed does not interfere with legitimate rights and interests of media users, notably to receive information. Principles of media pluralism come into mind, but also principles of equality and that nobody should be principally excluded from information access, based on her profile. This again would seem to include a right to specifically reject personalisation, or effectuate a positive right of choice, as already the Dutch Data Protection Authority hinted at. Since personalised recommendations will be an important application of data in a smart TV environment, it is high time to revisit the regulation of EPGs, and here in particular the national initiatives to promote public policy values such as diversity and inclusiveness.

[20] Recital 31of European Commission, 2016.

[21] "The moment data generated during the consumption of audiovisual media services relates to an identified or identifiable natural person, it is personal data, and as a consequence falls under the scope of the EU Data Protection Directive (95/46/EC)." (European Commission, 2013)

Third, this also would include effective means to manage permissions, in other words users' express consent to collect viewing data in relation to specific purposes, instead of tying permissions for desired functionalities with less desirable one. This could require media-specific interpretations of how the new data protection principles of privacy by design and default should be implemented. In 2016, the German consumer test organisation criticized that users of Smart TVs are expected to manage permissions for each television channel and media app separately, some of which require up to three opt-out from different means of tracking (Stiftung Warentest, 2016). In this regard, a right to anonymity of media consumption may help affirm the default that datavaillance of media consumption requires users' explicit consent.

Fourth, matters of media users' privacy require cooperation between data protection and media authorities, similar to the remarkable alliance of German authorities in media and data protection when adopting the joint position on "Smart TV only with smart data protection" (Düsseldorfer Kreis & der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, 2014). Member States' media authorities should be more vigorous and empowered (in terms of competency as well as funding) in how they pursue media policy objectives in relation to media users' dataveillance. They should have the ability to cooperate with the competent data protection authorities and avail themselves of opportunities to give their point of view on realising media policy objectives through protecting users' privacy.

At this point in time two key legislative instruments for EU media policy are up for revision which could both carry new guarantees to protect media user's from datavaillance. The European Commission presented its proposal to modernise the Audiovisual Media Services Directive in light of changing market realities (European Commission, 2016) and also a proposal for a Privacy and Electronic Communications Regulation (European Commission, 2017). The EU legislator could inject a provision in the reform proposal for the Audiovisual Media Services Directive to the end that users have a right to anonymity when viewing audiovidual media content. Providers should have the obligation to offer such anonymity unless users request personalised recommendation services or, in all other instances, have explicitly consented to the collection and use of data about their media consumption.

The new legislative proposal for a Privacy and Electronic Communications Regulation that should replace today's e-Privacy Directive (European Commission, 2017) could become a suitable vehicle to carry a proposal on the comprehensive protection of confidentiality and security in connection with interactive television and online content services. In the area of data protection, pursuant to Article 16 TFEU the EU has the exclusive competence to legislate which could be harnessed to introduce provisions that would protect the confidentiality and security of media consumption. It would not be the first time that EU regulation for the electronic communications sector is used to promote media policy objectives (Irion & Valcke, 2015). This reform provides a chance to harmonise the protection of the confidentiality of electronically delivered services in general, including media services, or in relation to the confidentiality of audiovisual media services in particular.

Acknowledgment

This work was supported by the European Research Council under Grant 638514 (PersoNews). Two anonymous JTPO reviewers' comments on earlier versions helped to improve the paper substantially.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, (347), 509–514. doi:10.1126/science.aaa1465

Arthur, C. (2013). Information commissioner investigates LG snooping smart TV data collection. *The Guardian*. Retrieved February 28, 2016, from http://www.theguardian.com/technology/2013/nov/21/information-commissioner-investigates-lg-snooping-smart-tv-data-collection

Article 29 Working Party. (2003). *Working document on biometrics*. doi:WP 80

Article 29 Working Party. (2012). *Opinion 3/2012 on developments in biometric technologies*. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

Article 29 Working Party. (2013). *Opinion 2/2013 on apps on smart devices*. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/

Article 29 Working Party. (2014). *Opinion 05/2014 on Anonymisation Techniques*. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Autoriteit Persoonsgegevens. (2013). *Beantwoording Kamervragen i.v.m. cookiebeleid NPO*. Den Hague. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/

Autoriteit Persoonsgegevens. (2014). *Annual Report 2014*. Den Hague. Retrieved from https://cbpweb.nl/sites/default/files/atoms/files/annual_report_2014.pdf

Autoriteit Persoonsgegevens. Investigation into the processing of personal data by use of interactive digital television services of Ziggo (2015). Retrieved from https://cbpweb.nl/sites/default/files/

Autoriteit Persoonsgegevens. Conclusions Dutch Data Protection Authority of the investigation into KPN and XS4ALL digital interactive TV (2016). Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_report_xs4all_kpn.pdf

Autoriteit Persoonsgegevens. (2016b). XS4ALL and KPN end privacy violations digital TV. *Press Release*. Den Hague. Retrieved from https://autoriteitpersoonsgegevens.nl/en/news/xs4all-and-kpn-end-privacy-violations-digital-tv

BayLDA. (2015). Datenschutz und Smart-TV. Ansbach. Retrieved from https://www.lda.bayern.de/media/pm2015_02.pdf

Broemel, R. (2012). Hybrid-TV als Regulierungsproblem? *Zeitschrift Für Urheber- Und Medienrecht*, *56*(11), 866–877.

CBP. (2013). *Onderzoek naar de verwerking van persoonsgegevens met of door een Philips smart tv door TP Vision Netherlands B.V.* Den Hague. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/pb/pb_20130822-persoonsgegevens-smart-tv.pdf

CBP. (2014). *Onderzoek CBP naar de verwerking van persoonsgegevens met cookies door de publieke omroep (NPO)*. Den Hague. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rap_2013_npo-cookies-publieke-omroep.pdf

CJEU. Scarlet Extended (2011). doi:EU:C:2011:771

CJEU. Case C-131/12 (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González) (2014). doi:ECLI:EU:C:2014:317

CJEU. Patrick Breyer v Deutschland (2016). doi:ECLI:EU:C:2016:779

Cohen, J. E. (1996). A Right to Read Anonymously: A Closer Look at "Copyright Management" In Cyberspace. *Connecticut Law Reviw*, *28*, 981–1039.

Council of Europe. (2013). *Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies*. Retrieved from https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c8011

Craig, P., & De Burca, G. (2015). *EU Law: Text Cases and Materials* (Sixth.). Oxford: Oxford University Press.

Crossley, D. (2015). Samsung's listening TV is proof that tech has outpaced our rights. *The Guardian*. Retrieved from http://www.theguardian.com/media-network/2015/feb/13/samsungs-listening-tv-tech-rights

Daalen, R. van. (2014). Liberty Global to Buy Ziggo for $9.4 Billion. *The Wall Street Journal*. New York. Retrieved from http://www.wsj.com/articles/SB10001424052702303277704579346041003510948

Düsseldorfer Kreis. (2015). *Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste*. Retrieved from https://datenschutz-berlin.de/attachments/1153/2015-Orientierungshilfe_SmartTV.pdf?

Düsseldorfer Kreis, & der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten. (2014). *Gemeinsame Position: Smartes Fernsehen nur mit smartem Datenschutz*. Retrieved from http://www.bfdi.bund.de/SharedDocs/

European Audiovisual Observatory. (2016). *Smart TV and data protection*. Strasburg.

European Commission. (2013). *Green Paper Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values, COM(2013) 231 final GREEN*. Brussels. Retrieved from https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/convergence_green_paper_en_0.pdf

European Commission. (2015). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market, COM(2015) 192 final Strategy for Europe*. doi:52015DC0192

European Commission. Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual m.

, Pub. L. No. COM/2016/0287 final (2016). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464618463840&uri=COM:2016:287:FIN

European Commission. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and personal data in electronic communications and repealing Directive 2002/58/EC ("Privacy and Electronic Communications Regulation") (2017).

European Parliament and of the Council. Directive 2010/13/EU of the European Parliament and of the 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 (Au (2010). Official Journal of the European Union L 95/1.

European Parliament and the Council. Directive 95/46/EC of the European Parliament and of the 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 (1995). Official Journal L 281/31. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

European Parliament and the Council. Directive 2002/21/EC of the European Parliament and of the 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 (2002). unofficially consolidated version. Retrieved from https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/140framework_5.pdf

European Parliament and the Council. Directive 2002/58/EC of the European Parliament and of the 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 ame (2002). (unofficially consolidated version). Retrieved from https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/24eprivacy_2.pdf

European Parliament and the Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da (2016). Official Journal of the European Union L 119/1. doi:L:2016:119:TOC

Ghiglieri, M., Hansen, M., Nebel, M., Pörschke, J. V., & Fhom, H. S. (2016). *Smart-TV und Privatheit - Bedrohungspotenziale und Handlungschancen*. (P. Zoche, R. A. Quinn, M. Hansen, J. Heesen, T. Hess, J. Lamla, … M. Waidner, Eds.) (Forum Priv.). Karlsruhe. Retrieved from https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/Forschungsbericht-Smart-TV-und-Privatheit_Druckfassung.pdf

Ghiglieri, M., Oswald, F., & Tews, E. (2013). HbbTV – I know what you are watching. In *13. German IT Security Congress of the BSI*. Retrieved from https://www.sit.tu-darmstadt.de/fileadmin/user_

Helberger, N. (2011). Diversity by Design. *Journal of Information Policy*, *1*, 441. doi:10.5325/jinfopoli.1.2011.0441

Helberger, N. (2016). Policy implications from algorithmic profiling and the changing relationship between newsreaders and the media. *Javnost*, *23*(2), 188–203. doi:10.1080/13183222.2016.1162989

Irion, K., & Valcke, P. (2015). Cultural Diversity in the Digital Age. In E. Psychogiopoulou (Ed.), *Cultural Governance and the European Union* (Palgrave S., pp. 75–90). Houndmills: Palgrave Macmillan.

Jakobsen, S. S. (2014). EU Internet Law in the era of Convergence: The Interplay with EU Telecoms and Media Law. In A. Savin & J. Trzaskowski (Eds.), *Research Handbook on EU Internet Law* (pp. 60–78). Cheltenham: Elgar.

Krotoszynski, R. J. (2016). *Privacy Revisited: A Global Perspective on the Right to be Left Alone*. Oxford: Oxford University Press.

Kuner, C. (2007). *European Data Protection Law*. Oxford: Oxford University Press.

Ladeur, K.-H., & Gostomzyk, T. (2014). Medienkollisionsrecht: Der Rundfunk im Netzwerk der Netzwerke. *Computer Und Recht*, (1), 28–35.

Michéle, B., & Karpow, A. (2014). Watch and be watched: Compromising all Smart TV generations. In *2014 IEEE 11th Consumer Communications and Networking Conference, CCNC 2014* (pp. 351–356). doi:10.1109/CCNC.2014.6866594

Newman, N., Fletcher, R., Levy, D. a. L., & Kleis Nielsen, R. (2016). *Digital News Report 2016*. Oxford. doi:10.1017/CBO9781107415324.004

Ofcom. (2015a). *International Communications Market Report 2015*. Retrieved from http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr15/icmr15/icmr_2015.pdf

Ofcom. (2015b). *Measurement framework for media plurality*. London. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0024/84174/measurement_framework_for_media_plurality_statement.pdf

Oostveen, M., & Irion, K. (2017). The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? In M. Bakhoum, B. C. Gallego, M.-O. Mackenordt, & G. Surblyte (Eds.), *Personal Data in Competition, Consumer Protection and IP Law - Towards a Holistic Approach?* Berlin Heidelberg: Springer Press.

Resnick, P., Garrett, R. K., Kriplean, T., Munson, S. a., & Stroud, N. J. (2013). Bursting your (filter) bubble. *Proceedings of the 2013 Conference on Computer Supported Cooperative Work Companion - CSCW '13*, 95. doi:10.1145/2441955.2441981

Richards, N. M. (2008). Intellectual Privacy. *Texas Law Review*, *87*, 387. Retrieved from http://papers.ssrn.com/abstract=1108268

Richards, N. M. (2014). *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford: Oxford University Press.

Roettgers, J. (2014). Gigaom | Netflix spends $150 million on content recommendations every year. *GIGAOM*. Retrieved February 28, 2016, from https://gigaom.com/2014/10/09/netflix-spends-150-million-on-content-recommendations-every-year/

Rössler, B. (2005). *The Value of Privacy*. Cambridge: Polity Press. doi:9780745631103

Schmidtmann, K., & Schwiering, S. (2014). Datenschutzrechtliche Rahmenbedingungen bei Smart-TV - Zulässigkeit von HbbTV-Applikationen. *Zeitschrift Für Datenschutz*, (9), 448–453.

Solove, D. J. (2010). *Understanding Privacy*. Harvard: Harvard University Press.

Stiftung Warentest. (2014). Ausgespäht: Datenschutz beim Fernsehen. *Test*, 40–41. Retrieved from https://www.test.de/Smart-TV-und-Datenschutz-Spion-im-Wohnzimmer-wenn-der-Fernseher-zurueckschaut-4695977-4695982/

Stiftung Warentest. (2016). Smart TV und Datenschutz: Was der Fernseher heimlich sendet. Retrieved from https://www.test.de/Smart-TV-und-Datenschutz-Was-der-Fernseher-heimlich-sendet-5039955-0/

Townend, J. (2017). Freedom of Expression and the Chilling Effect. In H. Tumbler & S. Waisbord (Eds.), *The Routledge Companion to Media and Human Rights*. Abingdon: Routledge.

Van der Sloot, B. (2012). Walking a Thin Line: The Regulation of EPGs. *Jipitec*, *3*(2). Retrieved from http://www.jipitec.eu/issues/jipitec-3-2-2012/3441

Visionary Analytics, SQW, & Ramboll. (2016). *Survey and data gathering to support the Impact Assessment of a possible new legislative proposal concerning Directive 2010 / 13 / EU (AVMSD) and in particular the provisions on media freedom , public interest and access for disabled people*. Brussels. Retrieved from http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=15867

Walden, I., & Woods, L. (2011). Broadcasting Privacy. *Journal of Media Law*, *3*(1), 117–141. doi:10.5235/175776311796471323

Zuiderveen Borgesius, F. (2016). Singling Out People Without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation. *Computer Law & Security Review*, *32*(2), 256–271. doi:http://dx.doi.org/10.1016/j.clsr.2015.12.013

Zuiderveen Borgesius, F. J., Trilling, D., Möller, J., Bodó, B., de Vreese, C. H., & Helberger, N. (2016). Should we worry about filter bubbles? *Internet Policy Review*, *5*(1), 1–16. doi:10.14763/2016.1.401