A right to reset your user profile and more: GDPR-rights for personalized news consumers

Eskens, S.

Published in: International Data Privacy Law

DOI: 10.1093/idpl/ipz007

Link to publication

Creative Commons License (see https://creativecommons.org/use-remix/cc-licenses): CC BY-NC-ND

A right to reset your user profile and more: GDPR-rights for personalized news consumers

Sarah Eskens*

Key Points
- News media more and more process personal data of news consumers to provide a personalized news selection on the news media home pages or in their apps.
- This article shows that the journalism provision in Article 85 of the EU General Data Protection Regulation (‘GDPR’) does not apply to the processing of personal data for news personalization. Therefore, the GDPR generally applies to such processing.
- This article finds that through exercising their data protection rights, news consumers may stop personalization or change their profile on which the personalization is based, to change the content that they are being recommended.
- We argue that in the context of news personalization, the most important function of the GDPR is to enable news consumers to determine how they are profiled or ‘read’.

Introduction
The personal data of online news consumers are increasingly being used for news personalization.1 Previously, news media distributed news to large anonymous audiences and processed personal data of news consumers only for subscription handling, marketing, and—on an aggregated level—advertising. These days, many online news media collect and analyse personal data to build detailed user profiles and to provide everyone a news selection based on his or her demographic details, geolocation, time zone, news stories read, website sections visited, device type, etc. A personalized news selection contains stories that are specifically relevant for a particular person. The New York Times, for example, states on its website:

We want to help you discover The New York Times journalism that is most interesting to you. To do that, we personalize aspects of your digital experience by offering story recommendations that are based on what you have already read, listened to or viewed.2

Personalization may mean, for example, that if you have read many news stories about Formula One in your daily news app the past few weeks, while you have never visited the section on Environment, your news app prioritizes a story about Lewis Hamilton winning the Singapore Grand Prix over a report about how micro plastics can spread via flying insects.

News websites provide personalization mostly in the form of recommendations in a sidebar or below articles as to what to read or view next,3 yet they are also

3 Kunert and Thurman (n 1), at 16.

* Sarah Eskens is currently affiliated to Institute for Information Law, University of Amsterdam, The Netherlands. This work was supported by the European Research Council under Grant 638514 (PersoNews). The author would like to thank the editors of this journal, the anonymous reviewers, and her doctoral supervisors Natali Helberger, Frederik Zuiderveen Borgesius, and Judith Möller for their useful suggestions and comments on this article.

© The Author(s) 2019. Published by Oxford University Press. This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs licence (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial reproduction and distribution of the work, in any medium, provided the original work is not altered or transformed in any way, and that the work is properly cited. For commercial re-use, please contact journals.permissions@oup.com
developing and experimenting with personalized homepages, apps, and push notifications. In addition, it is a widespread concern that there is a profile of them somewhere in the online realm. Personalized news systems extensively collect and store revealing personal data of news consumers. Mobile apps generally collect even more personal data than browser-based applications and thus create more data protection risks such as the misuse, leakage, or cross-context transfer of data. The General Data Protection Regulation (‘GDPR’) provides people who worry about the processing of their personal data for personalization some control over their data. However, the application of the GDPR to news personalization is not straightforward. The GDPR obliges Member States to create exemptions for personal data processing carried out for journalistic purposes, although it is an open question if this provision applies to news personalization. In addition, the meaning of many GDPR rules heavily depends on the context of application. For example, to understand how news consumers can stop the use of their personal data for personalization, it is necessary to know on which legal ground news organizations may process personal data. To answer that question, one needs to consider the news media market, the personalization technologies, and other contextual factors.

This paper assesses to what extent the GDPR provides people control over the processing of their personal data for news personalization. Previous work has studied the rights to privacy and data protection in the context of interactive television and personalized recommendations for television programs. This article focuses on data protection in the online personalized news context. The research is guided by two research questions: Does the journalism provision in the GDPR apply to news personalization? And, how does the GDPR provide people control over the processing of their personal data for news personalization?

Empirical research has shown that people who are concerned about their privacy often do not use privacy-preserving strategies and still disclose their personal data for news personalization. There are many third-party trackers associated with news apps among the apps having the most third-party trackers associated with them; see Reuben Binns and others (n 1).

This paper assesses to what extent the GDPR provides people control over the processing of their personal data for news personalization. Previous work has studied the rights to privacy and data protection in the context of interactive television and personalized recommendations for television programs. This article focuses on data protection in the online personalized news context. The research is guided by two research questions: Does the journalism provision in the GDPR apply to news personalization? And, how does the GDPR provide people control over the processing of their personal data for news personalization?
data to organizations.\textsuperscript{13} This privacy paradox has been explained by cognitive limitations that interfere with rational privacy decision-making.\textsuperscript{14} Another explanation for the observed privacy paradox is that people resign from privacy decision-making because they feel they have no real choice after all.\textsuperscript{15} Scholars and commentators therefore criticize the regulatory and scholarly focus on individual control.\textsuperscript{16} Nevertheless, as argued by Ausloos and Dewitte, even if only a few people exercise control, this may already provide a check and balance on the data processing activities of controllers.\textsuperscript{17} If a small group of news consumers exercises control over their personal data and, for example, demands changes in how personalization is provided to them, this could already have a disciplining effect on personalized news providers.

**Scope and plan of the paper**

In this article, we understand news personalization as:

A form of user-to-system interactivity that uses a set of technological features to adapt the selection, prioritization, and dissemination of news items to individual users’ interests, preferences, and other personal characteristics.\textsuperscript{18} \textsuperscript{18}

The technological features mentioned include recommender systems, which are computer programs that produce lists of relevant news items for different users, and machine-learning algorithms used within these systems to predict what are someone’s interests and to classify, select, and rank the news items.\textsuperscript{19} If news personalization relies primarily on information actively disclosed by news consumers themselves, we call it ‘user-driven personalization’. For example, some news apps ask people to fill in their personal details and tick boxes that indicate their favourite news topics or sources. Other personalized systems collect page views, search history, clicks, and likes to infer or predict someone’s interests, for which we use the term ‘system-driven personalization’.\textsuperscript{20}

To limit the scope of the article, we take the following as a starting point. Both user-driven and system-driven personalization generally involve the processing of personal data within the meaning of the GDPR.\textsuperscript{21} Any data relating to identified or identifiable news consumers are personal data.\textsuperscript{22} Someone is identifiable if she can be identified by name, IP address, cookies, or another online identifier such as a browser fingerprint.\textsuperscript{23}

An organization that provides people personalized news via a website or app is a controller, since it determines the purpose (namely: personalization) and means (namely: requiring people to indicate interests; storing and accessing cookies; logging website and app use; etc.) of the data processing.\textsuperscript{24} In its judgment in Case C-210/16 (*Wirtschaftsfakademie Schleswig-Holstein*), the European Court of Justice (‘the Court’) ruled that an administrator of a fan page hosted on a social network is a joint controller with the social media company.\textsuperscript{25} One can infer from this ruling that a news organization with a page on Facebook or any other social network is a joint controller regarding personalization via this social media page. A company that processes personal data on behalf of another news organization is a processor.\textsuperscript{26} News organizations, especially small sized ones, often hire subcontractors to do the user profiling and personalization if they do not have the in-house expertise.
knowledge for these operations.\(^{27}\) App stores, where people can download news applications for their devices, often also have an important role in determining the level of data protection offered to users, next to the controllers and processors.\(^ {28}\)

The GDPR’s territorial scope covers news organizations that conduct personalization if they are established in the EU or have a processor in the EU,\(^ {29}\) or if they are not established in the EU and neither have an EU-based processor, yet are processing personal data of news consumers in the EU by monitoring their behaviour.\(^ {30}\) In this article, we will not assess the general principles relating to the processing of personal data,\(^ {31}\) whether valid consent is given,\(^ {32}\) or how sensitive news user data should be dealt with.\(^ {33}\)

We will discuss provisions about the following topics: providing and withdrawing consent; entering and terminating a contract; objecting to processing in general and objecting to automated decisions-making specifically; right to rectification; right to erasure (‘right to be forgotten’); right to data portability. We do not discuss the right to restriction of processing, because it will be more useful for news consumers to rectify or erase data from their personal profile than just asking the organization to temporarily not to use data about them.\(^ {34}\)

The ‘Introduction’ section has just introduced our research question. The ‘Journalism provision’ section discusses the journalism provision. The ‘Stopping personalization’ section looks at various ways in which people can stop news personalization via their data protection rights. The ‘Amending your profile’ section demonstrates how people can change the kind of content they are being recommended by exercising their data protection rights, and the ‘Moving your profile’ section analyses if people can move their profiles to other news providers. The ‘Conclusion’ section concludes.

### Journalism provision

The GDPR obliges Member States to reconcile personal data protection with freedom of expression, including, among others, journalism.\(^ {35}\) More specifically, Article 85, paragraph 2, of the GDPR requires Member States to include in their domestic laws exemptions or derogations for journalistic data processing from a range of provisions of the GDPR.\(^ {36}\) For the purposes of this article, we call this provision the ‘journalism provision’, although the provision also covers academic, artistic, and literary expression. If the journalism provision applies to news personalization, then news organizations may be exempted from certain data protection rules when they process personal data for personalization.

The journalism provision is one example of where the GDPR allows Member States some discretion to adopt their own data protection rules.\(^ {37}\) Still, the EU Treaties oblige Member States to not impede the direct effect of the GDPR or hinder its simultaneous and uniform application in the EU when they adopt national data protection measures.\(^ {38}\) Under the Data Protection Directive (‘DPD’), the predecessor of the GDPR, Member States had implemented the journalism provision very differently in their domestic laws.\(^ {39}\) As one of the aims of the GDPR is to harmonize national data protection legislation, a straightforward interpretation of the scope of the journalism provision is necessary to limit national legal differences.

To get an impression of the effects of the application of the journalism provision for the individual rights of...

---

27 For example, Personyze, Akingo, and Viafoura provide personalization technology to website publishers; see <https://www.personyze.com/>; <http://www.akingo.com/>, and <https://viafoura.com/personalization/>.


29 Art 3(1) GDPR. See also European Data Protection Board, ‘Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version for public consultation’ (23 November 2018).

30 Art 3(2)(b) GDPR.

31 Art 5 GDPR.

32 Art 7 GDPR.

33 Art 9 GDPR. To limit the scope of this article, the author of this article will not discuss sensitive consumer data in another study.

34 The right to restriction of processing might be useful in other contexts. For example, if someone switches services and the old service provider is legally obliged to store client data for a certain period, then the data subject can request the restriction of processing to ensure that her data will not be used for other goals.

35 Art 85(1) GDPR.

36 Art 85(2) GDPR.


38 Note that the Commission calls such clauses ‘specification clauses’, maybe to prevent the suggestion that the GDPR does not aim for full harmonisation; see <http://www.europarl.europa.eu/doceo/document/P-8-2018-03121-ASW_EN.html> (all accessed 24 March 2019) and Paul Nemitz as paraphrased in Dennis Kenji Kipker, ‘How Much Diversity in Data Protection Law Does Europe Need or Can Afford Reports: Germany’ (2017) 3(2) European Data Protection Law Review (EDPL) 229, at 231.

39 Fratelli Zerboni Snc v Amministrazione delle Finanze dello Stato (Italian Finance Administration), Case 95/77 [1978], at paras 24 and 25.

news consumers, we take as an example the Netherlands. The journalism provision in the Dutch law implementing the GDPR entails that news consumers do not have the rights to withdraw consent, to rectification, to erasure, to restrict processing, or to object against automated decision-making. Furthermore, under the Dutch journalism provision, news organizations outside of Europe would not be obliged to appoint a representative in the EU to which people can turn if they have questions or complaints about the processing of their data for personalization.

The application of the journalism provision to news personalization would thus derive news consumers of many of their data protection rights. From a user rights perspective, one might therefore want to argue that the journalism provision does not apply to news personalization. In its judgment in Case C-131/12 (Google Spain), the European Court of Justice indeed held that data protection rights ‘as a general rule’ override the interest of internet users to access information. Since this judgment, legal scholars have pointed out that the Court seems to favour data protection over freedom of expression, that is, seems to have established a hierarchy of rights with data protection above freedom of expression.

On the other hand, the Court delivered its judgment in Google Spain in the context of someone requesting a search engine to remove personal data relating to him so that these data would no longer be included in the search results and the hyperlinks to a news website. Brkan therefore remarks that the Court’s established hierarchy could be limited to such specific cases instead of applying to data protection in general.

In the remainder of this section, we analyse if the journalism provision applies to news personalization. We use three different legal interpretation techniques to find arguments for both sides of the argument and then draw a conclusion.

**Textual approach**

We start with the exact phrasing of the journalism provision and ask what its terms mean:

For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations (…) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

The key term here is ‘journalistic purposes’. The question is if news personalization is a journalistic purpose within the meaning of the GDPR. The European Court of Justice noted in its judgment in Case C-73/07 (Satamedia) that ‘it is necessary (…) to interpret notions relating to [freedom of expression], such as journalism, broadly’. The Court then held that activities are regarded as ‘solely for journalistic purposes’ if ‘the sole object of those activities is the disclosure to the public of information, opinions or ideas’. In Satamedia, the Court thus laid down a broad notion of journalism, under which almost all expressive activities can be journalism.

But in its subsequent judgment in Google Spain, the Court narrowed the notion of journalism by stating that the publication of personal data by the operator of a search engine is not carried out solely for journalistic purposes. The Court did not specify what it is about

---

40 Art 43 Uitvoeringswet Algemene verordening gegevensbescherming (‘UAVG’).
41 Art 43 UAVG.
42 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 [2014] ECLI:EU:C:2014:317, at paras 81 and 97.
44 Google Spain (n 42) para 15.
45 Brkan (n 43) para 826.

47 Art 85(1) GDPR.
49 Ibid para 62. Note that this case concerned the journalism provision in the DPD. In the DPD, the journalism provision required exemptions for the processing of personal data carried out ‘solely for journalistic purposes’. This is why the Court also talks about ‘solely’ here.
50 Google Spain (n 42) para 85. The judgment was handed down in Spanish and the English translation of the case contained a translating mistake. The translation provided that it ‘does not appear’ that search engine operators process personal data for journalistic purposes, thereby suggesting that under certain circumstances, search engine operators could actually process data for journalistic purposes. The original Spanish text, however, rules this out entirely; see Stefan Kulk and Frederik J Zuiderveen Borgesius, ‘Google Spain v. González: Did the Court Forget about Freedom of Expression?’ Case C-131/12 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González’ (2014) 5(3) European Journal of Risk Regulation 389, at 395 in fn 58. See also David Erdos, ‘From the Scylla of Restriction to the Charybdis of Licence! Exploring the Scope of the “Special Purposes”'
the publication of personal data by search engines that distinguishes it from publication by news websites. We presume the Court holds the view that merely making personal data more accessible by including it in a list of search results, like a search engine does, is not sufficiently substantive do be deemed journalism. Or, as Erdos argues, the Court in Google Spain implied, and in its more recent judgment in Case C-345/17 (Buivids), explicitly confirmed that its reference in Satamedia to ‘the public’ should be understood as ‘the body politic’ and not just ‘any indeterminate number of people’. The journalism provision would then apply only to personal data processing that contributes to a public debate. In any case, if one upholds a narrow notion of ‘journalistic purposes’, then the journalism provision is to be narrowly construed.

Other textual elements of the GDPR also indicate that the journalism provision is narrow. The recitals to the GDPR stipulate that exemptions and derogations are allowed for ‘processing of personal data solely for journalistic purposes’. Next to that, the journalism provision states that exceptions and derogations should be provided if they are necessary to reconcile the right to the protection of personal data with freedom of expression and information. The necessity requirement implies a restrictive interpretation. If one maintains that journalism consists of news production and publication, then an exemption for news personalization activities is not necessary to reconcile media freedom and data protection. News organizations may produce and publish as much content as they like, regardless of whether they are able to disseminate this content to their audiences in a personalized manner.

Some scholars however argue that with today’s online, networked journalism, ‘the question of who gets which story and how becomes a matter of concern for many journalists’. Napoli and Caplan also observe that the three core activities of media companies (production, distribution, and exhibition) have merged through digitization and media convergence. Others say it is part of the civic role of journalism to deploy personalized recommender systems to provide citizens with the information they need. Furthermore, personalized news systems essentially make decisions previously made by human editors, such as how to prioritize various news stories and who should see which news selection. From this perspective, one could say that personalized dissemination of news is part of journalism, hence should fall under the journalism provision. Through the digitalization of both the production and dissemination of news, the two are harder to distinguish. The Article 29 Working Party foresaw a blurring of the borders between clear journalistic activities and related activities already in 1997:

The moving of traditional media towards electronic publishing and the provision of on-line services seems to add further elements for reflection. The distinction between editorial activities and non-editorial activities assumes new dimensions in relation to on-line services which, unlike all traditional media, allow an identification of the recipients of the services.

Finally, the European Court of Human Rights (‘ECtHR’) held that the right to freedom of expression is guaranteed in the European Convention on Human Rights also protects the means of transmission or reception of communication, next to the content, because any restriction imposed on communication technologies interferes with the right to receive and impart information. The ECtHR further held that the right to

53 Ibid.
54 Recital 153 GDPR [author’s emphasis in quoted text]. See similarly, Jozwiak (n 43) 412. The requirement that the journalism provision applies to data processing ‘solely for journalistic purposes’ moved from the operative provisions in the DPD to the recitals in the GDPR; see (n 49).
55 The Court in Satamedia (n 48), para 56, even held that exemptions should be strictly necessary.
freedom of expression does not apply solely to certain types of information or forms of expression, yet also covers information of a commercial nature and advertisements. A wide reading of the journalism provision would be in line with the broad scope given to the right to freedom of expression by the ECtHR.

The textual approach is thus inconclusive. A solution could be to determine that news organizations can invoke the journalism provision for news personalization, whereas social media, search engines, and news aggregators cannot. Facebook notably sees itself as a social network service, not as a kind of media. If an organization does not want to qualify as a media entity, it cannot invoke the journalism provision either.

**Historical approach**

Since the textual approach is inconclusive, we try to determine what the drafters of the journalism provision meant when they drafted it and what they would do when presented with the facts of the case. Several EU Member States included exemptions for the media in their domestic data protection laws, long before the DPD and later the GDPR were enacted. In 1990–92, the European legislator was drafting the DPD. The European legislator obliged Member States to grant exemptions for the press because it wanted to harmonize the different national approaches towards personal data and the media. When the European legislator was negotiating the GDPR in 2012–16, it did not substantively change the journalism provision, beyond the fact that it integrated case law of the Court of Justice of the European Union in the recitals. The European legislator also added to the recitals that the journalism provision should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. We have not found any indication that the European legislator considered the journalism provision should apply to more ancillary activities performed by news media, even though personalization and other new technologies for journalism existed when the GDPR was drafted.

Next to that, the Article 29 Working Party observed in 1997 that in various countries, the ordinary data protection regime generally applies to non-editorial activities performed by the media. The Working Party concluded that derogations and exemptions should cover ‘only data processing for journalistic (editorial) purposes including electronic publishing’, and that any other form of data processing by journalists or the media should be subject to the ordinary rules of the DPD. The Working Party stressed that the distinction between editorial and other purposes pursued by the media was particularly relevant in relation to electronic publishing, since the processing of subscriber data for billing or direct marketing should fall under the normal rules.

We argue that personalization is more similar to billing or direct marketing than to producing news. A historical view suggests that the journalism provision was written to protect the production and publication of news content, whereas news personalization is a different kind of journalistic activity. The historical approach would thus lead to the conclusion that the journalism provision is not applicable to news personalization. Overall, EU Member States, the European Commission, and Data Protection Authorities have always adopted a rather narrow understanding of the journalism provision.

**Functional approach**

Because the textual and historical approach leave doubt about the interpretation of the journalism provision, we finally consider what the purpose of the exemption is. The journalism provision was written to deal with situations in which news stories contain personal information of people involved in a story, such as their name or

---

65 Erdos found that data protection authorities indeed generally apply data protection rules to social networking services and search engines; see David Erdos, ‘Data Protection Conflicts of Freedom of Expression on the “New Media” Internet: The Stance of European Regulatory Authorities’ (2015) 40(4) European Law Review 531.
66 Mark Zuckerberg said in an interview: ‘In general, we’re a social network. I prefer that because I think it is focused on the people part of it — as opposed to some people call it social media, which I think focuses more on the content. For me, it’s always been about the people’; see Kara Swisher, ‘Zuckerberg: The Recode Interview’ (Recode, 18 July 2018) <https://www.recode.net/2018/7/18/17572156/mark-zuckerberg-interview-facebook-recode-kara-swisher> (accessed 24 March 2019). See also Matt Carlson, ‘Facebook in the News’ (2018) 6(1) Digital Journalism 4.
67 Note however, that in litigation, Facebook lawyers have tried to make the argument that Facebook should be able to rely on free speech protections for the media.
70 European Commission, PROPOSAL, COM/2012/011 final, 25 Jan 2012, Recital 121, echoes Satamedia and Google Spain, among others.
71 Recital 133 GDPR.
72 Article 29 Working Party, ‘Recommendation 1/97’ (n 61) 6. Author corrected ‘non editorial’ in the original text into ‘non-editorial’.
73 Ibid 8.
74 Ibid.
75 Erdos (n 50) 132 and further.
picture. By publishing such a story containing personal data, the media interferes with someone’s fundamental right to the protection of personal data. In that case, strict application of the data protection rules could limit media freedom.76 Legal restrictions on the processing of personal data by media actors are effectively a governmental decision on what information media can publish. Furthermore, the fears of sanctions or claims for violation of data protection law could also have a chilling effect on the exercise of journalistic freedoms.77 In other words, the function of the journalism provision is to ensure news media can produce and publish news stories containing personal data. The journalism provision does not aim to exempt the processing of personal data in order to enable news dissemination.

Sub-conclusion

We conclude that the journalism provision does not apply to news personalization, in so far as news personalization concerns the processing of personal data to disseminate news stories to specific audience members.78 The media needs exemptions or derogations when strict data protection rules would hinder the production and publication of a news story. The journalism provision therefore enables them to freely use personal data in a publication, whereas news personalization as discussed in this article is about the processing of personal data to disseminate stories. Besides, the media’s right to freedom of expression and the public’s right to receive information is only slightly interfered with when the media is required to comply with the GDPR to personalize the news. The GDPR does not block the media from disseminating news content; it merely conditions how the media may process personal data to disseminate news in a personalized manner.

Stopping personalization

If the journalism provision in the GDPR does not apply to personalization, then news consumers may exercise the full range of their data protection rights. People are empowered to control the processing of their personal data for news personalization, and with that they might as well influence the kind of news content that they are recommended and receive. Taken together, the data protection rights of news consumers boil down to two options: people may stop personalization altogether or they may amend their profile on which the personalization is based. In this section, we discuss stopping personalization and in the next section amending personalization profiles.

The way in which someone may (temporarily) stop personalization depends on which legal ground the personal data processing is based. The GDPR states that personal data processing is lawful only if the data controller can rely on one of six legal grounds for processing.79 In the context of news personalization, four of the six legal grounds are relevant (consent; contract; public task; legitimate interests), which leads to two different ways to stop personalization. A third way to stop personalization is based on rules concerning objecting against automated processing and decision-making. The legal ground to process personal data for news personalization is important because it determines how people can intervene with personalization and to what extent Member States can introduce more specific measures to ensure lawful and fair processing and personalization.

Withholding or withdrawing consent

News personalization might be lawful if a news consumer has given consent to the processing of her data

76 Tietosuoja- ja civilivakuutuskomissio v Satukunan Markkinapörsi v Ny and Sata media Oy, Case C-73/07 [2008] (ECLI:EU:C:2008:727), Opinion of AG Kokott, para 43.
78 Our analysis would be different for personalised content creation. For example, the Dutch news publication FD is developing a system to provide personalised summaries of news articles, in which people’s interests and preferences will be used to create content, not just to get the content to them. See Ernst-Jan Hamel, ‘Waar blijft de robotjournalistiek in Nederland?’ Stimuleringsfonds voor de Journalistiek, 1 May 2018 <https://www.svdj.nl/nieuws/waar-blijft-robotjournalistiek-in-nederland/> (accessed 24 March 2019). Adar and others created the PersaLog tool for personalisation within news articles; see Eytan Adar and others, ‘PersaLog: Personalization of News Article Content’, in Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (ACM 2017).
79 Art 6(1) GDPR provides that processing of personal data shall be lawful only if and to the extent that at least one of the following legal grounds applies: (a) the data subject has given consent; or processing is necessary for (b) the performance of a contract; (c) compliance with a legal obligation to which the controller is subject; (d) protecting someone’s vital interests; (e) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) the purposes of the legitimate interests pursued by the controller or by a third party.

If a news organisation collects data for personalisation via cookies or other tracking techniques, art 5(3) ePrivacy Directive requires them to obtain consent to store and access these tracking technologies on someone’s device, regardless of the legal ground relied on to further process the data and regardless of whether the cookies collect personal data or any other kind of data. On the relationship between the GDPR and the ePrivacy rules, see among others Frederik J Zuiderveen Borgesius, ‘Personal Data Processing for Behavioural Targeting: Which Legal Basis?’ (2015) 5(3) International Data Privacy Law 163 and Andrew Cormack, ‘The Draft ePrivacy Regulation: No More Lex Specialis for Cookie Processing?’ (2017) 14(2) SCRIPTed 345.
for the personalization.80 When installing a news app and people are prompted to consent, an option to cancel or otherwise halt the installation of the app should be available, instead of just an ‘accept’ button.81 People may withdraw consent at any time to stop the processing of their data for personalization, and thus effectively stop personalization.82

Organizations often need a set of personal data for several purposes, such as personalization, billing, marketing, and advertising. These different purposes might be based on different legal grounds. If a set of personal data is covered by multiple legal grounds to legitimize the processing, a news organization might still be able to process the data for another purpose after someone has withdrawn consent for personalization.83

Withdrawing consent for personalization without detriment

News consumers’ consent should be freely given, specific, and informed.84 People cannot freely give consent if they are unable to refuse or to withdraw consent without negative effects.85 According to the Article 29 Working Party, this means news organizations should enable people to withdraw consent free of charge and ‘without lowering service levels’.86 The latter requirement is problematic if personalization is regarded as an value-added service. If people do not consent to personalization, it is impossible for website operators to still provide the same service level.

The rules on obtaining and withdrawing consent could mean two different things for the personalized news market. One could argue that every news organization that asks people for consent to personalize their news stream should as well offer a non-personalized service to those who do not want to give consent. Otherwise these people would be pressured into accepting personalization in order to receive at least some news via that service. This seemed to be the reasoning of the Dutch Data Protection Authority in a couple of enforcement actions regarding smart televisions. The Dutch Data Protection Authority found that television viewers should be able to choose between agreeing or disagreeing to personalized recommendation services via their smart television,87 instead of between agreeing or not having an internet connected television at all.

One could also argue that the entire news service market should be taken into account to assess if consent is freely given, instead of just taking one particular service as the frame of reference. If there are personalized and non-personalized news services of a similar quality and orientation on the market, people can freely reject personalization by one news outlet and still use other news sources. But if there are only personalized news services on the market or just personalized services and non-personalized news services of a very different quality and orientation as the personalized ones,88 and these personalized news services do not allow people to withhold consent for news personalization specifically, then privacy-minded people who do not want personalization can only opt for not receiving news at all or receiving news of a different quality and orientation.89 Under such circumstances, people cannot freely give or withdraw consent for news personalization. The question in this scenario is who should ensure there are also non-personalized services. Should the government, via public service media or regulation, or the market account for that? Here, a question of data protection law develops into a media policy question.

Withdrawing consent specifically for personalization

The GDPR requires that news consumers give consent for the specific purpose of personalization.90 In the context of news apps, simply clicking an ‘install’ button does not result in specific consent, so during installation more specific consent for personalization should be obtained.91 When their data is being processed for multiple purposes, people should be free to accept one purpose and not the other.92 Research into privacy policies of Dutch and German newspapers indicates that news organizations often combine consent for different

80 Art 6(1)(a) GDPR.
82 Art 7(3) GDPR.
84 Art (6)(1) GDPR. See also, Recitals 32, 40, 42, and 43 GDPR.
85 Recital 42. See also Article 29 Working Party, ‘Guidelines on consent’ (n 83) 5.
86 Ibid 21.
87 Irion and Helberger (n 12) 176–77.
88 See similarly, the Dutch Data Protection Authority, as cited by Irion and Helberger (n 12) 180: there is no alternative for Dutch public broadcasting content, so when the Dutch Public Broadcasting Organisation provides people a cookie wall, they cannot freely give consent.
89 See similarly, Zuiderveen Borgesius and others regarding consent and tracking walls: ‘It is dubious whether consent is still “freely given” if a company uses a tracking wall and there are no competitors that offer a similar, more privacy-friendly service. Somebody who does not want to disclose personal data would not have the possibility to use a certain type of service’; see Frederik J Zuiderveen Borgesius and others, ‘Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation’ (2017) 3(3) European Data Protection Law Review 353, at 362.
91 Article 29 Working Party, ‘Opinion 02/2013’ (n 10) 15.
processing purposes. An exception are several websites from Dutch public broadcasters. For example, when you enter the website of the VPRO, you are asked to provide consent for personalized content, social media cookies, and targeted advertising.

There have been complaints about the amount of consent requests from Dutch public broadcasters, but in our view they take the right approach. News organizations may not group consent for news personalization, marketing, and targeted advertising. Personalization of journalistic content and targeted marketing or advertising are different processing purposes because they serve different objectives. News personalization has many objectives, among which are showing the diversity of content, pushing important stories that reached too few people, serving niche audiences with specific interests, driving pay-per-article sales, or providing more context to news events. The objectives of targeted marketing and advertising partially overlap with the objectives of news personalization, such as growing readership, yet marketing and advertising do not have any of the editorial goals that news personalization has.

It should be remarked that regardless of the rules on specific consent, internet users often do not distinguish between personalized news, targeted advertising, personalized movies and music recommendations, and responsive websites. What contributes to the confusion

93 Mariella Bastian, Jaron Harambam, and Mykola Makhortykh, ‘Personalizing the news: How media outlets communicate their algorithmic recommendation practices online’ (Amsterdam Privacy Conference, Amsterdam, 10–12 October 2018).

94 <www.vpro.nl> (accessed 8 November 2018). See Figure 1.


96 Irion and Helberger (n 12) 174.


98 Monzer and others (n 9). See similarly, Sarikakis and Winter (n 15) 10: social media users do not distinguish online platforms and services in...
is that news websites sometimes display sidebars that contain both personalized recommendations for editorial content and targeted advertisements. People are getting used to web personalization and they just like or dislike a personalized online experience. In that regard, the legal framework does not suit people’s mental model of the internet.

Terminating a contract

News personalization might be lawful if it is necessary for the performance of a news subscription or another kind of news contract, such as a paid news aggregation service. News consumers may terminate the news subscription according to the rules of national contract law and accordingly stop personalization. Almost half of news publishers (44 per cent) surveyed by Reuters Institute see subscriptions, that is contracts, as a very important source of digital revenue.

According to the Article 29 Working Party, data processing cannot be legitimized by a contract if the controller imposes unnecessary data processing on the data subject, claiming it is necessary for the performance of said contract. For example, webstores may not profile their customers based on items purchased while citing the sales contract as a legal ground, since such profiling is not necessary to deliver the good or service. This means that if a news organization sells not-personalized news services, it cannot just implement news personalization alleging this is necessary for the performance of the contract. Furthermore, if a news organization offers a personalized news service, yet also includes in its contract consent for other data processing purposes, such as marketing, news room data analytics, or behavioural advertising, the consent provisions should be clearly distinguishable from the other contract provisions.

Many traditional news organizations are currently renewing their services by making their websites and apps more personalized. For existing news subscriptions, personalization will not be deemed necessary for the performance of the contract since it was never part of the original service. These news organizations will need to ask their subscribers for additional consent to personalize their news offerings. In the latter case, people may refuse consent or later withdraw consent to stop personalization.

Objecting to Processing

Next to consent or a contract, news personalization might also be lawful if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (‘public task-ground’), or if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (‘legitimate interest-ground’). When news organizations rely on one of these two legal grounds, news consumers have the right to object to the involved processing of their personal data.

The difference between refusing to give consent or terminating a contract and objecting to personalization, is that news organizations cannot challenge the refusal of consent or a lawfully terminated contract. In contrast, in the case of objection, a news organization may continue processing the personal data if it can give compelling legitimate grounds for the processing which override the interests of the data subject. The burden of proof is on the new organization to demonstrate that its interest overrides the interests of the data subject. For example, a news organization could argue it is necessary to deploy news personalization for voice-assistant devices (without screens) because it is impossible to display a home page or side column on these. Furthermore, Member States may introduce more specific requirements for the personal data processing and other measures to ensure lawful and fair processing if the personalization is based on the public task-ground. National law could demand, for example, that news consumers are able to reset their personalization profile to continue with a clean slate.

99 Kunert and Thurman (n 1) 16–17.
100 Art 6(1)(b) GDPR.
103 Ibid 17.
105 See previous subsection ‘Withdrawing consent specifically for personalisation’.
106 Art 6(1)(e) GDPR.
107 Art 6(1)(f) GDPR.
108 Art 21(1) GDPR.
109 Art 21(1), second sentence, GDPR.
110 Recital 69 GDPR.
111 Art 6(2) GDPR.
May media organizations invoke their public task or legitimate interest?

The question is under what conditions public and private news media may invoke the public task- or legitimate interest-ground for personalization. In any case, public authorities may not invoke the legitimate interest-ground for processing carried out in the performance of their tasks.112 The idea is that public authorities may process data in performance of their tasks only if they are democratically authorized by law to do so and not when they themselves just decide it is necessary.113 The GDPR does not define ‘public authority’ and according to the Article 29 Working Party, domestic law should determine this notion.114 Some national laws implementing the GDPR indeed define ‘public authority’115 whereas others do not.116 Regardless of national differences, the Article 29 Working Party determined that public authority may be exercised by both public authorities and other natural or legal persons governed by public or private law, such as public service broadcasters (this is an example given by the Working Party).117 For the purpose of this article, we therefore assume that public service media are a public authority within the meaning of the GDPR. Public service media thus may not carry out personalization based on the legitimate interest-ground.

Instead, public service media could lawfully personalize the news if this processing of personal data is necessary for the performance of their public interest task.118 The legal basis for such processing should be laid down by Union or Member State law and the purpose of the processing (in this case, personalization) should be necessary for the task to be performed (in this case, the public service remit).119 The recitals to the GDPR state that it is not required to have a specific law for each individual processing operation.120 The Article 29 Working Party further specified that the legal basis should be ‘specific and precise enough in framing the kind of data processing that may be allowed’.121 Furthermore, the Union or Member State law should meet an objective of public interest and be proportionate to the legitimate aim pursued.122 The latter conditions echo the general conditions of Article 52, first paragraph, of the EU Charter for limitations on fundamental rights and freedoms.123 We can imagine that, for example, a domestic law which requires public service media to collect personal data of news consumers across the entire internet, beyond the websites of these public service media themselves, would not be proportionate to the aim of delivering diverse news.

The GDPR allows that Union or Member State law appoints a public authority, another natural or legal person governed by public law, or a natural or legal person governed by private law, carries out the public interest task.124 For example, the United Kingdom and France have private media with public service commitments (respectively ITV and TF1).

On the basis of these provisions, personalization by public service media or private media with public service commitments can be lawful if Union or Member State law specify a public interest task for such media, this law serves a public interest and is proportionate, and it can be argued that personalization is necessary for this public remit. For example, the Dutch Media Act defines the public media task as ensuring a media offering that aims to provide a wide and diverse audience with information, culture, and education, via all available channels.125 The Dutch public media task also includes stimulating innovation regarding media satisfaction.

112 Art 6(1)(f) GDPR: ‘Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks’.
113 Article 29 Working Party, ‘Opinion 06/2014’ (n 102) 27. If the law oblige public authorities to process data for a public task, the processing falls under the c-ground.
114 Article 29 Working Party, ‘Guidelines on Data Protection Officers (’DPOs’)’ (WP 243.rev01, 5 April 2017), 6. With thanks to @Paapst for pointing this out.
115 See for example, art 5 of the Belgium law implementing the GDPR.
116 See for example, the Dutch Uitvoeringswet Algemene verordening gegevensbescherming (GDPR Implementation Act). Still, the Explanatory Memorandum with the Dutch GDPR Implementation Act states: ‘Er kan, zoals de Autoriteit persoonsgegevens terecht heeft opgemerkt, worden aangesloten bij algemene leerstukken van het bestuurlijk organiseren (attributie, mandaat, delegatie en de begrippen bestuursorgaan, publiekrechtelijke bevoegdheid en publiekrechtelijke taak)’. With thanks to @ICTRecht, who showed me where to find the answer to this question.
118 Art 6(1)(e) GDPR.
119 Art 6(3) GDPR.
120 Recital 45 GDPR.
121 Article 29 Working Party, ‘Opinion 06/2014’ (n 102) 22. Note that this opinion of the Article 29 Working Party related to the Data Protection Directive. The DPD did not require that the public interest task be laid down by Union or Member State law. Nevertheless, the Article 29 Working Party considered that the ‘public task will have been typically attributed in statutory laws or other legal regulations’. In that context, it added that ‘the legal basis should be specific and precise enough in framing the kind of data processing that may be allowed’. We presume that this consideration of the Article 29 Working Party also holds for the GDPR, which does explicitly require a legal basis for the public interest task.
122 Art 6(3), last sentence, GDPR.
123 Art 52(1) EU Charter: ‘Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others’.
124 Recital 45 GDPR.
125 Art 2.1(1)(a) Dutch Media Act [author’s translation],
offerings using new opportunities to serve media content to the public with novel media- and dissemination technologies. On this basis, Dutch public media could probably use personalization to perform their public media task. Other research has also found that many public service media indeed see personalization as a way to realize their public task of universality, that is, the provision of diverse news to all citizens. In this area, and other sectors, the GDPR thus allows for national differences regarding lawful instances of data processing.

Private sector media could lawfully personalize news if it is necessary for the purpose of their own legitimate interest or a third party’s interest, except where the interests or fundamental rights of the news consumer outweigh these legitimate interests. The Article 29 Working Party finds that the interest of controllers in getting to know their customers’ preferences to better personalize their offers and offer products and services that better meet the needs and desires of the customers, is a legitimate interest. News organizations may thus invoke their own commercial interest to personalize news. Besides that, the Article 29 Working Party has determined that organizations may also cite more socially relevant interests, such as the interest of the press to publish information about government corruption. Private news media could thus also argue that news personalization is in the public interest.

Objecting

If news media rely on the public task- or legitimate interest-ground, people may object to the personalization on grounds relating to their particular situation. In contrast, objection is not possible if the processing is based on consent or a contract. The reason for this limitation is that people already have control over their personal data through (not) providing consent or (not) signing a contract. The right to object compensates for the fact that people have no initial control over their personal data when an organization invokes the public task- or legitimate interest-ground.

News organizations may rebut the objection to personalization by demonstrating that its compelling legitimate grounds for the processing override the interests or rights of the news consumer. A media organization could try to argue, for example, that news personalization is necessary to carry out their task to educate people on political affairs, for which people may have different entry levels requiring different kinds of news messages. When the lawmaker determines that certain data should be processed for a public task or when an organization invokes the legitimate interest-ground, they can consider the interests of a group of data subjects but it is practically impossible for them to consider the interests of each individual data subject at that stage. An objection requires a news organization to more specifically consider someone’s personal situation and balance this with the public interest or its own legitimate interests.

If a news consumer objects against personalization, she may ask the controller to restrict the processing. The news organization should then ‘interrupt (or avoid starting)’ the personal data processing. While the news organization is still assessing whether the public interest or its own interest overrides those of the data subject, the processing should already be restricted. After a successful objection (that is, when there are no overriding legitimate grounds for the processing), the news consumer may further ask the news organization to erase the data.

When someone successfully objects and the controller restricts the processing, other data processing operations on the same data may continue, such as storing the data. For example, if you object to direct marketing

126 Art 2.1(1)(c) Dutch Media Act [author’s translation].
127 Van den Bulck and Moe (n 97) 16.
128 Wagner and Benecce (n 37).
129 Art 6(1)(f) GDPR. This section focuses only on the question whether news personalization is a legitimate interest. The legitimate interest-ground also demands that organisations show the processing is necessary, and that they balance their legitimate interest with the data subject’s interests. If the data subject’s interests override the legitimate interest, an organization may not invoke the legitimate interest-ground.
131 Ibid 24.
132 Art 21(1) GDPR. Under art 14(a) DPD, data subjects had to give compelling legitimate grounds relating to their situation to successfully object to the processing. Under the GDPR, data subjects only need to give grounds and controllers need to give compelling legitimate grounds to rebut the objection. In that regard, the GDPR entails a shift of the burden of proof; see Article 29 Working Party, ‘Guidelines on consent’ (n 83) 19. The controller now has to prove that the processing is legitimate, whereas previously the data subject had to demonstrate that he or she had good reasons to object. This shift of the burden of proof is reasonable, since the controller is in a better position to know all the implications of the processing; see Cécile de Tervagne, ‘The Right to Be Forgotten and the Informational Autonomy in the Digital Environment’ (European Commission 2013), 16. The shift of the burden of proof also fits the introduction of the new accountability principle of art 5(2) GDPR.
133 Note that the right not to be subject to a decision based on automated processing is available in the context of consent or a contract; see next subsection ‘Not Being Subject to Automated Individual Decision-making’.
134 Art 21(1) and Recital 69 GDPR.
135 Google Spain (n 42) para 76. See also Article 29 Working Party, ‘Guidelines on consent’ (n 83) 18-19.
136 Art 18(1)(d) GDPR.
138 Art 18(1)(d) GDPR.
139 Art 17(1)(c) GDPR.
by phone, the marketer will put your telephone number on a do-not-call list, but it will not delete your telephone number and stop processing your personal information altogether. In the context of personalization, people might thus successfully object to personalization, after which their data could still be used for other processing operations, such as building models and profiles for collaborative filtering. News organizations that expect difficulties for their algorithmically created models for news recommendations if people would erase their data (see ‘Amending your profile’ section), could thus try to nudge people who do not want personalization to only object against processing for the purpose of personalization instead of to erase their data entirely from the systems.

**Not being subject to automated individual decision-making**

Under Article 22 GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. We see news personalization as a form of decision-making based on automated processing in the sense that every time a news algorithm decides to recommend someone a particular news item, this recommendation is based on automated processing such as collecting and analysing personal data of news consumers. The implications of the right not to be subject to automated decision-making are potentially huge, since it could mean that news organizations are prohibited from using news personalization. However, as we will see, the right not to be subject to automated decision-making is conditioned and applies to news personalization only in very limited situations.

The first question is whether news personalization produces legal effects concerning news consumers or similarly significantly affects them. The notion of ‘legal effect’ was already used in the DPD and the Article 29 Working Party explains the notion similarly to how scholars interpreted it previously, namely as an effect on someone’s legal rights or obligations, such as the freedom to associate or to vote in an election. A legal effect may also be an effect on someone’s legal status or rights under a contract, the denial of a particular social benefit granted by law, or the refused admission to a country. The Article 29 Working Party also established that the right not to be subject to automated decision-making covers only ‘serious impactful effects’. It thus appears that the notion of ‘legal effect’ has a substantive and a relative element: is there an established legal right that is affected, and, is the effect sufficiently serious? If someone is not automatically recommended a certain news item that is actually of high interest to her, her legal right to receive information could be affected. However, a faulty recommendation is a relatively modest effect compared to the effects Article 22 intends to cover.

News personalization could have a serious impactful legal effect on the right to receive information of news consumers if it leads to online filter bubbles or echo chambers. The existence of filter bubbles or echo chambers in the online information sphere are widely disputed. Nevertheless, experimental studies found that personalization technologies increase the extent to which people selectively expose themselves to political news articles that align with their own political views, and decreases their exposure to contrasting political viewpoints. Research also indicates that while on

---

140 De Terwangne (n 132) 21.
141 Art 22(1) GDPR.
142 Following the Article 29 Working Party, we see the ‘right’ not to be subject to automated decision-making as a prohibition for organisations, rather than a right that people should exercise; see Article 29 Working Party, ‘Guidelines on consent’ (n 83) 19–20.
145 Ibid.
149 Frederik J Zuiderveen Borgesius and others, ‘Should We Worry about Filter Bubbles?’ (2016) 5(1) Internet Policy Review. See for an extensive and more recent overview of other studies rejecting filter bubble-fears: Pablo Barbera and others, ‘Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature’ (Hewlett Foundation 2018), 16 and 53.
150 Dylko and others (n 20); Ivan Dylko and others, ‘Impact of Customizability Technology on Political Polarization’ (2018) 15(1) Journal of Information Technology & Politics 19. The amount that people exposed themselves to news articles was measured with the number of clicks on articles and the time spent reading those articles. The 2018 study by Dylko and others confirms their earlier findings and shows that user-driven personalization weakens the relationship between system-driven personalization and political selective exposure, that is, decreases some of the filter bubble-like effects. This study thus provides an
average people are not in filter bubbles, certain groups of individuals might be more susceptible to homogeneous news diets.\textsuperscript{151} Under such conditions, news personalization could severely impact people’s right to receive information from diverse sources and perspectives.

If news personalization does not produce real legal effects, it could still similarly significantly affect news consumers. The GDPR does not give a standard for a similarly significantly effect, but the recitals give as an example automatic refusal of an online credit application or e-recruiting practices without any human intervention.\textsuperscript{152} The Article 29 Working Party added that for data processing to significantly affect someone, the effects must be sufficiently great or important to be worthy of attention.\textsuperscript{153} That is to say, the decision must have the potential to significantly affect the circumstances, behaviour, or choices of the people concerned; have a prolonged or permanent impact on the data subject; or lead to the exclusion or discrimination of people.\textsuperscript{154} From this perspective, personalization could significantly affect people if, for example, it leads to certain groups being excluded from the democratic process because they are profiled as people who are uninterested in political news. However, it is not clear if such impacts on democratic inclusion would be prolonged or permanent or just temporary; this will require longitudinal studies into the effects of news personalization. News organizations will initially decide which effects are significant, yet data protection authorities and eventually the court supervise their findings.

Our assessment shows that the application of Article 22 GDPR to news personalization is limited. Other conditions in this provision further limit its application. First of all, the right not to be subject to automated decision-making does not apply if the personalization is necessary for the performance of a news subscription, is based on Union or Member State law, or is not, based on news consumers’ explicit consent.\textsuperscript{155} According to the Article 29 Working Party, the term ‘explicit’ refers to the way data subjects express their consent. The Working Party suggests that in the online context, people may give explicit consent by typing in a statement in an electronic form, sending an email, signing electronically, or using two stage verification, in which people first click ‘agree’ and then receive a verification code per email or text message to confirm the agreement.\textsuperscript{156} Normal consent requires only a clear affirmative act such as ticking a box when visiting an internet website or adjusting settings in a browser.\textsuperscript{157} News organizations could thus avoid the application of Article 22 GDPR by asking for explicit consent. However, obtaining explicit consent is laborious and requires a more complex user interface and interactions than normal consent.\textsuperscript{158}

Furthermore, the criterion of ‘solely’ in Article 22 means that the right not to be subject to automated decision-making does not apply if there is meaningful human oversight of the personalization.\textsuperscript{159} However, news personalization will generally involve large groups of news consumers, so it is unrealistic to expect that news organizations can hire editors who oversee every decision to recommend someone a particular news item. At the very best, journalists, editors, or developers can monitor the overall workings of the recommender system.

News consumers may have the right not to be subject to a personalization decision, if the personalization is based on consent, is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or if it is necessary for the purposes of the legitimate interests pursued by the controller or a third party.\textsuperscript{160}

In conclusion, the right not to be subject to automated decision-making could mean that news organizations are prohibited, in limited circumstances, from using personalization. News organizations will need to assess whether they qualify for one of the exceptions to the right, and if not, they need to ensure that news personalization has no legal or similarly significant effects on news consumers. This will require news organizations to check that people do not end up in filter bubbles or miss out on information they need to make informed political decisions, engage with issues they

\begin{itemize}
  \item \textsuperscript{151} Balázs Bodó and others, ‘Interested in Diversity: The Role of User Attitudes, Algorithmic Feedback Loops, and Policy in News Personalization’ (2019) 7(2) Digital Journalism 206.
  \item \textsuperscript{152} Recital 71 GDPR.
  \item \textsuperscript{153} Article 29 Working Party, ‘Guidelines on Automated individual decision-making’ (n 143) 21.
  \item \textsuperscript{154} Ibid.
  \item \textsuperscript{155} Art 22(2) GDPR. Note that these three exceptions resemble three of the legal grounds that legitimize personal data processing, yet they are not exactly the same, so one cannot say that only in the case of the other three legal grounds, people have a right not to be subject to automated decision-making.
  \item \textsuperscript{156} Article 29 Working Party, ‘Guidelines on consent’ (n 83) 18–19.
  \item \textsuperscript{157} Art 4(11) and Recital 32 GDPR.
  \item \textsuperscript{158} Federico Ferretti, ‘Not-So-Big and Big Credit Data Between Traditional Consumer Finance, FinTechs, and the Banking Union: Old and New Challenges in an Enduring EU Policy and Legal Conundrum’ (2018) 18(1) Global Jurist 1, at 27.
  \item \textsuperscript{159} Article 29 Working Party, ‘Guidelines on Automated individual decision-making’ (n 143) 21.
  \item \textsuperscript{160} Art 22(a) and (b) GDPR.
\end{itemize}
personally find important, or develop into the person they want to be.

**Amending your profile**

In this section, we set out the bundle of rights that effectively gives people a right to amend their personal profiles on which the news personalization is based. Such a right embodies the right to informational self-determination: the right of every individual to be in control of the image of himself which he projects upon society. The right to amend your personal profile consists of a right to rectify, erase, and restrict the processing of data.

... By rectifying data

News consumers have the right to obtain from the news organizations the rectification of inaccurate personal data and to have incomplete personal data completed. The criterion of ‘inaccurate’ refers to the accuracy principle: personal data should be accurate and kept up to date. The right to rectify data is mirrored in the obligation for news organizations to take every reasonable step to ensure that personal data that are inaccurate are erased or rectified without delay. When someone contests the accuracy of her personal data and the controller is still busy verifying if the data are accurate, this person has the right to already obtain restriction of processing.

For the right to rectify (and the right to erasure as discussed in the next subsection), we distinguish three types of personal data: data submitted by news consumers themselves, for example by filling in their name, address, and age, or by ticking boxes for topics or sources that they are interested in; data observed by the controller, such as website usage and search activities; and inferred data, which is data that the controller infers from submitted and observed data, such as what someone’s interests (probably) are.

The right to rectify data applies to submitted, observed, and inferred data. The Article 29 Working Party has stated that people may challenge the accuracy of the data used and any grouping or category that has been applied to them. The rights to rectification and erasure apply to both the “input personal data” (the personal data used to create the profile) and the “output data” (the profile itself or “score” assigned to the person). Where the Working Party refers to ‘personal data used to create the profile’ this should include submitted and observed data, since the GDPR states someone has a right to rectify ‘personal data concerning him or her’.

By rectifying inferred data, news consumers may thus change the profile on which the news recommendations for them are based. This is important since someone’s profile determines the quality of the news recommendations she receives. Furthermore, as noted before, news consumers may express anxiety about the idea there is a profile of them somewhere online, regardless of how these kinds of data are used. If people can exercise some control over their profile this might relieve some of their worries. The right to have incomplete personal data completed is important because algorithms only process the bits of personal data that it can read, that are legible to it. These pieces of data stand in for actual users, while personal characteristics that are less legible are neglected or roughly approximated. Through their right to have personal data completed, news consumers can add information about less algorithmically legible characteristics and improve the quality of the recommendations they receive. The right to rectification thus enables people to engage and tinker with the personalization process, instead of just stopping personalization when they feel uncomfortable with the profile that is being created of them.

An open question is whether people have a right to rectify just objectively or also subjectively inaccurate data. For example, is someone entitled to only rectify her age or geolocation in her profile when these are

---


162 Art 16 GDPR.

163 Art 5(1)(d) GDPR.

164 Ibid.

165 Art 18(1)(a) GDPR.

166 The World Economic Forum distinguished volunteered, observed, and inferred data; World Economic Forum, ‘Personal Data: The Emergence of a New Asset Class’ (World Economic Forum 2011), 7. The Article 29 Working Party distinguishes data provided (which includes observed data) and inferred and derived data; Article 29 Working Party, ‘Guidelines on the right to data portability’ (WP 242 rev.01, 5 April 2017), 9–10. For another taxonomy, see Gianclaudio Malgeri, ‘Property and (Intellectual) Ownership of Consumers’ Information: A New Taxonomy for Personal Data’ [2016] 4 Privacy in Germany – PinG, 133. We could also add acquired data, which is data that organizations obtain via data brokers or other organizations.


168 Monzer and others (n 9).


incorrect, or is she allowed to also rectify a personal characteristic such as ‘prefers sensational local news’ if she aspires to be a different kind of news consumer? The Article 29 Working Party found that ‘accurate’ means accurate as to a matter of fact, which suggests that the Working Party holds that only objectively inaccurate facts may be rectified. However, the Working Party developed this notion of accuracy in the context of delisting or erasing search results. In that case, a narrow reading of ‘inaccurate’ is justified because it minimizes the implications of the removal of information for other fundamental rights, such as the right to freedom of expression and information of other internet users. In the context of personal profiles for news personalization, there are no such risks to other people’s rights when people would be allowed to also rectify subjectively inaccurate data.

... By erasing data

Instead of rectifying personal data, news consumers may also obtain from a news organization the erasure of personal data concerning them (‘right to be forgotten’), in the following situations: the personal data are no longer necessary for the personalization or have been unlawfully processed; the news consumer withdraws consent and there are no other legal grounds for the processing or she objects to the processing pursuant to Article 21(1); the news organization is legally obliged to erase the data; or the personal data have been collected when the news consumer was still a child. The right to erase personal data gives people control over their profile on which personalization is based, because it enables them to start afresh and to reset their profile.

When a news consumer objects to processing that is based on the public task- or legitimate interest-ground and then requests erasure, the news organization should grant the erasure if ‘there are no overriding legitimate grounds for the processing’. A news organization could try to argue, for example, that the personal data concerned are needed to maintain the algorithmically created model for news recommendations, which is also used to provide relevant recommendations to other news consumers who are similar to the person that makes the request. In such a case, the right to erasure requires that news organizations balance the various interests at stake, while taking into account the particular situation of the news consumer (and not just the interest of the data subjects involved as an undefined group). However, it is hard to see how someone’s data protection interests could be outweighed by the interest of the news provider to keep its recommender models intact, or the interest of other news consumers to receive relevant recommendations.

The right to erasure is not applicable when the processing of personal data is necessary for, among others, exercising the right to freedom of expression and information. The reference to freedom of expression in this provision is broader than the reference to freedom of expression in the journalism provision of Article 85(2) GDPR. The journalism provision provides an arrangement for freedom of expression by journalists, academics, artists, or literary authors, whereas the right to erasure contains an arrangement for freedom of expression in general—not just freedom of expression as exercised by a specific group of people. Nevertheless, in the context of this article, the right to erasure has to be balanced just with the right to freedom of expression of news media. We are interested in personal data in personalization profiles, not personal data in news stories. Erasing data from a personalization profile could limit only how news media can express themselves by providing personalized recommendations.

It is thus the question, like in the context of the journalism provision, if news personalization is necessary for exercising the right to freedom of expression and information of news organizations. We argued in the ‘Journalism provision’ section that news organizations can produce and publish news without being able to disseminate it in a personalized manner. In line with that, we argue that the right to erasure applies to personal data processed in the context of news personalization as usual.

In addition to that, the right to erasure does not apply when the processing of personal data is necessary for the performance of a task carried out in the public

---

172 Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgement on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12 WP 225, 26 November 2014, 15.
173 Art 17(1)(a) and (d) GDPR.
174 See ‘Stopping personalization’ section.
175 Art 17(1)(c) GDPR.
176 Art 17(1)(e) GDPR.
177 Art 17(1)(d) GDPR.
178 Art 17(1)(c) in conjunction with art 21(1) and art 6(1)(e) or (f) GDPR.
179 Google Spain (n 42) para 76. As discussed in the ‘Stopping personalization’ section, when the legislator determines certain data should be processed for a public task, or when an organisation decides to legitimize data processing on the legitimate interest-ground, they simply consider the interests of a group of data subjects but not of each individual data subject.
180 Art 17(3)(a) GDPR.
181 With thanks to an anonymous reviewer for pointing this out.
182 Unless me cutting down my profile also effects your profile by the way our nodes are connected—a circumstance too complicated to consider in this article.
interest. In that case, Union law or Member State law should lay down the basis for the processing and this law should be proportionate to the public interest pursued (see section ‘Stopping personalisation’). If public service media personalize news in the performance of their public task, people might thus not have a right to erasure. This is an unsatisfying conclusion from the perspective of individual rights protection.

When a controller has made personal data public and is obliged to erase some of it, it should inform other controllers that are also processing these data that the data subject has requested the erasure of any links to, or copy or replication of the data. This obligation is relevant for news personalization because news media might share data and algorithmic models. For example, in Germany and the UK, publishers are pooling personal data in platforms for targeted advertising and single log-in procedures. Similar data pooling initiatives could arise for news personalization, especially if these data pools can help online publishers to counter the dominance of major social network services and search engines, who have better access to user data. People whose personal data ends up in one of such data pools should be able to erase their data by filing a request to one news provider, after which the provider should inform other partners in the data pool that the data should be erased.

Many scholars and commentators are critical of the right to be forgotten because it could lead to private censorship. However, in the personalized news context, there is no risk that the right to erasure becomes a tool of private censorship. There is a difference between data that was communicated to the public in a news story or hyperlink and data that is stored in the back-end systems of organizations, including inferred data. The erasure of public data might be critiqued from a freedom of expression and information perspective. In contrast, the erasure of back-end data rightfully enables people to control how they are represented in systems that are used to make decisions about or for them.

As already stated earlier in this section, a set of guidelines from the Article 29 Working Party indicates that people can exercise a right to erasure over submitted, observed, and inferred data.

Moving your profile

Finally, when the processing of personal data for news personalization is based on consent or a contract, news consumers have the right to receive the personal data concerning them and to transmit those data to another news organization without hindrance from the news organization to which they initially provided the data (‘right to data portability’). People also have the right to have their personal data transmitted directly from one news organization to another, at least where technically feasible. In the latter case, people just instruct an organization to pass the data on to another organization. When people exercise their right to data portability, they may exercise their right to erasure at the same time, but they do not need to do so. Therefore, a news organization does not automatically need to delete the data from its own systems when people port their data to another service.

The right to data portability covers data which someone ‘has provided to a controller’, that is, submitted data such as name, address, or stated interests. According to the Article 29 Working Party, provided data includes observed data, such as activity logs, website usage, and search activities. The Article 29 Working Party reasons that people ‘provide’ such data by virtue of their use of the service or device.

183 Art 17(3) GDPR. There are more circumstances when the right to erasure does not apply, but these are not relevant in the context of news personalisation.
184 Art 6(3) GDPR.
185 Art 17(2) GDPR.
189 Art 20(1) GDPR.
190 Art 20(2) GDPR. It is not stated what is the standard for ‘technical feasibility’.
191 Art 20(3) GDPR.
192 Art 20(1) GDPR.
194 Ibid 9.
right to data portability excludes inferred data, such as personal interests deduced from other data. 195

Some commentators see the right to data portability as a tool to prevent lock-in effects and increase competition among online services. 196 When people can download their data and conveniently import these into another service, they can more easily switch to a better service. The Article 29 Working Party nevertheless stresses that while the right to data portability may enhance competition, it is most importantly a data protection right that supports user choice, control, and empowerment. 197 For personalized news consumers, the right to data portability would be useful if it would enable them to switch to another news service and receive relevant recommendations immediately when starting to use the new service (on the basis of their old profile). However, as just discussed, the right to data portability covers only submitted and observed data, whereas most personalization happens on the basis of inferred data. The right to data portability will thus be useful only for user-driven personalization but not for system-driven personalization.

People have the right to receive their data in a structured, commonly used and machine-readable format. 198 Nevertheless, data controllers are only encouraged but not obliged to develop actual interoperable formats that enable data portability. 199 Furthermore, the right to data portability does not create an obligation for organizations to build processing systems which are technically compatible. 200 Experience in the telecoms sector with number portability suggests that the right to have personal data transmitted directly from one news organization to another might be difficult to enforce without an obligation to create interoperable formats or technically compatible systems. If news service providers do not have such obligations, and need to ensure interoperability only where technically feasible, they could avoid compliance by not developing technical standards in cooperation with other service providers. 201 This is a missed opportunity for improving news recommendations, since interoperable news user profiles could solve the problem of providing relevant recommendations to novel users for whom the system has not yet registered any preferences (the so-called ‘cold start problem’).

The right to data portability does not apply when personalization is based on a legal ground other than consent or contract. 202 Thus, when news personalization is necessary for the performance of a task carried out in the public interest, such as when public service media personalize the news, or when it is necessary for the legitimate interests of the news organization or a third party, people cannot download their data or transfer their profiles.

Conclusion

People increasingly receive a daily news selection that is specifically shaped to their interests and preferences, via among others personalized news websites, mobile apps, and social media. News personalization relies on the large-scale collection and processing of personal data of news consumers. The personal data are used to profile people and to infer or predict which news stories are relevant to them. People are worried about the processing of their personal data for personalization, while they also appreciate how personalization can improve their news experience.

In this article, we first asked if the journalism provision in the GDPR applies to news personalization. With the use of three different legal interpretation techniques (textual, historical, and functional), we concluded that the journalism provision does not apply to news personalization. The main reason is that the journalism provision aims to enable the use of personal data in news stories, but not the use of personal data to disseminate news. News media should be free to produce and publish the news they deem important, and the journalism provision guarantees this freedom to the extent that news stories contain personal data of the people concerned in the reported event. The GDPR consequently conditions how the media may bring these stories to their readers in case they do so in a personalized manner.

Secondly, we asked how the GDPR provides news consumers control over the processing of their personal data.
for news personalization. We showed that through exercising their data protection rights, people can either stop personalization or prevent it from beginning at all, or they can change their personal profile on which the personalization is based. Furthermore, from the application of the GDPR it follows that news organizations should provide personalized and non-personalized services of a similar orientation and quality, or that at least the entire online news market should cater for such choices. The various rights that enable people to change their personal profile could be translated into a right to reset: people have the right to keep their news service account, but they should be able to remove all the observed personal data from their profile, so that they can start afresh.

Besides complying with the GDPR, news organizations can do more to develop privacy-friendly services—supposing that they want to, since many online media have repeatedly stated that they care about the privacy of their users. For example, Kobsa has suggested various privacy-enhancing technologies (‘PETs’) for personalization, including client-side personalization, where personal data is stored and processed at the user side rather than the server side, and collaborative filtering with distributed rather than central repositories.203 This study has not dealt with special categories of personal data (‘sensitive data’) in the context of news personalization. Sensitive data are personal data revealing, among others, racial or ethnic origin, political opinions, religious or philosophical beliefs, or data concerning someone’s sexual orientation.204 According to the Article 29 Working Party, this prohibition includes ‘not only data which by its nature contains sensitive information (…), but also data from which sensitive information with regard to an individual can be concluded’.205 Data that serves as a proxy for sensitive data are thus to be treated as sensitive data. It is an open question to what extent the data that people disclose by their news use, such as data that they are interested in certain political or cultural topics, also reveal things such as their political beliefs or racial identity. If one argues that all or much of the personal data processed for news personalization is sensitive data, then the analysis under the GDPR changes and will be much more focused on explicit consent—one of the legal grounds to legitimize the processing of sensitive data.206

The analysis on the right not to be subject to automated individual decision-making will also change,207 and a data protection impact assessment might be required.208 Since the regime for the processing of sensitive data raises many more questions with regard to news personalization, more research is needed on this topic.

That said, providing people control over their personal data through consent or explicit consent might be of lesser importance in the context of news personalization. As Edwards and Veale argue with Hildebrandt, in the digital environment, ‘what we increasingly want is not a right not to be profiled—which means effectively excluding ourselves from society and its benefits—but to determine how we are profiled and on the basis of what data—a “right how to be read”’.209 Similarly, we argue that in the case of news personalization, seeing that many people are actually open to such services, the most important function of the GDPR is to enable people to control how their news interests and preferences are registered in the system and how they are perceived online by the various recommender systems. The GDPR is not opposed to news personalization and if news organizations consider the GDPR while designing their systems, the legal norms can help them to develop privacy-friendly news services.

204 Art 9 GDPR.
206 Art 9(2)(a) GDPR.
207 Art 22(4) GDPR.
208 Art 35(3)(b) GDPR.