A Matter of (Joint) control? Virtual assistants and the general data protection regulation

van Mil, J.; Quintais, J.P.

DOI
10.1016/j.clsr.2022.105689
Publication date
2022
Document Version
Final published version
Published in
Computer Law & Security Review

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

A Matter of (Joint) control? Virtual assistants and the general data protection regulation

Jurriaan van Mil[†], *João Pedro Quintais*[†,*]

Institute for Information Law (IViR), University of Amsterdam the Netherlands

ARTICLE INFO

Keywords:
General data protection regulation
Controller
Joint controller
Household exception
Virtual assistant
Google assistant

ABSTRACT

This article provides an overview and critical examination of the rules for determining who qualifies as controller or joint controller under the General Data Protection Regulation. Using Google Assistant – an artificial intelligence-driven virtual assistant – as a case study, we argue that these rules are overreaching and difficult to apply in the present-day information society and Internet of Things environments. First, as a consequence of recent developments in case law and supervisory guidance, these rules lead to a complex and ambiguous test to determine (joint) control. Second, due to advances in technological applications and business models, it is increasingly challenging to apply such rules to contemporary processing operations. In particular, as illustrated by the Google Assistant, individuals will likely be qualified as joint controllers, together with Google and also third-party developers, for at least the collection and possible transmission of other individuals' personal data via the virtual assistant. Third, we identify follow-on issues relating to the apportionment of responsibilities between joint controllers and the effective and complete protection of data subjects. We conclude by questioning whether the framework for determining who qualifies as controller or joint controller is future-proof and normatively desirable.

1. Introduction

Virtual voice assistants have been on the rise ever since Apple popularised the technology when it brought Siri to the iPhone in October 2011.[1] The technology appears to be here to stay. Since Siri, end-users have been introduced to Microsoft's Cor-

* Corresponding author.
E-mail address: j.p.quintais@uva.nl (J.P. Quintais).

† The authors contributed equally to this article. The authors wish to thank Thomas Poell, Theo Araujo and te anonymous reviewers for their valuable comments. All errors remain ours.

[1] Natalie Harrison and Teresa Brewer, 'Apple Launches iPhone 4S, iOS 5 & iCloud' (*Apple*, 4 October 2011) <https://www.apple.com/newsroom/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud/> accessed 2 February 2022. Developers have been working on voice-controlled computing devices for decades, and the technology can be traced back to, for example, the invention of IBM's Shoebox calculator in 1961. See IBM, 'IBM Shoebox' (*IBM*) <https://www.ibm.com/ibm/history/exhibits/specialprod1/specialprod1_7.html> accessed 2 February 2022.

https://doi.org/10.1016/j.clsr.2022.105689

tana,[2] Amazon's Alexa,[3] and Google Assistant,[4] to name but a few examples. The number of digital voice assistants in use across the globe has been projected to grow from approximately 3.25 billion in 2019 to 8 billion in 2023.[5] This spectacular growth could redefine how individuals interact with computational devices: from a graphical user interface in combination with a touchscreen to an AI-powered conversational user interface. In their marketing materials, developers frame their virtual assistants as a step towards making computing more intuitive, as they can mimic human language and reasoning capabilities.

Nonetheless, virtual assistants could pose serious risks to the protection of privacy and personal data, as recognised in the General Data Protection Regulation[6] ("GDPR" or "Regulation"). Throughout the years, many accounts have emerged to this effect. For instance, multiple journalists exposed that Amazon, Apple, and Google had contractors manually review (confidential) audio, recorded by their virtual assistants, for quality control purposes without end-users' knowledge.[7] Naturally, this sparked the interest of supervisory authorities across the European Union ("EU").[8] In another instance, security researchers have shown that nefarious actors can use lasers to hack into certain virtual assistants from distances as far as one hundred meters.[9] Other security researchers have identified more than 1.000 words that trigger voice assistants in smart speakers incorrectly, which can result in the erroneous and surreptitious recording and processing of private conversations.[10] Against that backdrop, it should not come as a surprise that in 2021 the European Data Protection Board ("EDPB") published released guidelines on virtual voice assistants, in which it identifies compliance challenges and makes remediating recommendations.[11]

These incidents raise the fundamental question of which actors involved in the operation of a virtual assistant should be considered (joint) controllers under the GDPR? The GDPR allocates responsibility to (joint) controllers and processors,[12] whereas it awards rights to data subjects.[13] It is therefore crucial to ascertain which actors qualify as (joint) controllers and processors in a given context, as they have responsibilities towards data subjects. In turn, data subjects can enforce their rights against (joint) controllers and processors.

This article provides an overview and critical examination of the rules for determining (joint) controllership in the context of virtual assistants, looking through the particular lens of Google Assistant. We carry out doctrinal legal analysis to explore the application of joint controllership rules to virtual

[2] Microsoft News Center, 'Microsoft showcases latest updates to Windows, opportunities for developers' (*Microsoft News Center*, 2 April 2014) <https://news.microsoft.com/2014/04/02/microsoft-showcases-latest-updates-to-windows-opportunities-for-developers/> accessed 2 February 2022. Cortana is set to disappear on Android and iOS devices as part of Microsoft's broader vision to incorporate conversational computing in all of its platforms and devices. See Tom Warren, 'Microsoft is killing off its Cortana app for iOS and Android in January' (*The Verge*, 16 November 2019) <https://www.theverge.com/2019/11/16/20967875/microsoft-cortana-ios-android-app-removal-countries-support-document> accessed 2 February 2022.

[3] Darrell Etherington, 'Amazon Echo Is A $199 Connected Speaker Packing An Always-On Siri-Style Assistant' (*TechCrunch*, 6 November 2014) <https://techcrunch.com/2014/11/06/amazon-echo/> accessed 2 February 2022.

[4] Sundar Pichai, 'A personal Google, just for you' (*Google*, 4 October 2016) <https://www.blog.google/products/assistant/personal-google-just-you/> accessed 2 February 2022.

[5] Statista, 'Number of Voice Assistants in Use Worldwide 2019-2023 | Statista' (2020) <https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/> accessed 2 February 2022.

[6] 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 [2016] OJ L119/1.

[7] Matt Day, Giles Turner and Natalia Drozdiak, 'Amazon Workers Are Listening to What You Tell Alexa' (*Bloomberg*, 11 April 2019) <https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio> accessed 2 February 2022; Lente Van Hee, Denny Baert, Tim Verheyden and Ruben Van Den Heuvel, "Google employees are eavesdropping, even in your living room, VRT NWS has discovered" (*VRT NWS*, 10 July 2019) <https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping-even-in-flemish-living-rooms/> accessed 2 February 2022; Alex Hern, 'Apple contractors 'regularly hear confidential details' on Siri recordings' (*The Guardian*, 26 July 2019) <https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings> accessed 2 February 2022; Joseph Cox, 'Revealed: Microsoft Contractors Are Listening to Some Skype Calls' (*Motherbroad*, 7 August 2019) <https://www.vice.com/en_us/article/xweqbq/microsoft-contractors-listen-to-skype-calls> accessed 2 February 2022.

[8] Hamburg Commissioner for Data Protection and Freedom of Information, 'Automatic speech assistant systems - Implementation of data protection measures by Google and other providers required' (2019) <https://datenschutz-hamburg.de/assets/pdf/2019-08-26_press-release_Google-speech-assistant-systems.pdf> accessed 10 July 2020; Leo Kelion, 'Amazon Alexa: Luxembourg watchdog in discussions about recordings' (*BBC*, 6 August 2019) <https://www.bbc.com/news/technology-49252503> accessed 2 February 2022; Data Protection Commission, 'The DPC's take on digital assistants' (*Data Protection Commission*, 2 December 2019) <https://www.dataprotection.ie/en/news-media/blogs/dpcs-take-digital-assistants> accessed 2 February 2022.

[9] Takeshi Sugawara and others, 'Light Commands: {Laser-Based} Audio Injection Attacks on {Voice-Controllable} Systems' (2020) <https://www.usenix.org/conference/usenixsecurity20/presentation/sugawara> accessed 2 February 2022.

[10] Lea Schönherr, Maximilian Golla, Jan Wiele, Thorsten Eisenhofer, Dorothea Kolossa and Thorsten Holz, 'Unacceptable, where is my privacy? Exploring Accidental Triggers of Smart Speakers' (*GitHub*, 1 July 2020) <https://unacceptable-privacy.github.io> accessed 2 February 2022.

[11] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (European Data Protection Board (EDPB) 2021) Guidelines <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022021-virtual-voice-assistants_en> accessed 2 February 2022.

[12] Articles 4(7) and 4(8) GDPR. A controller is the entity that, alone or jointly with others, determines the purposes and means of the processing of personal data; a processor is the entity that processes personal data on behalf of a controller. See section 4.

[13] Article 4(1) GDPR. A data subject is an identified or identifiable natural person to whom personal data relates. See section 3.1.1.

assistants. This focus means that beyond what is necessary for the purposes of our analysis, we do not examine other important issues at the intersection of data protection and virtual assistants, such as data minimization, accountability, data protection by design and by default, and mechanisms to exercise data subject rights.[14] The analysis proceeds as follows. Section 2 offers a conceptual primer on how virtual assistants in general and the Google Assistant in particular operate, focussing on the technologies developers incorporate in their virtual assistants and the interaction between end-users and virtual assistants. Section 3 critically examines the GDPR's rules on (joint) controllership. Section 4 then builds on this analysis and develops scenarios to discuss how the GDPR applies to Google Assistant, as a concrete example of a virtual assistant. Section 5 then discusses the apportionment of responsibilities between joint controllers in the context of virtual assistants as well as the effective and complete protection of data subjects. Section 6 offers tentative recommendations based on our findings.

2. What are virtual assistants?

This section a baseline understanding of the technology through conceptual primer on how virtual assistants in general and the Google Assistant in particular operate. We do not aim to provide a detailed account of the technology, since the workings of virtual assistants are often complex and obfuscated.[15] Rather, we conceptualise features and functionalities that are relevant from a legal perspective.[16]

2.1. *Virtual assistants in general*

Even though differences exist between Apple's Siri, Microsoft's Cortana, Amazon's Alexa and Google Assistant, virtual assistants share key features and functionalities. The EDPB defines "virtual voice assistants" as a "service that understands voice commands and executes them or mediates with other IT systems if needed", adding that they "are currently available on most smartphones and tablets, traditional computers, and, in the latest years, even standalone devices like smart speakers".[17] For our purposes, we consider virtual assistants as a type of "conversational agent" typically controlled by voice and used by end-users to carry out personal or private tasks. In turn, conversational agents are "software that accepts natural language as input and generates natural language as output, engaging in a conversation with the user".[18] To successfully manage interaction with end-users, conversational agents usually integrate different types of technologies: automatic speech recognition,[19] natural language understanding,[20] dialogue management, natural language generation,[21] and text-to-speech synthesis.[22] [23] From a technological perspective, virtual assistants can be seen as a pipeline of different software components, some of which include artificial intelligence systems.[24]

Virtual assistants are incorporated into a plethora of end-user products, such as smartphones, smart home devices,[25]

[14] These topics are addressed for instance in European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11).

[15] Simone Natale, 'To Believe in Siri: A Critical Analysis of AI Voice Assistants' 17; Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' 31 50.

[16] For a more detailed technical analysis following a similar approach, see European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 8–12, 37–39.

[17] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 3.

[18] David Griol, Javier Carbó and JoséM Molina, 'An Automatic Dialog Simulation Technique to Develop and Evaluate Interactive Conversational Agents' (2013) 27 Applied Artificial Intelligence 759.

[19] DeepAI has defined automatic speech recognition as "a subfield of computational linguistics that is concerned with recognition and translation of spoken language into text by computers". See DeepAI, 'Automatic Speech Recognition' (*DeepAI*) <https://deepai.org/machine-learning-glossary-and-terms/automatic-speech-recognition> accessed 2 February 2022.

[20] Techopedia has defined natural language understanding as "a unique category of natural language processing that involves modeling human reading comprehension or in other words, parses and translates input according to natural language principles". See Techopedia, 'Natural Language Understanding (NLU)' (*Techopedia*) <https://www.techopedia.com/definition/33013/natural-language-understanding-nlu> accessed 2 February 2022. Similarly, Google has defined natural language understanding as "[the] The capability of software to understand and parse user input". See Google, 'Actions on Google glossary' (*Google*, 20 May 2020) <https://developers.google.com/assistant/conversational/df-asdk/glossary> accessed 2 February 2022.

[21] Techopedia has defined natural language generation as a particular artificial intelligence-complete task "that involves generating language from non-language inputs". See Techopedia, 'Natural Language Generation (NLG)' (*Techopedia*) <https://www.techopedia.com/definition/33012/natural-language-generation-nlg> accessed 2 February 2022.

[22] Techopedia has defined text-to-speech (synthesis) as "a natural language modelling process that requires changing units of text into units of speech for audio presentation". See Techopedia, 'Text to Speech (TTS)' (*Techopedia*) <https://www.techopedia.com/definition/23843/text-to-speech-tts> accessed 2 February 2022.

[23] Griol, Carbo and Molina (n 18) 760.

[24] The Commission Proposal for an AI Act defines an AI system as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate output such as content, predictions, recommendations, or decisions influencing the environments they interact with". See Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts COM/2021/206 final, art. 3(1). Annex I lists various techniques and approaches, including: (a) different types of machine learning (supervised, unsupervised and reinforcement) using a variety of different methods (e.g. deep learning); (b) logic- and knowledge-based approaches; and (c) statistical approaches. See ibid. Annex I and Art. 3(2) AI Act proposal.

[25] Google has reported that over 30.000 smart home devices from more than 3.500 popular brands have been compatible with the Google Assistant since May 2019. See Manuel Bronstein, 'Bringing you the next-generation Google Assistant' (*Google*, 7

wearables, and cars.[26] Therefore, they are characterized by a significant degree of device-embeddedness. Furthermore, virtual assistants are predominantly designed and developed to assist end-users in the performance of tasks in the private sphere. For example, virtual assistants incorporate an increasing number of functionalities[27]: end-users can call on assistants to place orders over the internet (e.g., Postmates), to stream music and videos (e.g. Spotify and Netflix), to conduct search queries (e.g. Google Search), and turn on smart lights (e.g. Philips Hue). Even though we are only interested in the use of virtual assistants in the private sphere, it is important to note that they are increasingly used in public and commercial contexts as well.[28] These latter applications are however outside the scope of this article.

2.2. *Google assistant in particular*

Building on the foregoing considerations, we shift our focus to the operation of Google Assistant. As a preliminary step, an end-user needs to ensure that the Google Assistant application is installed on their compatible (third-party) device before they can start operating it. With respect to smartphones, recent versions of Google's operating system, Android, come with Google Assistant pre-installed.[29] End-users that use an iPhone or an older version of Android need to download and install the Google Assistant application via Apple's App Store[30] and Google Play,[31] respectively. With respect to smart home devices, Google Assistant is being increasingly incorporated into numerous devices, such as speakers manufactured by Bose[32] and Sonos.[33]

Furthermore, our end-user needs to sign in with a Google Account in the Google Assistant application. In simple terms, Google prompts end-users during the registration process to provide a selection of (personal) data, including name and gender, and to consent to its terms of service,[34] consolidated privacy policy,[35] and some specific processing operations like pushing personal advertisements. Google again prompts end-users to authorise some specific processing operations like service personalisation when signing in with their Google Account in the Google Assistant application.

Finally, our end-user can start operating Google Assistant. For our purposes, it is instructive to distinguish the following three stages of processing operations: (1) the collection of data, (2) the processing of data, and (3) the transfer of data. We discuss these stages below.

2.2.1. *Stage 1: the collection of data*

Firstly, our end-user needs to activate Google Assistant, which is on perpetual standby mode, by uttering one of the following two *trigger phrases* or "wake-up expressions"[36] in English: "Hey Google" or "Ok Google". Google deploys automatic speech recognition software to detect whether someone called upon the virtual assistant.[37] After one of the two trigger phrases, our end-user needs to utter an *invocation*, which provides the virtual assistant with input about what kind of assistance is needed. Our end-user can request search queries (e.g. Google Search) or trigger a selection of native (e.g. Google Maps) as well as third-party (e.g. Spotify) functionalities. Google calls

May 2019) <https://www.blog.google/products/assistant/next-generation-google-assistant-io/> accessed 2 February 2022; Chris Turkstra, 'The Google Assistant comes to more devices at home' (*Google*, 5 September 2019) <https://www.blog.google/products/assistant/google-assistant-comes-more-devices-home/> accessed 2 February 2022.

[26] Hyundai owners can use an Action, Blue Link, to set the desired cabin temperature, and to remotely lock and unlock their vehicle, among other things. See Google, 'Blue Link' (*Google*) <https://assistant.google.com/services/a/uid/000000970a7506be?hl=en-IE> accessed 2 February 2022.

[27] Google has highlighted that over one million functionalities were accessible via the Google Assistant in July 2020. See Google, 'What can your Assistant do?' (*Google*) <https://assistant.google.com/explore?hl=en_us> accessed 29 May 2020. It is important to note that Google has only been doing so on the American version of the discovery website of the Google Assistant, whereas it has been silent on the number of accessible functionalities on the Irish counterpart. Compare Google, 'What can your Assistant do?' (Google) <https://assistant.google.com/explore?hl=en-ie> accessed 2 February 2022.

[28] For example, the operator of John F. Kennedy International Airport uses the "interpreter mode" of the Google Assistant to help international passengers. See Lilian Rincon, 'Interpreter mode expands globally to airports, banks and more' (*Google*, 7 January 2020) <https://blog.google/products/assistant/interpreter-mode-expands-help-more-people-communicate-around-world/> accessed 2 February 2022.

[29] Google has suggested, in February 2018, that the Google Assistant application is built into the Android Go and KaiOS operating systems. See Manuel Bronstein, 'Building the Google Assistant on Phones for Everyone, Everywhere' (*Google*, 25 February 2019) <https://blog.google/products/assistant/building-google-assistant-phones-everyone-everywhere/> accessed 2 February 2022.

[30] Apple, 'Google Assistant. Your own personal Google' (*Apple*, 25 March 2020) <https://apps.apple.com/ie/app/google-assistant/id1220976145> accessed 2 February 2022.

[31] Google, 'Google Assistant - Get things done, hands-free' (Google, 9 March 2018) <https://www.play.google.com/store/apps/details?id=com.google.android.apps.googleassistant&hl=en> accessed 2 February 2022.

[32] Anurag Jain, 'Bose speakers get smarter with the Google Assistant' (*Google*, 21 May 2019) <https://www.blog.google/products/assistant/bose-speakers-get-smarter-google-assistant/> accessed 2 February 2022.

[33] Anurag Jain, 'With the Google Assistant, your Sonos system gets even smarter' (*Google*, 14 May 2019) <https://www.blog.google/products/assistant/google-assistant-your-sonos-system-gets-even-smarter/> accessed 2 February 2022.

[34] Google, 'Google Terms of Service' (*Google*) <https://policies.google.com/terms> accessed 21 July 2020.

[35] Google, 'Google Privacy Policy' (*Google*) <https://policies.google.com/privacy> accessed 16 July 2020.

[36] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 11. ("…almost all VVAs on the market are based on the detection of a wake-up expression or word to switch to active listening mode (also known as activation word or wake-up word / hot word).")

[37] Assaf Hurwitz Michaely and others, 'Keyword Spotting for Google Assistant Using Contextual Speech Recognition', *2017 IEEE Automatic Speech Recognition and Understanding Workshop (ASRU)* (2017).

such functionalities *Actions*, whereas Apple and Amazon call them *Shortcuts*[38] and *Skills*,[39] respectively.

In this context, we need to distinguish between explicit and implicit invocations. In order to invoke an Action *explicitly*, our end-user needs to follow a precise grammar consisting of a *trigger phrase* (e.g. "Hey Google, ask"), an *invocation name* (e.g. "Spotify"), and an optional *invocation phrase* (e.g. "to play 'Lost' by Frank Ocean").[40] Third-party developers need to specify one or more *invocation names* and optional *invocation phrases* for their Actions in accordance with Google's policies.[41] Alternatively, our end-user invokes an Action *implicitly* when they do not include an *invocation name* in the query (e.g. "Hey Google, play 'You Should Be Here' by Kehlani"). Google Assistant will then match the utterance to an Action on the basis of a recommendation algorithm.[42] When the end-user has a Spotify subscription, the virtual assistant can then use the service to stream the song.

2.2.2. *Stage 2: the processing of data*

Concomitantly, Google Assistant starts processing the query while our end-user continues to utter. Due to the limited computational resources incorporated in most compatible devices, the virtual assistants transmits our end-users' vocal input to Google's servers for processing.[43] But technological advances may make that Google Assistant soon increasingly or completely processes the end-user's query "locally" on-device.[44] This appears to be the expectation for most virtual voice assistants going forward.[45] Upon reception, Google uses a pipeline of software components to process the audio recordings: automatic speech recognition software transcribes speech into text, and natural language processing software transforms text into machine-readable instructions.[46] Subsequently, the explicit or implicit invocation is matched to an Action and the corresponding *intent*, which is a unique identifier that provides Google and third-party developers with input about the query.[47] Google fulfils the query directly when our end-user has invoked a search query (e.g. Google Search), a native Action (e.g. Google Maps), or a fully integrated third-party Action (e.g. Spotify). Response actions by the virtual assistant to the users' queries that consist of answer phrases are enabled by speech synthesis, i.e. the artificial production of human speech.[48]

2.2.3. *Stage 3: the transfer of data*

An important distinction applies when our end-user has invoked a partly integrated third-party Action. In that case, Google transmits the intent to the corresponding third-party developer's servers.[49] Upon reception, the third-party developer handles the request using either Google's or its own natural language understanding software. The third-party developer either directly fulfils the requests or transmits a response back to Google Assistant. For our purposes, this scenario is relevant insofar as there is a transfer of our end-user's data from Google to the third-party developer. This appears to be the case also for other virtual assistants and may include the transfer of sensitive data.[50]

3. Where does the GDPR stand on (joint) controllership?

Because the EDPB has been clear on the operation of "virtual voice assistants", involving a plurality of personal data and processing operations,[51] we brush over the preliminary

[38] Apple, 'Use Siri Shortcuts' (*Apple*, 26 May 2020) <https://www.support.apple.com/en-ie/HT209055> accessed 2 February 2022.

[39] Amazon, 'Getting started' (*Amazon*) <https://www.amazon.com/Alexa-Skills-Getting-Started-Guide/b/?ie=UTF8&node=15144553011&ref_=sv_a2s_5> 21 July 2020. It is important to note that rather than hosting an Irish version of the website for customers trying to access <http://www.amazon.ie/>, Amazon redirects those customers to the British version of the website. Compare Amazon, 'Getting started' (*Amazon*) <https://www.amazon.co.uk/b/?ie=UTF8&node=11242734031&ref_=sv_a2s_5> accessed 21 July 2020.

[40] Google, 'Explicit Invocation' (*Google*) <https://developers.google.com/assistant/discovery/explicit> accessed 2 February 2022.

[41] Google, 'Policies for Actions on Google' (*Google*) <https://developers.google.com/assistant/console/policies/general-policies#naming_directory_listing_and_promotion> accessed 2 February 2022.

[42] Google, 'Implicit invocation' (Google) <https://developers.google.com/assistant/discovery/implicit> accessed 2 February 2022.

[43] Google has compared the "future virtual assistants" to the current Google Assistant, which relies on the internet and Google's cloud environment. See Bronstein (n 29).

[44] Bronstein (n 29). Compare Khari Johson, "AI Weekly: Why Google still needs the cloud even with on-device ML" (*VentureBeat*, 18 October 2019) <https://venturebeat.com/2019/10/18/ai-weekly-why-google-still-needs-the-cloud-even-with-on-device-ml/> accessed 2 February 2022.

[45] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 10.("…while currently most voice related processing is performed in remote servers, some VVA [*virtual voice assistants*] providers are developing systems that could perform part of this processing locally")

[46] Google has identified that the Google Assistant incorporates speech transcription and language understanding models. See Bronstein (n 29).

[47] Google has defined intent as the goal or task that an end-user wants to do, which "is represented as a unique identifier and the corresponding user queries that can trigger [it]". See Google, 'Actions on Google Glossary' (n 20).

[48] For a brief explanation of automatic speech recognition, natural language processing and speech synthesis, see European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 37–39.

[49] Google, 'Actions on Google webhook formats' (*Google*) <https://developers.google.com/assistant/actions/build/json> accessed 2 February 2022.

[50] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 9. ("VVAs allow the installation of third party components or apps that expand their core functionalities. Each VVA name the components differently but all involve the exchange of users' personal data between the VVA designer and the app developer. 14. Although most VVAs do not share the voice snippet with the app developers, these actors still process personal data. Moreover, depending on the nature of the functionality provided, the app developer receives intentions and slots which could include sensitive information like health data.)

[51] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 13–14.

questions on the material[52] and territorial[53] scope, and focus on the core subject-matter of this article: (joint) controllership within the context of virtual assistants. The concept of (joint) controllership is crucial because it determines to whom the GDPR allocates the principal burden of observing compliance.[54] We describe the legal framework for determining (joint) controllership, which breaks down into the household exemption, controllership, and joint controllership. Because our aim for this section is primarily descriptive, we only deduce a taxonomy of relevant criteria from the CJEU's case law, the EDPB's guidance, and legal scholarship. Our normative reflections are carried out in the subsequent sections.

3.1. *The household exemption: undertaking a purely personal or household activity?*

Even when natural persons satisfy all conditions for qualifying as (joint) controllers, they are not automatically responsible under the GDPR. The household exemption excludes natural persons from the material scope of the Regulation, provided that they process personal data "in the course of a purely personal or household activity".[55] The preamble specifies that the processing of personal data by natural persons cannot have a connection to a professional or commercial activity. It further specifies that "correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities" could constitute a purely personal or household activity. When natural persons can successfully appeal the household exemption, the GDPR will still apply to the controllers and processors that provide them the means for the processing of personal data.[56] Because the GDPR is light on the scope of the household exemption, the CJEU's case law and the EDPB's guidance are of particular relevance.

Lindqvist[57] and *Ryneš*[58] are the first cases in which the CJEU introduced criteria for determining whether a natural person can successfully appeal the household exemption under the Data Protection Directive.[59] From these cases follows that an activity cannot be regarded as a purely personal or household activity when it: (1) makes personal data accessible to an indefinite number of people[60]; or (2) covers, even partially, a public space and is accordingly directed outwards from the private setting of the natural person processing the personal data.[61] Factual circumstances rather than domestic purposes are decisive in this regard.[62] These criteria were later reinforced in *Jehovan todistajat* and *Buivids*.[63] In the absence of additional guidance, it is unclear not only when specific cases match these criteria but also to what extent other criteria could be considered when determining the applicability of the household exemption.[64] Considering the Court's stance that the exemption must be construed narrowly,[65] one can reasonably expect that other restricting criteria could be taken into account in any case.

The EDPB has reiterated the criteria set out in *Lindqvist* and *Ryneš* in the context of the GDPR in Guidelines 3/2019.[66] Importantly, it held that an overall assessment is required to draw a conclusion on the applicability of the exemption.[67] This assessment should consider, where relevant, the personal relationship between the natural person processing personal data and the data subject, the scale or frequency of the processing, and its potential adverse impact on the data subject.[68] The guidance suggests that the CJEU's case law on the household exemption under the Data Protection Directive remains relevant under the GDPR.[69]

[52] As for its material scope, the GDPR applies to the automated processing of personal data. See Article 2 GDPR.

[53] As for its territorial scope, the GDPR applies to the processing of personal data in three specific situations: (1) when a controller has an establishment in the EU and the processing of personal data is carried out in the context of the establishment's activities; (2) when a controller is not established in the EU, but its processing operations either target data subjects in the EU or monitors their behaviour in the EU; and (3) when a controller is not established in the EU but "in a place where Member State law applies by virtue of public international law". See Article 3 GDPR.

[54] Article 5(2) GDPR.

[55] Article 2(2)(c) GDPR.

[56] Recital 18 GDPR.

[57] Case C-101/01 *Bodil Lindqvist* [2003] ECLI:EU:C:2003:596.

[58] Case C-212/13 *Ryneš* [2014] ECLI:EU:C:2014:2428.

[59] 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.

[60] *Lindqvist* (n 57) para 47-48.

[61] *Ryneš* (n 58) 33-35.

[62] Cf Jiahong Chen et al., 'Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10 International Data Privacy Law 279, 286.

[63] Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551 para 42; Case C–345/17 *Sergejs Buivids v Datu valsts inspekcija* [2019] ECLI:EU:C:2019:122, para 43. See Herke Kranenborg, 'Article 2. Material scope' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 68.

[64] To be sure, we note that it is unclear how realistic the threat of other people accessing the personal data must be, and how to determine what constitutes an indefinite number of people.

[65] *Ryneš* (n 58) paras 27-30.

[66] European Data Protection Board, 'Guidelines 3/2019 on processing of personal data through video devices' (2020) 7-8. See also Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (WP 242, 5 April 2017) 5; European Data Protection Board, 'Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications' (2020) 15.

[67] European Data Protection Board, 'Guidelines 3/2019 on processing of personal data through video devices. Version 2.0 Adopted on 29 January 2020' (n 66) 8.

[68] ibid.

[69] In theory, although the EDPB has not endorsed the WP29's guidelines on the application of the household exemption in various contexts, those guidelines could provide further guidance a. See Article 29 Data Protection Working Party, 'Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance' (WP 89, 11 February 2004) 14; Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136, 20 June 2007) 4-5; Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking' (WP 163, 12 June 2009) 6; Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices' (WP 202, 27 February 2013) 9; Article 29 Data Protection Working Party, 'Opinion 8/2014 on the on Recent Devel-

3.2. *The controller: determining the purposes and means?*

The GDPR attributes the principal burden of compliance to controllers: entities that, alone or jointly with others, determine the purposes and means of the processing of personal data.[70] While other classifications are possible, we identify three conditions in the definition of the notion of controller: (1) an actor has to be a "natural or legal person, public authority, agency or other body"; (2) that actor has to determine the *purposes* of a processing operation; and (3) the actor also has to determine the *means* of the processing operation. Pluralistic control is a viable option to the extent that actors can jointly determine the purposes and means of a processing operation. Beyond this, further guidance on controllership needs to be found in the CJEU's case law and the EDPB's guidance.

In May 2014, the CJEU held in *Google Spain* that the concept of controller must be interpreted broadly in a way that reflects the aim of the former Data Protection Directive and that ensures the effective and complete protection of data subjects.[71] Following that expansive interpretation, the Court concluded that Google qualified as controller for processing operations in the context of Google Search because it processed personal data, published elsewhere on the internet, for its own independently determined purposes.[72] The Court further concluded that Google must ensure, within the framework of its responsibilities, powers and capabilities, that it complies with the national implementations of the Data Protection Directive.[73] However, it is unclear what this proviso actually entails.[74]

More recently, the EDPB adopted Guidelines 07/2020[75] and 08/2020,[76] in which it provides guidance on (joint) controllership under the GDPR by essentially revamping the WP29's Opinion 1/2010.[77] It is worth highlighting some of their main takeaways. Most importantly, the EDPB has held that the concept of controller is functional in the sense that it aims "to allocate responsibilities according to the actual roles of the parties" and, consequently, that actual circumstances should trump formal designations.[78] This means that an actor must have actually exerted a determinative influence over the purposes and the *essential* means of a processing operation, though it is not necessary that the actor has access to the personal data.[79] Furthermore, the EDPB has specified that controllership mandates a case-by-case assessment, meaning that an actor can be considered both a controller for the entirety of processing operation as well as a processor or data subject for another processing operation.[80]

3.3. *The joint controllers: jointly determining the purposes and means*

The GDPR accepts a model of pluralistic control by acknowledging that actors can jointly determine the purposes and the means of a processing operation. The GDPR states that "[where] two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers".[81] It further stipulates how joint controllers should go about their shared responsibilities: they must determine their respective responsibilities in a transparent manner by means of an arrangement, and they can designate a contact point for data subjects.[82] Beyond this, clarity on the concept of joint controllership must be again be sought in the CJEU's jurisprudence and the EDPB's guidance.

Since June 2018, the CJEU has interpreted joint control in three cases: *Wirtschaftsakademie; Jehovan todistajat*; and *Fashion ID*. In those cases, the Court has developed a taxonomy of criteria for determining joint controllership. Because these cases have been extensively commented elsewhere, we highlight only those criteria most relevant to our analysis.[83]

---

opments on the Internet of Things' (WP 223, 16 September 2014) 13; Article 29 Data Protection Working Party, 'Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones' (WP 231, 16 June 2015) 9;

[70] Article 4(7) GDPR.

[71] Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317 paras 34 and 38.

[72] ibid paras 32-41.

[73] ibid para 38. We note that this limiting principle has been underscored by an Advocate General, which reinforces its importance. See Case C–40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629, Opinion of AG Bobek, para 92.

[74] Rene Mahieu, Joris van Hoboken, and Hadi Asghari, 'Responsibility for Data Protection in a Networked World – On the Question of the Controller, "Effective and Complete Protection" and Its Application to Data Access Rights in Europe' (2019) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 85, 85, 89 and 97.

[75] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (Version 2.0, Adopted 7 July 2021).

[76] European Data Protection Board, 'Guidelines 08/2020 on the targeting of social media users' (2020).

[77] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (WP 169, 16 February 2010) 4-6.

[78] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 75) 9. The functional nature of the concept of controller has been underscored by two Advocate Generals, which reinforces the necessity of a factual rather than formal analysis. See Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, Opinion of AG Jääskinen, para 83; Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] ECLI:EU:C:2018:388, Opinion of AG Bot, para 46.

[79] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 75) 10-16.

[80] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 75) 11 and 15.

[81] Article 26(1) GDPR.

[82] Article 26 GDPR.

[83] For recent analysis of these cases against the concept of controllership, see e.g. Michèle Finck, 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law' (2021) 11 International Data Privacy Law 333; Lilian Edwards and others, 'Data Subjects as Data Controllers: A "Fashionable" Concept? | Internet Policy Review' (*Internet Policy Review*, 13 June 2019); Rene Mahieu, Joris van Hoboken, and Hadi Asghari (n 74); Silvia De Conca, 'Between a Rock and a Hard Place: Owners of Smart Speakers and Joint Control' (2020) 17 SCRIPTed 238; Charlotte Ducuing and Jessica Schroers, 'The Recent Case Law of the CJEU on (Joint) Controllership: Have We Lost the Purpose of "Purpose"?' (20201121)

The CJEU has repeatedly held that the concept of controller and, consequently, that of joint controller must be interpreted broadly in a way that reflects the aim of the Data Protection Directive and that ensures the effective and complete protection of data subjects.[84] Furthermore, the Court seems to have placed a strong emphasis on the determination of the purposes: it held in *Jehovan todistajat* that an actor "who exerts influence over the processing of personal data, for their own purposes, and who participates, as a result, in the determination of the purposes and means of that processing", can be considered a controller.[85] This raises the question of whether it is sufficient for an actor to only determine the purposes of a processing operation to be considered the controller of that processing operation. Moreover, the Court held in *Fashion ID* that an actor can only qualify as joint controller for the processing of personal data for which it actually jointly determines the purposes and means.[86] In other words, an actor cannot qualify as joint controller for the processing operations *preceding* or *succeeding* those for which it actually determines the purposes and means. Besides, the Court stated in *Wirtschaftsakdemie* that the concept of joint controller does not necessarily imply equal responsibility amongst joint controllers because they "may be involved at different stages of that processing of personal data and to different degrees".[87] This phase-orientated assessment could limit overly broad interpretations of joint controllership. Even though not decisive, the "effective control" and the "conception that the data subject has of the controller" can also be taken into account, as the CJEU noted in *Jehovan todistajat*.[88]

In our interpretation, the CJEU's case law sets a low threshold to conclude that an actor exerts sufficient influence over the determination of the purposes and means to qualify as joint controller.[89] For instance, in *Wirtschaftsakademie, contributing* to the processing of personal data *ex post* by creating a fan page on a social network without determining the purposes and means *ex ante* can be sufficient.[90] In *Fashion ID*, by embedding a third-party plug-in, an operator of a website exerted *decisive influence* over the collection and transmission of the personal data of visitors of its website.[91] It remains unclear to what *extent* an actor actually needs to contribute to the determination of the purposes as well as the means in order to be considered a joint controller. Nevertheless, in all three judgments discussed, the Court ultimately concluded or suggested that joint controllership could be established.[92]

As a result of the CJEU's case law, it is expected that specific processing operations will involve more joint controllers than previously assumed.[93] It is also expected that the legal qualification of actors involved in a processing operation enters a state of flux, "sometimes switching between controller, processor, and joint controller depending on what processing activity is being undertaken at a given moment in time".[94] The concept of "controller" therefore requires a case-by-case assessment to determine who is responsible for specific processing operations at certain moments in time. However, the CJEU has so far not formulated standardised rules on how to determine what degree of influence must be exerted by an actor for them to qualify as a joint controller.

The EDPB has provided guidance on the concept of joint controllership in Guidelines 07/2020 and Guidelines 08/2020.[95] It has stated that the assessment of joint controllership should mirror that of single controllership, meaning that a functional approach and a case-by-case assessment are also prescribed in this regard.[96] It has further held that the joint determination of the purposes and means can take different forms. These include common as well as converging decisions, with different contributions from different actors.[97] Decisions are *converging* when "they complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing".[98] Consequently, actors' processing operations have to be *inextricably linked*: the processing of personal data should not be possible without the actors' contributions thereto.[99] This means not only that actors can be considered joint controllers when they pursue closely linked or complementary purposes but also that actors do not always need to be involved in the determination of all the means.[100]

2020 Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht 424.

[84] Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388 paras 26-28; *Jehovan todistajat* (n 63) para 66; Case C–40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629; Case C-272/19 *VQ v Land Hessen* [2020] ECLI:EU:C:2020:535, para 66.

[85] *Jehovan todistajat* (n 63) para 68.

[86] *Fashion ID* (n 84) paras 71-74.

[87] *Wirtschaftsakademie* (n 84) paras 38 and 43.

[88] *Jehovan todistajat* (n 63) para 21.

[89] Finck aptly describes this as a "mellow definition of control". Finck (n 83) 333.

[90] ibid paras 34-43. In *Jehovan todistajat*, the CJEU held that *participating* in the determination of the purposes and means of the processing of personal data by organising, coordinating and encouraging an activity that involves data processing can be sufficient for joint controllership. See *Jehovan todistajat* (n 63) paras 70-72.

[91] *Fashion ID* (n 84) para 78.

[92] *Wirtschaftsakademie* (n 84) para 39; *Jehovan todistajat* (n 63) paras 73 and 75; *Fashion ID* (n 84) paras 79, 81 and 84-85.

[93] Rene Mahieu, Joris van Hoboken, and Hadi Asghari (n 74); Finck (n 83).

[94] Christopher Millard et al., 'At This Rate, Everyone Will Be a [Joint] Controller of Personal Data!' (2019) 9 International Data Privacy Law 217, 218.

[95] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (n. 75); European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users' (2020).

[96] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (n 75) 17.

[97] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (n 75) 18.

[98] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (n 75) 18.

[99] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (n 75) 18.

[100] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (n 75) 19–20.

4. How does the law apply to virtual assistants?

Having examined the rules on (joint) controllership, we now apply them to the contemporary processing operations of virtual assistants, using Google Assistant as a case study. To make our analysis concrete and manageable, we develop and use three scenarios that we consider to have explanatory power vis-à-vis the determination of joint controllership, and which we introduce as this section progresses. The aim of our scenarios is to map how the rules on joint controllership apply to the operation of virtual assistants. Because this is mapping exercise focusing on joint controllership, the analysis does not dive into all possible scenarios regarding all stakeholders involved in the operation and use of virtual assistants, nor does it discuss the potential application of all elements of data protection law in this regard.[101] In addition, we note that Google Assistant is available on a plethora of end-user products and new functionalities are released on a rolling basis; both aspects can have an impact on our analysis.[102]

4.1. *Scenario 1: a linear data processing model*

The first scenario is as follows: Alice asks Google Assistant, which she operates via a Google Home, to search what the GDPR is. Shortly thereafter, Google Assistant informs Alice about the number one hit on Google Search. This scenario involves two actors: Alice, the natural person using the virtual assistant; and Google, the legal person operating the virtual assistant. Google is the only actor that processes Alice's personal data as needed to carry out their query.

This scenario involves a "linear model" of processing: one actor collects personal data from another actor, and subsequently uses the data until their ultimate deletion.[103] As such, Alice qualifies as data subject, while Google qualifies as controller for the processing of their personal data as needed to carry out the query.[104]

An interesting question is whether Alice can also qualify as (joint) controller for the processing of their own personal data. If we adopt an extensive interpretation of the determination of the purposes and means, they might arguably qualify as controller, alone or jointly with Google. It can be argued that Alice has Google collect their personal data for their own purposes, which may partially or fully coincide with Google's purposes: improving their knowledge on the law in general and data protection law in particular. There are judicial and supervisory leads that undergird this argument. As to the means, it can be argued that Alice has determined the technical means of the collection of their personal data by using Google Assistant, and querying it to conduct a search, when they could have also used another virtual assistant or conducted a manual search.[105] There is also judicial and supervisory support for this. For instance, the CJEU held in *Fashion ID* that a website operator exerted decisive influence over the processing of visitors' personal data by embedding a plug-in on its website, without which the processing would not have happened.[106]

However, that would be an incorrect qualification in our view. First, it collides with the CJEU's principle of effective and complete protection in the sense that it could not only deprive the data subject of protection but also subject them to obligations ordinarily imposed on controllers in order to protect their interests in their personal data.[107] Although not explicitly stated as such, this also appears to be the understanding of the EDPB it its Guidelines 02/2021 on virtual voice assistants.[108] Second, Alice could benefit from the household exemption by arguing that their personal data is not made "accessible to an indefinite number of people" and the processing is not directed outwards from their private setting.[109] The crux is that the CJEU has never been asked to rule on the application of the household exemption in such a case, leaving the door open for discussion. Nonetheless, based on our analysis, our tentative conclusion is that in this scenario Alice qualifies as data subject, whereas Google qualifies as controller for the processing of their personal data.[110]

4.2. *Scenario 2: a data processing chain*

The second scenario is as follows: While reading up on what the GDPR is, Alice queries the Google Assistant to play 'Lost' by Frank Ocean on Spotify. In a matter of seconds, the song starts playing on their Google Home. This scenario involves three actors: Alice, the natural person using the virtual assistant; Google, the legal person operating the virtual assistant

[101] Other scenarios could be devised, e.g. around the different stakeholders involved, as noted in European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 15. ("… the main stakeholders can be identified under the role of a provider or designer, an application developer, an integrator, an owner, or a combination of them. Different scenarios are possible, depending on who is doing what in the stakeholders' business relationship, on the user's request, the personal data, the data processing activities and their purposes.")

[102] Google and third-party manufacturers increasingly incorporate the Google Assistant into a plethora of end-user products, such as smartphones and smart home devices as well as wearables and cars (section 0), meaning that individuals can also use the Google Assistant outside of the home, which, when applying the framework, can yield different results than presented in this paper. We clarify such differentiation, where relevant.

[103] Omer Tene, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74 Ohio State Law Journal 1217, 1219.

[104] De Conca (n 83) 253–254.

[105] De Conca (n 83) 249–256.

[106] *Fashion ID* (n 84) para 78. See also *Wirtschaftsakademie* (n 84) paras 36-37; Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010) WP 169 14.

[107] Lee A. Bygrave and Luca Tosoni, 'Article 4(7). Controller', *The EU General Data Protection Regulation (GDPR). A Commentary* (Oxford University Press 2020) 154.

[108] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 15-17 (cit. 15).

[109] *Lindqvist* (n 57) paras 47-48; *Ryneš* (n 58) paras 33-35. See also *Jehovan todistajat* (n 63) paras 44-45; *Buivids* (n 63) para 43. The exemption might not be available in certain sub-scenarios. For example, if Alice had queried the Google Assistant to post their query on LinkedIn, which could involve making her personal data accessible to an indefinite number of people.

[110] De Conca (n 83) 253–254.

and collaborating with Spotify; and Spotify,[111] the legal person operating Spotify and collaborating with Google. In that connection, Google processes personal data as needed to transmit Alice's query to Spotify, which processes the data as needed to carry out their query. For our purposes, we assume that the Spotify Action is not fully integrated in the Google Assistant.[112]

Similar to our analysis of the first scenario, Alice qualifies as data subject, while Google qualifies as controller for the processing their personal data as needed to carry out the query. But this second scenario involves Spotify as an additional actor. Spotify may receive the processed personal data from Google, which it will process to start streaming the song. Alternatively, even if Spotify is fully integrated in Google Assistant, it may still register in Alice's account that the song was streamed.

Here it is important to refer to *Google Spain*, where the CJEU qualified Google as separate controller for the processing of personal data in the context of Google Search because the processing "can be distinguished from and is additional to that carried out by publishers of websites", and it "affects the data subject's fundamental rights additionally".[113] Applying this reasoning here, Google and Spotify likely qualify: as joint controllers for processing operations that involve both actors; or as singular controllers for processing operations that involve one actor. It is also relevant to mention *Fashion ID*, where the Court clarified that an actor can only be considered a joint controller with respect to the processing of personal data for which it jointly determines the purposes and means and not also those operations preceding or succeeding it.[114] By analogy, an actor should only qualify as sole controller for the processing of personal data for which it singularly determines the purposes and means.[115]

To better understand this second scenario we are presenting, it is useful to make a further distinction between processing operations that involve the collection, use, and transfer of personal data in a virtual assistant. For that reason, we examine below first the collection of Alice's personal data by Google and their possible transmission to Spotify (4.2.1). In the second place, we look into the use of Alice's personal data by Google and Spotify (4.2.2).

4.2.1. *The collection and transmission of personal data*

As concluded, Google acts as controller for the initial collection and the possible transmission of Alice's personal data. As to Spotify, it is important to examine the degree of influence it exerts on the determination of the purposes and means of these processing operations.

Spotify has Google collect and possibly transmit Alice's personal data for its own purposes, which may partially or fully coincide with Google's purposes: providing its streaming services to Alice via a conversational user interface. In that connection, the CJEU found in *Fashion ID* that, by embedding a plug-in on its website, a website operator seemed to have "consented, at least implicitly", to the collection and transmission of personal data of visitors of the website as to "optimise the publicity of its goods by making the more visible" on a social network operated by the developer of the plug-in.[116] Applying this reasoning here, it can be argued that Spotify has *de facto* consented to the collection and possible transmission of Alice's personal data. In order to make its streaming service accessible via the Google Assistant, Spotify had to deliberately go through a development cycle as well as rigorous review by Google. This suggests that Spotify has explicitly consented to at least the collection and possible transmission of personal data and possibly also to the other processing operations. Additionally, the Court stated in *Fashion ID* that the processing serves the economic interests of the operator of the website as well as the developer of the plug-in, which can apparently be indicative for the joint determination of the purposes.[117] In our scenario, the collection and possible transmission of Alice's personal data ultimately serve the economic interests of Spotify as well as Google: Spotify is able to sell its streaming subscription to Alice and to improve its services; Google is able to sell more services and devices compatible with the Assistant to Alice and to improve its targeted advertising system.

Lastly, there is support in the case law and in supervisory guidance to the argument that influencing the processing of personal data for one's own purposes can be sufficient to lead to a qualification as (joint) controller.[118] Spotify has arguably done this, though some doubts may subsist.

As to the means, Spotify has arguably jointly determined the technical means of the collection and possible transmission of Alice's personal data by making its streaming service accessible via the Google Assistant.[119] Following *Fashion ID*, it is likely that Spotify exerts decisive influence over the collec-

---

[111] To be sure, European individuals contract with Spotify AB, a private limited liability company under Swedish law, with its headquarters in Stockholm, Sweden. However, Spotify AB is publicly traded in the New York Stock Exchange through Spotify Technology S.A., a public limited liability company under Luxembourgish law, with its headquarters in Stockholm, Sweden. By and large, we proceed on the assumption that Spotify is subject to the GDPR, to the extent it *de jure* processes personal data, because it seems likely that both companies qualify as a European establishment within the meaning of the GDPR. Besides, Spotify AB refers to the GDPR in its privacy policy, which suggests that Spotify assumes that it is, at least to some extent subject to the GDPR (Spotify, 'Spotify Privacy Policy' (*Spotify*) <https://www.spotify.com/ie/legal/privacy-policy/> accessed 2 February 2022).

[112] See section 2.2.

[113] *Google Spain* (n 71) paras 35, 38 and 83.

[114] *Fashion ID* (n 84) para 71-74.

[115] This approach is also endorsed by the EDPB when examining the processing by data controllers and processors in the context of virtual voice assistants. See European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 15–17.

[116] *Fashion ID* (n 84) para 80.

[117] ibid. See also *Wirtschaftsakademie* (n 84) para 34.

[118] *Jehovan todistajat* (n 63) para 68; European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (n 75) 19; European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users' (n 95) 22–23.

[119] European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users' (n 95) 19–20. Afterall, Spotify could have instead made it streaming service accessible via another third-party virtual assistant or not virtual assistant at all, or it could have developed its own virtual assistant.

tion and possible transmission of Alice's personal data, since they probably did not query Google Assistant to stream the song via Spotify if this service was not accessible through the virtual assistant.

To be sure, it can be questioned whether Spotify has "effective control" on the determination of the means. This is because Google provides tools for the development and operation of Actions.[120] Still, and in our view, qualifying Spotify as joint controller for the collection and possible transmission of Alice's personal data aligns best with the CJEU's principle of effective and complete protection, as it ensures that Alice is not deprived of protection.[121]

In light of the above, and while recognising that the complexity of a virtual assistant's ecosystem requires a case-by-case assessment,[122] our tentative conclusion is that Spotify qualifies as joint controller for the collection and possible transmission of Alice's personal data.

4.2.2. *The use of personal data*

As to the use of Alice's personal data by Google and Spotify, both actors evidently qualify as controllers for their own use of Alice's personal data. It is thus important to examine the degree of influence Spotify exerts on the determination of the purposes and means of Google's use of Alice's personal data, and vice versa.

On Spotify's contribution, the company qualifies as joint controller for Google's use of Alice's personal data for the reasons presented above at 4.2.1. In *Fashion ID*, the CJEU restricted the scope of its investigation to the collection and transmission of personal data via a plug-in as it considered impossible for a website operator to determine the purposes and means of any subsequent processing of personal data carried out by the developer of the plug-in.[123] Applying that logic here, Spotify's contribution would not extend to Google's use of Alice's personal data.

Nevertheless, it seems that both the website operator's and Spotify's purposes go beyond the collection and possible transmission of personal data. Both are arguably more interested in the results of the subsequent use, respectively: optimising the publicity of its services by making them more visible on a social network; selling more subscriptions and improving its streaming services. It thus appears artificial to restrict the contribution of either actor to the collection and possible transmission of personal data.

Therefore, we see two possible interpretations. If one follows the CJEU's reasoning, Spotify does *not* qualify as joint controller for Google's use of Alice's personal data. Alternatively, if we challenge the Court's reading on the grounds noted above, Spotify will qualify as joint controller for Google's use of Alice's personal data.[124] While we are sympathetic to the latter option, *de lege lata* it appears that Google should qualify as sole controller for its use of Alice's personal data.

Following that same approach, on Google's contribution, Spotify should qualify as the sole controller for its use of Alice's personal data. Still, it is important to note that Google provides third-party developers with dedicated software and a cloud environment to use received personal data.[125] As a consequence, depending on the facts of the case, it cannot be excluded that Google may qualify as processor for personal data stored and used in a dedicated cloud environment.[126]

4.3. *Scenario 3: complicating the data processing chain*

The third scenario is as follows: Bob, Alice's room-mate, expresses their distaste for the music playing, and they call on the Google Assistant to stream 'You Should Be Here' by Kehlani on Spotify. The music changes in an instant. Four actors play a part in this scenario: Alice, the natural person owner of (and hosting) the virtual assistant (the registered user); Bob, the natural person using the virtual assistant (the non-registered but not accidental user[127]); Google, the legal person operating the virtual assistant and collaborating with Spotify; and Spotify, the legal person operating Spotify and collaborating with Google. As results from the previous analysis, Google processes personal data as needed to transmit Bob's query to Spotify, which also processes personal data as needed to carry out Bob's query.

In light of the first and second scenarios, Bob will qualify as data subject, while Google and Spotify qualify as: joint controllers for the collection and possible transmission of Bob's personal data; and sole controllers for their own use of Bob's personal data. It is therefore important to examine the degree of influence Alice exerts on the determination of the purposes and means of the processing operations at issue.

Alice will qualify as joint controller for the collection and possible transmission of Bob's personal data, since the arguments presented in the context of second scenario apply here.[128] As noted in the first scenario, it can be argued that Alice has Google collect and possibly transmit Bob's personal data for their own purposes, which may partially or fully coincide with Google's and Spotify's purposes: entertaining their guests by having them stream their favourite songs via a conversational user interface.[129] It can also be argued that Alice

[120] *Jehovan todistajat* (n 63) para 21; European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (n 96) 13–14 and 19–20.

[121] *Google Spain* (n 71) paras 34 and 38; *Wirtschaftsakademie* (n 84) paras 26-28; *Jehovan todistajat* (n 63) para 66; *Fashion ID* (n 84) para 66.

[122] See European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 15-18 (cit. 18). (making reference to "ecosystem complexity" as a barrier to transparency and the determination of processors and controllers as regards virtual voice assistants).

[123] *Fashion ID* (n 84) paras 75-76.

[124] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (n 75) 22; European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users' (n 95) 13–14, 17–20.

[125] Google, 'Dialogflow' (*Google*) <https://cloud.google.com/dialogflow> accessed 2 February 2022.

[126] We do not further examine Google's possible qualification as processor.

[127] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 15. (discussing different types of users in context of a plurality of data subjects interacting with a virtual voice assistant).

[128] This assertion assumes the simplest scenario where Alice qualifies as (joint) controller but Bob does not.

[129] See section 4.2.1.

has determined the technical means of the collection and possible transmission of Bob's personal data by using the virtual assistant and leaving it running on standby in the background, when they could have also used another virtual assistant, dismantled the Google Home, or changed the song on Bob's behalf.[130] Still, it is debatable whether Alice would also qualify as joint controller if Bob's personal data had accidentally been collected and possibly transmitted by Google, as argued by De Conca.[131] In our view, Alice prima facie qualifies as joint controller for the collection and possible transmission of Bob's personal data, at least outside cases of accidental processing. This qualification of Alice as a joint controller is a manifestation of what has been called the "diversion of responsibility to the data subject".[132]

But can Alice benefit from the household exemption? As noted, the household exemption arguably applies. Alice, Google and Spotify do not make Bob's personal data "accessible to an indefinite number of people". Furthermore, the collection and possible transmission of that data is not directed outwards from Alice's private setting.[133] However, the household exemption would likely not apply if Bob had, for instance, queried Google Assistant to upload their music preferences to their (publicly available) Instagram account, thereby making their personal data accessible to an indefinite number of people. The exemption would also probably not apply if Alice had Google Assistant running on their smartphone, while they were out and about running errands, and the virtual assistant collected bystanders' personal data.[134]

4.4. *Summary of scenarios: a complex controllership test*

The analysis above highlights the challenges in applying the GDPR rules on controllership to Google Assistant in particular and, by extension, to virtual assistants in general. The test that emerges from these rules, considering CJEU case law and supervisory guidance, is both complex and ambiguous, raising legal certainty concerns. The analysis shows that the concepts of data subject, controller and joint controller are in flux. Although there are benefits to this flexibility, the associated trade-offs in complexity and legal uncertainty are patent in the particular context of virtual assistants and most likely also in the broader setting of the Internet of Things.[135] Table 1 provides a schematic visualisation of our conclusions.

Table 1 illustrates that the first scenario, the most straightforward of the three, only involves one data subject, Alice, and one controller, Google. The qualifications change as soon as Alice queries Google Assistant to stream music via Spotify, a third-party Action. In this second scenario, Alice still qualifies as data subject, but Google now qualifies as sole controller or joint controller depending on the processing operation. In addition, Spotify is now involved in the processing of Alice's personal data as sole controller or joint controller depending also on the processing operation. To complicate things further, the qualifications change once more when it is not Alice but their room-mate Bob who queries the virtual assistant to stream music via Spotify. In this third scenario, Bob qualifies as data subject, whereas Alice arguably qualifies as joint controller for the collection and possible transmission of Bob's personal data; Google and Spotify qualify as sole or joint controller depending again on the precise processing operation. Although courts may arrive at different conclusions, the crux of the matter is that the case-by-case test to determine (joint) controllership is complex and ambiguous as a consequence of the broad interpretation of the CJEU.

In reality, the legal assessment is more complex than our analysis indicates, due to the plurality of personal data, data subjects and data processing at stake in the operation of virtual assistants.[136] Additional scenarios could be envisaged that consider additional stakeholders (e.g. "provider or designer, an application developer, an integrator, an owner, or a combination of them"[137]), as well as a more granular analysis of their processing operations.

Further complexity arises from the requirements applicable to data controllers, such as transparency obligations.[138] Although the topic is outside the scope of our analysis, it may impact our scenario analysis above. Controllers must "inform users of the processing of their personal data in a concise, transparent, intelligible form, and in an easily accessible way"; where they fail to do so, they are in breach of their obligations, which "may affect the legitimacy of the data processing" in the operation of virtual assistants.[139] However, as noted by the EDPB, complying with transparency obligations is challenging for controllers as it relates to virtual assistants, due to the plurality of users (including vulnerable categories of individuals), ecosystem complexity, and the specificities of the technology (namely the vocal interface).[140] For instance, providers of virtual assistants like Google may bundle their assistant services with additional services (email, storage, music and video streaming, online shopping, etc.), resulting in the need for "lengthy and complex privacy policies", which "greatly hinder fulfilling the transparency principle".[141] In another example, it is also particularly challenging in practice to comply with transparency obligations vis-à-vis non-registered users

[130] See section 4.2.1.
[131] De Conca (n 83) 257.
[132] Finck (n 83) 341.
[133] See supra at 3.1.
[134] De Conca (n 83) 267.
[135] Chen et al. (n 62).
[136] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 14–17.
[137] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 15.
[138] See Articles 5(1)(a), 12 and 13 GDPR.
[139] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 17.
[140] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 17–18. (noting the substantial asymmetry of information between users and service providers in this context, and suggesting inter alia that providers improve the interactive functionality of virtual assistants in concrete ways to enhance transparency).
[141] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 18.

Table 1 – Application of the controllership rules to Google Assistant.

	Alice	Google	Spotify	Bob
Scenario 1	data subject	controller	–	–
Scenario 2	data subject	controller; joint controller	controller; joint controller	–
Scenario 3	joint controller[1]	controller; joint controller	controller; joint controller	data subject

[1] To keep the scope of this article manageable, we decided against considering the possibility of Alice qualifying as a data subject in the third scenario. However, when Google and Spotify save Bob's query with Alice's account, the query could qualify as Alice's personal data. Where it does not, that query actually relates to Bob. This could trigger issues with the principle of data accuracy as set out in Article 5(1)(d) GDPR. Clearly explaining from both a legal and technical perspective would require a more thorough probe into the actual workings of Google Assistant at a given moment in time.

that do not own the device where an assistant is installed and running, such as Bob in our third scenario.[142] Although, the EDPB suggests concrete solutions to mitigate some of these issues,[143] it is much vaguer as it regards controllership. In this respect, it merely recommends that "[*p*]articular consideration should be applied if devices allow adding third party functionality" (as in our Scenarios 2 and 3), since "during the normal use of the device the boundaries between the various controllers involved can be much less clear", and "the user might be not sufficiently informed how and by whom their data is processed (and to which extent) in a specific query".[144] In other words, a principled approached is suggested, but a concrete solution is lacking. The likely result is detrimental to the effectiveness of the law and the protection of data subjects.[145]

The upshot is that all this complexity of the rules on controllership and associated obligations makes their application to the operation and use of virtual assistants challenging and, in some instances, perhaps impractical. By the same token, these rules also facilitate the design of what has been called "complex cobwebs of control" that aim at complicating enforcement by multiplying the parties that qualify as "controller" – and by extension the associated responsibilities – while in practice effective and meaningful control rests with "real" data controllers.[146] In this sense, virtual assistants provide a powerful illustration of the increasing challenges posed by new data-driven technological systems to data protection rules in general, and the concept of controllership in particular. This leads to the question of how to consider responsibility for controllership in such an environment.

5. How to approach responsibility for controllership?

Having demonstrated that the framework used to determine who qualifies as controller or joint controller appears inappropriate and difficult to work with in the present-day information society, this article now flags some important follow-on issues relating to the correct and meaningful apportionment of responsibilities between joint controllers, and the effective and complete protection of data subjects.[147] Importantly, because the focus of our analysis is on the use of virtual assistants in the private sphere, the recommendations that follow should be understood as predominantly delimited to that scope.[148]

5.1. *The apportionment of responsibilities between joint controllers*

The GDPR provides some clarification on how joint controllers should go about their responsibilities vis-à-vis each other as well as data subjects. Importantly, joint controllers must apportion their respective responsibilities in a transparent manner, in particular with respect to their information obligations as well as the rights of data subjects, by means of an arrangement concluded between them.[149] In other words, joint controllers can freely apportion responsibilities amongst themselves on the condition that all responsibilities are met.[150] The arrangement may designate a contact point for data subjects and shall duly reflect the joint controllers' respective roles and relationships vis-à-vis data subjects.[151]

Crucially, however, the GDPR does not entail a clear mechanism on how to apportion responsibilities.[152] In Guidelines 07/2020, the EDPB has stated that responsibilities have to be allocated according to the factual circumstances, taking into

[142] See supra at 4.3 and European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 19–20. (noting that these "users should be informed at the earliest time possible and at the latest, at the time of the processing", while recognizing that such "condition could be especially difficult to fulfil in practice.")

[143] Examples include separate privacy policy sections for processing of data by virtual assistants, exact information provision to users on data processed and the current (active or passive) state of the assistant.

[144] European Data Protection Board, 'Guidelines 02/2021 on Virtual Voice Assistants (Version 2.0)' (n 11) 20.

[145] Finck (n 83) 334.

[146] Finck (n 83) 334, 344.

[147] To be sure, there are many more issues to flag, but space does not permit a comprehensive overview. For example, see Millard et al. (n 94) 218-219.

[148] See supra at 2.1.

[149] Article 26(1) GDPR. See also Christopher Millard and Dimitra Kamarinou, 'Article 26. Joint controllers' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 587.

[150] Rene Mahieu, Joris van Hoboken, and Hadi Asghari (n 74) 98.

[151] Articles 26(1) and 26(2) GDPR.

[152] Finck (n 83) 335–336.

account, for instance, who is competent to comply with data protection obligations, such as effectively answering to data subjects' rights.[153] Still, it remains unclear how to assign responsibilities to specific processing operations in a larger sets of consecutive processing operations, how to determine different degrees of responsibility in practice, and how to enforce unlawful processing operations in the context of joint control.[154] This raises the question of to what extent it is justified to partially or fully impose a regulatory burden on especially individuals.

As De Conca noted, there is a significant power imbalance between manufacturers of smart speakers and device owners. In that connection, she argues that qualifying such individuals as joint controllers "would mean to ignore the factual circumstances and ignore the necessity for actual decisional power", especially "if we consider average users might not even be fully aware of the functioning of the smart speakers".[155] Besides, it is unclear as to that extent power imbalances can be taken into account when apportioning responsibilities between joint controllers *de lege lata*. For a case in point, contrast *Google Spain*, where the Court notes that a controller must ensure compliance "within the framework of its responsibilities, powers and capabilities", with the opinion of AG Bot in *Wirtschaftsakademie*, to the effect that holding a fan page administrator accountable "is likely to have the ripple effect of encouraging the social networking platform itself to comply with those rules".[156]

Nonetheless, data subjects can exercise their rights vis-à-vis all joint controllers, irrespective of the terms of the arrangement concluded between them.[157] In other words, joint controllers can only use the arrangement to give practical effect as to whom is responsible for honouring data subjects' rights, but remain responsible that data subjects' rights are honoured, under penalty of joint and several liability.[158] In order to ensure effective compensation of data subjects, all joint controllers can be held liable for the damages suffered as a consequence of the unlawful processing of their personal data, though one joint controller can claim compensation from the others that matches their share of responsibility for the damages suffered.[159] Additionally, joint controllers are also subject to regulatory enforcement since a supervisory authority can impose effective, proportionate and effective administrative fines on them in the event they unlawfully process personal data.[160] The GDPR is as clear on the allocation *ex post* liability to joint controllers as it is unclear on the apportionment of *ex ante* obligations.[161]

To refer back to our case study, when the household exemption does not apply to Alice, it seems that they can only avoid being considered a joint controller by turning off their Google Home. While for some it might be reasonable to expect that individuals inform each other about the presence of potentially privacy-invasive technologies, it is nonetheless a different matter to require that this expectation is anchored in terms of allocating data protection obligations to end-users, as well as an accompanying set of rights to other individuals. This is especially so when affected individuals can already fall back on national laws, such as civil law remedies, in the event of disagreement.[162]

5.2. *The effective and complete protection of data subjects*

As noted, the expected consequence of the CJEU's broad interpretation of (joint) controllership is that specific processing operations will involve many more (joint) controllers than previously assumed.[163]

In connection with this explosion of (joint) controllers, the legal qualification of actors involved in data processing operation enters a state of flux, "sometimes switching between controller, processor, and joint controller depending on what processing activity is being undertaken at a given moment in time".[164] Indeed, it is often difficult to delineate "between joint controllers, separate controllers operating in cooperative networks, and other entities, such as processors", as noted by Bygrave and Tosoni.[165]

As Finck rightly notes, the motivation for the Court's "expansive approach towards controllership" lies with the (erroneous) "assumption that the more parties are responsible for compliance, the more protection data subjects enjoy".[166] But even from a descriptive standpoint, this assumption does not hold, as it is apparent that "broad definitions of control fail to achieve the stated objective of the complete and effective protection of data subjects", leading instead to a "pulverization and weakening of control".[167] The broad interpretation of (joint) controllership and the resulting ambiguities create legal uncertainty for actors attempting to accurately determine their legal qualification and respective obligations pursuant to the GDPR.[168] Paradoxically, the effective and complete protec-

[153] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 75) 41-42.
[154] Rene Mahieu, Joris van Hoboken, and Hadi Asghari (n 74) 99. See also Finck (n 84) 337. ("the distribution of duties among controllers is fraught with practical uncertainty")
[155] De Conca (n 83) 262.
[156] *Google Spain SL* (n 71) para 38; Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] ECLI:EU:C:2018:388, Opinion of AG Bot, para 74.
[157] Article 26(3) GDPR.
[158] Rene Mahieu, Joris van Hoboken, and Hadi Asghari (n 74) 98.
[159] Articles 82 GDPR. See also Brendan Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' (2017) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 271, 287.
[160] Article 83 GDPR.
[161] Chen et al. (n 62).
[162] De Conca (n 83) 262.
[163] Rene Mahieu, Joris van Hoboken, and Hadi Asghari (n 74) 95.
[164] Millard et al. (n 94) 219.
[165] Lee A. Bygrave and Luca Tosoni (n 107) 152.
[166] Finck (n 83) 333.
[167] Finck (n 83) 333, 337–338. (noting that "[a]s ultimately the 'genuine' controller needs to enforce the law and is held financially liable, the primary effect of a broad definition of control risks being the complication of accountability and hence a deterrence of data subject initiative"). From a normative standpoint, Finck further rejects the assumption on the basis that and expansive interpretation of controllership is "undesirable from a political economy perspective" and detrimental to the effectiveness of the law. See Finck (n 83) 341–344.
[168] Mahieu, van Hoboken and Asghari (n 74) 95.

tion of data subjects is actually at stake. In the prescient words of AG Bobek: "[making] everyone responsible means that no-one will in fact be responsible".[169] Besides, ambiguities can also make it difficult for data subjects to "obtain a meaningful understanding of a complex processing environment", and to determine against whom they can enforce their rights.[170]

Our case study brings the point across neatly. Apart from the question of who actually act as joint controllers in which circumstances, it is questionable to what extent Alice can effectively inform Bob about the processing of their personal data via the Google Assistant other than by noting that their data will be collected and transmitted for further processing, whatever that further processing may be. The challenging application of transparency obligations in the context of virtual assistants further amplifies the problem.[171] According to Mahieu and van Hoboken, this can create significant theoretical and practical issues from for properly addressing questions about the legitimacy of processing operations.[172] It is also questionable to what extent Alice can effectively honour Bob's rights, such as the right to access, as she has no actual influence over the means used to process their personal data, and is probably not able to access all their personal data.[173]

5.3. *Reconsidering control?*

From a normative perspective, the current state of the law is undesirable. The expansive concept of controllership and the rules on attendant responsibilities introduce complexity and legal uncertainty, bringing unintended legal and practical consequences for individual users of virtual assistants. One major consequence is the increasing muddying of the assessment of the correct and meaningful apportionment of responsibilities between joint controllers, and the effective and complete protection of data subjects. Another broader concern is whether passing on information duties and responsibilities to individuals that are otherwise data subjects hurts the legitimacy of the law in the eyes of those it aims to protect.

In this light, it is somewhat surprising that the European Commission's first ever review of the GDPR has characterised the rules on controllership as appropriate, despite inviting the EDPB to provide new guidance on the matter.[174] While that guidance has brought some clarity on (joint) controllership, it should have also elucidated how to assign responsibilities to specific processing operations in larger sets of consecutive processing operations, how to determine different degrees of responsibility in practice, and how to enforce unlawful processing operations in the context of joint control.[175]

Considering our findings, and at least as regards use of virtual assistants in the private sphere (and analogous settings), it is appropriate to question whether rather than relying on the household exemption, the concept of controller or joint controller should not be reconsidered, so as to exclude its applicability individuals that *de facto* do not or cannot act or function in that capacity.

In one such proposal, with a broader scope than our analysis here, Finck argues for an alternative interpretation of the concept of control that requires "meaningful influence over the techno-organizational elements of processing". According to this, "only those natural and legal persons that are effectively able to influence data processing (and hence exercise effective and real control over the data and software used to process it) are controllers".[176] This proposal is based not only on the etymology and history of the concept of control, and the GDPR's aims, but also on the characterisation of control in Articles 24 (on Responsibility of the controller) and 25 (on Data protection by design and by default). In short, the argument is that both provisions require that controllers must always influence the means of processing; Article 25 further demands "effectiveness" in the implementation of data protection principles. By elevating the requirement of Article 25 (to broader applicability) and combining it with Article 24, it would be possible to narrow the concept of controllership, focusing on parties that have "actual", "real" or "genuine" control, and setting aside its application to parties that do not have access to data and software, and enabling a clearer and more transparent allocation of responsibilities.[177]

The corollary of this reasoning is the outline of a new legal test for a "factual and functional approach to the determination of controllership" that would eventually set out a much needed de minimis threshold of control by elevating the required level of influence over the means of processing. This would mean that "only parties that determine the purposes and the means beyond the mere choice of a platform or service and the enabling of someone else's processing should be controllers."[178]

In our view, this is a sensible test: it allows for the practical application of the concept of controllership with the requisite degree of flexibility, while keeping in within reasonable bounds and avoiding overreach. The determinisation of a de minimis threshold of influence over the means is particularly consequential in the context of virtual assistants (at least within the scope of our analysis), as it will avoid the pulverisation controllership concept that leads to the appor-

[169] Case C–40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629, Opinion of AG Bobek, para. 92. See also Lee A. Bygrave and Luca Tosoni (n 107) 153.
[170] Millard et al. (n 94) 219.
[171] See supra at 4.1.4.
[172] René Mahieu and Joris van Hoboken, 'Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?' (*European Law Blog*, 30 September 2019) <https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/> accessed 2 February 2022.
[173] Chen et al. (n 62).
[174] European Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation' (Communication) COM (2020) 264 final, 10; European Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation' (Staff Working Document) SWD(2020) 115 final, 12 and 26-28.
[175] Rene Mahieu, Joris van Hoboken, and Hadi Asghari (n 74) 99.
[176] Finck (n 83) 334.
[177] Finck (n 83) 345–346.
[178] Finck (n 83) 347.

tionment of responsibilities to individuals that are otherwise data subjects, and the resulting erosion of the responsibility of those that factually and functionally in control. Doing so enables a clearer assessment of (joint) controllership and apportionment of responsibilities, including as regards transparency obligations, in increasingly complex technological ecosystems, like that of virtual assistants. Further research should address to what extent this alternative test holds in more public or commercial use cases of virtual assistants, such as using the interpreter mode of a virtual assistant at airports to help international passengers.[179]

6. Conclusion

This article provides an overview and critical examination of the rules for determining who qualifies as controller or joint controller under the GDPR, as interpreted by the CJEU and applied by the WP29 and EDPB. Using Google Assistant as a case study for the broader category of virtual assistants, we argue that these rules and their interpretation are challenging to apply in the increasingly complex reality of present-day information society services, especially in the context of the Internet of Things. The focus of our analysis is on the use of virtual assistants in the private sphere.

As a consequence of recent developments in case law and supervisory guidance, the rules on controllership have become complex, leading to an ambiguous legal test. In particular, the Court's broad interpretation is in essence justified only on the basis of the teleological argument of complete and effective protection of data subjects. In our view, this is a thin and perhaps even erroneous justification. As others have argued, an expansive interpretation of controllership may paradoxically lead to a diminution of data subjects' protection by eroding the concept and weakening the apportionment of responsibility.

Advances in technological applications and business models make it challenging to apply this test to contemporary processing operations. This is illustrated by our analysis of Google Assistant, but our findings could be generalised to most other virtual assistants. In particular, individuals can qualify as joint controllers, together with Google and also third-party developers, for at least the collection and possible transmission of other individuals' personal data through the virtual assistant. As this interpretative trend continues and as the Internet of Things continues to penetrate everyday life, individuals will increasingly qualify as joint controllers.

From a normative perspective, this is an undesirable outcome, as it introduces complexity and legal uncertainty for all stakeholders, particularly individual users of virtual assistants. Although an expansion of the currently narrow household exemption could mitigate some of the problems we have pointed out, our analysis identifies the increasingly broader and tentacular reach of controllership as the main problem in the current system. In that light, we suggest as a tentative solution a reconsideration of the concept of controllership that focuses on factual and functional control, thus targeting only parties that genuinely control the purposes and the means of processing. To that effect, we endorse Finck's proposal of operationalising this approach through a new test of controllership, which sets out a de minimis threshold of control, while noting that further research is needed on the application of this test to more public or commercial use cases of virtual assistants.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No data was used for the research described in the article.

[179] See supra at 2.1.