scripted

Volume 17, Issue 2, August 2020

Between a rock and a hard place: owners of smart speakers and joint control

*Silvia De Conca**

DOI: 10.2966/scrip.170220.238

Abstract

The paper analyses to what extent the owners of smart speakers, such as Amazon Echo and Google Home, can be considered joint controllers, and what are the implications of the household exemption under the GDPR, with regard to the personal data of guests or other individuals temporarily present in their houses. Based on the relevant interpretations of the elements constituting control and joint control, as given by the Art. 29 Working Party and by the European Court of Justice (in particular in the landmark cases *Wirtschaftsakademie*, *Jehovah's Witness*, *Ryneš*, and *Fashion ID*), this paper shows how the definition of joint control could be potentially stretched to the point of including the owners of smart speakers. The purpose of the paper is, however, to show how the preferred interpretation should be the one exempting owners of smart speakers from becoming liable under the GDPR (with certain exceptions), in the light of the asymmetry of positions between individuals and companies such as Google or Amazon and of the rationales and purposes of the GDPR. In doing so, this paper unveils a difficult balancing exercise between the rights of one individual (the data subject) and those of another individuals (the owner of a smart speaker used for private and household purposes

only).

Keywords
Joint controllers; smart speakers; data protection; vocal assistants; Google; Amazon

* PhD researcher, Tilburg Institute for Law, Technology, Markets, and Society (TILT-LTMS), University of Tilburg, Tilburg, The Netherlands, s.deconca@tilburguniversity.edu

1 Introduction

The European regime for personal data protection relies, among others, on assigning rights and duties to three main actors: i) the data subject, that is the (identified or identifiable) natural person whose personal data are being collected and processed; ii) the controller, the natural or legal person (including public entities and authorities) which determines the *whys* and *hows* of the processing of said personal data; and finally iii) the processor, the natural or legal person (including public entities or authorities) carrying out the processing on behalf of the controller.[1] The above-mentioned distinction was originally made based on the approach that processing was organized almost as a chain-of-assemblage or an industrial process. In practice, however, there have been many cases in which the three roles have partially overlapped, with data subjects or processors becoming also controllers. Factual circumstances have given life to the idea of pluralistic control, later synthetized in the GDPR as joint controllership, as will be explained more in details in part 3 below. Under pluralistic or joint controllership, multiple parties can be considered controllers and are, as such, subjected to the set of duties established by the GDPR.

This paper analyses if, and how, the owners of smart speakers powered by intelligent vocal assistants, such as Amazon Echo (powered by Alexa) and Google Home (powered by Google Assistant), can be considered joint controllers under the GDPR with regard to the personal data of guests or other individuals temporarily present in their houses.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. Hereinafter GDPR.

After a brief overview of how smart speakers and intelligent assistants work, part 3 will explain what the current definitions of controller, separate and joint controllership are, based on the GDPR but also on the relevant case law and guidelines issued under the previous regulatory regime, when still applicable. Part 4 will then explain how the current landscape shapes the roles that an owner of a smart speaker can assume under the GDPR: Data Subject and de facto separate controller. The role of the household exemption in relation to owners of smart speakers will also be discussed in part 4. Finally, in the conclusions, I will explain why the preferred interpretation should be the one exempting owners of smart speakers from becoming liable under the GDPR (with certain exceptions), also in the light of the reality of the position of individuals vis-à-vis big companies and of the purposes and intentions of the European legislators.

2 Technological background: What are smart speakers and what do they do?

Devices like Google Home and Amazon Echo are often referred to as smart speakers. The result of crossbreeding Internet of Things (IoT), Artificial Intelligence (AI), Networked Robotics, Domotics, and Ambient Intelligence, these small items of furniture have significantly gained popularity in the last two years in both the United States and Europe.[2] Smart speakers can be connected to a plethora of Internet-connected devices, which can be controlled through them: from smart TVs and fridges to smart locks, thermostats, switches and lightbulbs, and even to smart mattresses, coffee machines, adult toys, toothbrushes, closet

[2] See, for instance, the U.S. Smart Speaker Adoption Report 2019 compiled by Voicebot and Voicify, available at https://voicebot.ai/smart-speaker-consumer-adoption-report-2019 (accessed 28 July 2020).

organizers, dishwashers, and security cameras.[3] At the centre of this network of inter-connected devices stands the intelligent vocal assistant 'contained' by the smart speaker. The assistant represents both the voice with which users interface, and the software carrying out the tasks requested by the owner or another user. The very core of the smart speaker is, therefore, the assistant, the software capable of carrying out all the actions requested by the users.

From now on, the general term smart speaker(s) will be used, with the caveat that, for the purposes of this paper, this term refers to the combination of both the physical embedding (the speaker) and the software (the vocal assistant). With regard to the individuals interacting with smart speakers, the term owner will be used, even though arguments developed in this paper with regard to the qualification as controller can also be replicated for those users who do not legally own the smart speaker (in most cases).

Smart speakers collect data from their own sensors as well as the sensors present on the connected devices and process them in Cloud. In particular, with a procedure that appears similar for both Amazon and Google, the very first activation of the smart speaker coincides with the request to download on the user's phone the relating app. Via the app, the user is asked to consent to both the Terms and Conditions and the Privacy Policy relating to the vocal assistant and synch it with pre-existing accounts (or create a new account if necessary). From that moment on, any user can wake up the assistant using a trigger word, followed by the request for a task or by a command. Starting from a fraction of second before the trigger word, until the completion of the task requested, the smart speaker streams and records everything in Cloud, where it processes the

---

[3] Michael Simon, "Google Assistant works with over 5,000 smart devices, but Alexa is far in the lead with 12,000" (*Tech Hive*, 03 May 2018), available at https://www.techhive.com/article/3269825/google-assistant-5000-smart-devices.html (accessed 11 July 2019).

data and keeps logs of the recorded requests. The logs can be accessed via the app and deleted or, in the case of Alexa, a vocal instruction can be given to the assistant to delete the logs.[4] The information collected via the smart speaker and the connected devices is processed together with information coming from other sources (such as the purchase and Internet surfing history connected to the Amazon, Google, or even other accounts of the users), and other databases. The additional information deriving from said processing is then used for, according to the Privacy Policies of the devices: fulfilling the commands, personalising the experience, improving the natural language processing capabilities of the assistant, advertising, marketing and other business-related purposes.

Two additional elements should also be taken into consideration. One, particularly relevant for the purposes of this paper, concerns voice-matching. Amazon allows to create a general profile that associates multiple devices to the same house (called household profiles). Within the household profiles, individual profiles for each adult living in the house can be created. Amazon expressly states that voice profiles cannot be created for children. This, however, does not mean that children cannot use the smart speaker: they can request things to the device, which will comply, but no personal profile can be created for them, therefore the various requests will be recorded but not associated to an identity.[5] Each profile can then be connected to a voice that Alexa learns via a specific

---

[4] Jacob Kastrenakes, "Amazon now lets you tell Alexa to delete your voice recordings" (*The Verge*, 29 May 2019), available at https://www.theverge.com/2019/5/29/18644027/amazon-alexa-delete-voice-recordings-command-privacy-hub (accessed 11 July 2019).

[5] Please note that, at the time of writing, the U.S. Federal Trade Commission has started an investigation into Amazon for alleged violations of the Children's Online Privacy Protection Act (COPPA) with regard to a specific smart speaker, the Echo Dot, marketed as kids friendly. See, for instance, Makena Kelly, "Amazon's kid-friendly Echo Dot is under scrutiny for alleged child privacy violations" (*The Verge*, 09 May 2019), available at https://www.theverge.com/2019/5/9/18550425/amazon-echo-dot-kids-privacy-markey-blumenthal-ftc (accessed 26 June 2019).

function. Similarly, Google Assistant has a voice-matching function that allows users to be registered with a certain device and matched with their voices. In this way, the assistant recognises from the voice who is interacting with it, and only provides the content relating to his or her profile. This is particularly relevant for functions such as emails, messages, reminders, alarms, but also with regard to preferences concerning music or news. Google Home even has a guest mode that can be enabled by one of the registered users, thanks to which users can cast content through Google Home (via a Chromecast). Children can be associated to a voice profile, but mandatorily with the authorisation of an adult, and their profile is then subject to limitations, such as the impossibility to play YouTube videos or make online purchases.[6] Google Home also keeps the voices it cannot match with a profile into a separate log which can be accessed and, in case, deleted by the owner or one of the registered profiles.[7] Both devices also present a mute button, which the owners can push to prevent the device from listening at all (including searching for, and responding to, the wake word).

Finally, it should be pointed out that the assistants support applications that represent new capabilities and uses (in the case of Alexa the applications are not called apps, but skills). Skills and apps are available on the usual app stores, and they are often developed by third parties based on an application programming interface (API) made available by Amazon and Google.[8]

---

[6] "Let your child use the Google Assistant on your speaker or Smart Display" (*Google Assistant Help*), available at https://support.google.com/assistant/answer/9071584?hl=en&ref_topic=7658509 (accessed 21 June 2019).

[7] "Guests & Google Home" (*Google Nest Help*), available at https://support.google.com/googlenest/answer/7177221?hl=en (accessed 26 June 2019).

[8] With regard to the third parties developing the apps or skills, questions arise concerning the possible qualification as processor and/or joint controllers together with companies like Amazon and Google. Another, additional, question also concerns whether the Terms and Conditions to which third parties agree in order to use the API qualifies as an agreement

Having established who, or better what, Alexa and Assistant are, part 3 below will provide a summary of the way in which controllership is defined in the context of the GDPR (and the previous Data Protection Directive[9]), focusing in particular on the interpretation of the notion of joint controllership and of de facto pluralistic control (also referred to as separate control).

3 Data controller, separate and joint controllership

The definition of controller established by the GDPR was already introduced in almost exactly the same terms by Directive 95/46/EC, which followed the footprints of the Council of Europe's Convention 108.[10] According to art. 4(7) of the GDPR, the controller is: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". Identifying the controller (as well as the processor) is particularly important in the system of the GDPR because it is based on this qualification that a set of obligations is assigned.[11] Establishing who is the controller of the processing of personal data is, therefore, necessary in order to allocate responsibility.[12] The Article 29 Working Party, in its Opinion 1/2010

according to art. 26 of the GDPR (see part 3 below). The answer to these questions falls, however, outside of the scope of this paper and shall therefore be left for future research.

9 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, OJ 1995 L 281/31. Hereinafter the Data Protection Directive, the Directive, or Directive 95/46/EC.

10 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108, art. 2(d). See also Article 29 Data Protection Working Party, "Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'" (WP169, 2010), p. 8.

11 Andrej Savin, *EU Internet Law* (Elgar European Law, 2nd ed., 2017), p. 271.

12 Opinion 1/2010, p. 4. It shall be noted that while the Opinion refers to the definitions of controller and processor as established by the Data Protection Directive, the circumstance that they have not changed with the GDPR brings the author to affirm the Opinion is still in most of its parts valid today. Some differences concerning joint controllership will be discussed further on.

on the Concepts of "Controller" and "Processor", highlights the three main elements composing the definition of controller: (i) which subjects can be controllers (natural or legal persons, as well as an array of public entities), (ii) the potentially plural nature of control, and (iii) the qualifying circumstances (the determination of the purposes and means of the processing). Since the first one is not relevant for this paper, only the second and third element will be briefly analysed below.

Whether a subject is a controller is established based on a factual evaluation, meaning that any formal appointment of a subject as a controller does not matter if, *de facto*, that subject "*actually* is not in the position to 'determine'"[13] (emphasis added) the purposes and means of the processing. The use of the term 'actually' implies that factual circumstances need to be taken into consideration. Based on the factual circumstances, more than one subject can also be deemed controller, as expressly stated by article 4(7). This circumstance is generally indicated with the term 'joint control'. Under the regime of the Data Protection Directive, some doubts had arisen concerning the concrete application of joint control. Due to the complexity of the processing of data, in fact, different possible forms of joint control had been identified. Joint control could be exercised, for instance, on the entire processing or on one of its stages only, having therefore different controllers for each stage. From the perspective of the purposes, each controller could have different purposes for the same processing of the same data, or, alternatively, all the controllers could share the same purposes. Overall,

[13] Opinion 1/2010, p. 8. Being in an actualy position to determine purposes and means, while used by the Working Party in Opinion 1/2010, has not been further defined nor explained, but appears to be used as a starting point to evaluate the factual circumstances leading to the identification of (joint) controllers. I believe, however, that due to the complexity of the current technological landscape, the debate on the matter would greatly benefit from a more in depth analysis of what it means to *actually* be in the position to determine, by the European legislator and/or the ECJ.

the reality of how the processing takes place can give life to a looser or closer relationship among controllers.[14] Consequently, controllers are not necessarily responsibile for the all the obligations relating to data protection. Under the Data Protection Directive, this created some confusion as to how responsibilities were to be divided among controllers.[15] The Art.29 Working Party, in the abovementioned Opinion 1/2010, highlighted how this could "lead to undesired complexities and to a possible lack of clarity in the allocation of responsibilities. This would risk making the entire processing unlawful due to a lack of transparency and violate the principle of fair processing."[16] To add to the confusion, under the Data Protection Directive it was not fully clear whether joint controllers were subject to joint and several liability.[17] During the roughly twenty years of the Data Protection Directive being into effect, the European Court of Justice (ECJ) has often been addressed to clarify the issues connected to joint control. Two particularly significant cases are also very recent. These cases were issued after the GDPR entered into effectiveness but refer to the Data Protection Directive as they started before the 25th of May 2018: the *Wirtschatsakademie* and the *Jehovah's Witness* cases.[18]

In the first case, the ECJ affirmed that the administrators of a Facebook page are joint controllers together with Facebook for the processing of the data

---

14 Opinion 1/2010, pp. 18-21; *Handbook on European data protection law*, pp. 105-106.

15 Some authors have pointed out that the allocation of responsibilities has not been clarified in the current existing regime either. See Rene Mahieu, Joris van Hoboken, 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 Electronic Commerce Law* 39-59, paras. 26-28.

16 Opinion 1/2010, p. 24.

17 *Ibid*. 22.

18 Respectively, Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] (*Wirtschaftsakademie*), and Case C-25/17, *Tietosuojavaltuutettu v Jehovan todistajat —uskonnollinen yhdyskunta* [2018] (*Jehovah's Witness*).

of the followers of their page.[19] The decision has caught the attention of both experts and the general public, due to the very expanded notion of controller it entails. The Court points out that it goes without saying that the administrators of a Facebook page do not have any negotiating power concerning Facebook's terms and conditions, and that Facebook is the main party responsible for most of the processing. Nevertheless, they select the criteria based on which Facebook will direct a certain target audience to them. Furthermore, by accepting Facebook's offer to provide them with statistical (and as such anonymous) data on the users visiting their page, they indirectly trigger the installing of cookies on the computers of those visiting the page. Administrators of a Facebook page establish a purpose (statistical data) and, with the very creation of the Facebook page, the means too. The request for statistical information acts as a trigger for the use of the cookie (of which users were, furthermore, not informed). The interpretation chosen by the Court in this case expands the definition of controller. As a starting point, the Court affirms that page administrators are "enablers" (or, in the words of the Art. 29 Working Party, "facilitators")[20] of the processing. Building on that, the Court affirms that they are also (partially) beneficiary of the processing, specifying that they can be controllers even if they don't have access to the personal data[21] and don't have any power vis-à-vis the primary controller.

In the *Jehovah's Witness* case, the Court established that a religious institution was a joint controller, together with its members, of the data processing occurring during door-to-door preaching activities. Said activities were carried out by the members, but coordinated, organized and encouraged by

---

19 As well as of non-Facebook users that would open the page via a website, in the specific case the webpage of the Wirtschatsakademie.

20 Opinion 1/2010, p. 11.

21 *Wirtschaftsakademie*, para. 38.

the institution. In the decision, the court stressed how the idea of a plurality of controllers is a given of the data protection regime, and serves the purpose of ensuring an adequate protection to Data Subjects. Furthermore, the Court also confirmed the position of the Art. 29 Working Party in affirming that

> the existence of joint responsibility does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.[22]

For both the Court and the Art. 29 Working Party, therefore, joint control can assume different forms and relate to more loosen or tighter relationships among the controllers.

Following the direction pointed out by both the Art. 29 Working Party and the ECJ, the European legislator has addressed the main issues concerning joint control in the GDPR. Art. 26 of the GDPR, in fact, establishes that whenever two or more parties are involved in the determination of the purposes and means of processing, and are therefore joint controllers, they shall: "determine their respective responsibilities for compliance with the obligations under this Regulation". The allocation of responsibilities shall occur by means of an agreement, which shall: i) be a truthful representation of the factual control and consequent responsibilities of each controller, ii) made available to Data Subjects, and iii) indicate the contact point for the Data Subject. Finally, art. 26 clarifies the nature of the relationship among joint controllers, by establishing in its third paragraph that, no matter the terms of the agreement, "the data subject may

---

[22] *Jehovah's Witness*, para. 66.

exercise his or her rights under this Regulation in respect of and against each of the controllers". The wording of the article confirms that joint controllers are bound by joint and several liability. This implies that the individual controller that has been addressed by the Data Subject can obtain redress from the other controllers for their part of responsibility.

With regard to joint control, van Alsenoy proposes to distinguish the situation in which multiple controllers independently from each other process data, each for their own purpose. He named this circumstance "separate controllers", and explains that the independency of the processing can occur even if the separate controllers transfer the data from one to the other.[23] If, on the other hand, multiple controllers "jointly exercise decisions-making power concerning the purposes and means of the processing" then the terms "joint controllers" or "co-controllers" would apply.[24] According to van Alsenoy, the line between separate and joint control can be blurred by business practices and technology-related circumstances. However, if the controllers pursue different objectives via different means, it is reasonable to consider them separate controllers. This interpretation, while it has not necessarily found any official confirmation by the Courts or administrative authorities, can be seen in line with the wording of art. 26 of the GDPR, which expressly affirms that the multiple actors involved in the processing shall enter into an agreement to determine their share of responsibility. This case would be easily identified as joint control, as stated by the very title of art. 26. It is not clear, however, how art. 26 should apply to the case of de facto multiple control not regulated by an agreement, which would be the case of separate controllers. It is reasonable, based on the previous

---

[23] Brendan van Alsenoy, "Liability under the EU Data Protection law: From Directive 95/46 to the General Data Protection Regulation" (2016) 7 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 271-288, para. 2.3.1.

[24] *Ibid*.

interpretations given to the institute of joint control, that the mere incipit of art. 26 ("Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.") is enough to establish solidary liability among them too.

The third element constituting the definition of controller is the determination of the means and purposes of the processing. This element represents the very core of the definition of controller, and has to be interpreted in a factual way, as mentioned above. Means and purposes shall be intended, in this context, as the "how" (for instance technical and organizational elements)[25] and the "why" of the processing. The interpretation of the word "determine" has, however, raised several doubts in the past, as it has briefly been mentioned with regard to the *Wirtschaftsakademie* case. According to the Art. 29 Working Party, the evaluation revolves around what "level of influence"[26] is necessary to qualify an entity as a controller. It is, at this point, worth noting that, according to the Working Party: "while determining the purpose of the processing would in any case trigger the qualification as controller, *determining the means would imply control only when the determination concerns the essential elements of the means*" (emphasis added).[27] Essential elements, would be, for example and not as an exhaustive list, the kind of data to process and the duration of the processing.[28]

Once the controller(s) have been identified, the GDPR applies unless the processing falls within the so-called household exemption. The household exemption, already existing under the Data Protection Directive regime, is maintained by the GDPR. The household exemption establishes that the GDPR does not apply to the processing of personal data carried out "by a natural person

---

[25] Opinion 1/2010, p. 14.
[26] *Ibid*., p. 13.
[27] *Ibid*., p. 14.
[28] *Ibid*. (emphasis added).

in the course of a purely personal or household activity".[29] Purely personal or household activities is used to identify all those activities falling within the management of a house, of a family, or of personal life.[30] Activities falling within the professional, working, or charitable field do not qualify for the household exemption, regardless of whether they take place in the house or not.[31] A recent decision concerning the boundaries of the household exemption that is particularly relevant in this regard is *Ryneš*.[32] In this case, in fact, the Court established that an individual recording images with a security camera is indeed a controller. For the Court, the circumstance that the security camera was pointing at the entrance of his/her house, therefore at a public space, and not only to the inside of the house, excludes the application of the household exemption. It is evident that the location does play an important role in evaluating whether the processing would fall within the exemption, but that the very nature of the activities itself must nevertheless be personal or familiar.[33]

Recital 18 of the GDPR, following the suggestions elaborated by the ECJ and the Art. 29 Working Party during the previous decade, expands the scope of the household exemption to include not only traditionally private activities such as correspondence, keeping a diary, and the holding of addresses, but also "social networking and online activity undertaken within the context of such activities."[34] While the recital does not elaborate more in detail on the topic, it is reasonable to affirm that, based also on the position of the Art. 29 Working Party,

---

29 GDPR, art. 2, para. 2(c).

30 Art. 29 Data Protection Working Party, "Opinion 5/2009 on Online Social Networking" (WP 163, 2009), p. 3.

31 Handbook on European data protection law, p. 103.

32 Case C-212/13 *Ryneš v Úřad Pro Ochranu Osobnich Údajů* [2014] (*Ryneš*).

33 It should be noted that in *Ryneš*, the existence of a legitimate interest (safety and security) of the individual and the family could still be evoked to justify the processing without the necessity to require the consent of the grabbed individuals.

34 GDPR, Recital 18.

not all online and social network activities qualify for the household exemption. According to Opinion 5/2009 on social networking activities, in fact, three circumstances shall be analyzed in order to assess whether activities on a Social Network are 'purely personal or household'. From the point of view of the purpose of the use of a Social Network, acting on behalf of a company or association, or acting towards "commercial, political or charitable goals"[35] excludes the application of the exemption. From a more formal perspective, the use of an 'open profile' also excludes the application of the household exemption.[36] Having an open profile means that the user of a Social Network does not limit the fruition of the content to a contact list of known users (such as family and friends), but opens the content to every single user of the Social Network, including non-contacts, or makes it indexable by search engines. On the same topic, it should also be considered that for the Art. 29 Working Party the amount of contacts on a Social Media profile matters, since: "A high number of contacts could be an indication that the household exception does not apply."[37] Worryingly, for me as well as for any other Social Network user, what constitutes a high number of contacts has not been clarified.[38]

Normally, the owner of a smart speaker is considered only a Data Subject, as such entitled to the protection of his/her personal data via the rights established by the GDPR. However, doubts arise concerning the role of the owner

---

35 Opinion 5/2009, p. 6.

36 Case C–345/17 *Buivids* [2019], para. 43.

37 *Ibid*. See also, Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003], para. 47.

38 While art. 2 and recital 18 of the GDPR and the analysis of the Working Party offer some more guidance respect to the Data Protection Directive, the concept of "purely personal or household activity" applied to social network platforms still presents several unclear elements and is object of debate. For an analysis of the situation before the GDPR, but still in part relevant nowadays, see Brendan van Alsenoy et al., "Social networks and web 2.0: are users also bound by data protection regulations?" (2009) 2(1) *Identity in the Information Society*, 65–79; Patrick van Eecke and Maarten Truyens, "Privacy and social networks" (2010) 26(5) *Computer Law & Security Review* 535–546.

of a smart speaker vis-à-vis those individuals that might come into contact with said devices inside the home of the owner: guests, occasional third parties, or domestic helpers. Personal Data of temporary guests, in fact, can be recorded by the smart speaker in two ways. Guests can be recorded by accident, as background noises, or if they decide to use the smart speaker in the first person, for example by requesting the assistant to play a song, find information online, look for a take away restaurant, and so on. In the first case the smart speaker would be activated by the owner, and the voice of the guests would be processed in order to distinguish the owner's order from the background noise and avoid mistakes of the assistant. In the second case the guest would voluntarily awake the device to request something.[39] Part 4 below analyzes whether in such cases the owner of a smart speaker can be considered also a controller, based on what has been discussed so far.

4 "Alexa, am I a data controller?"

In order to evaluate whether the owner of a smart speaker can be qualified as controller, we should consider whether the conditions explored in part 3 are met. In order to do so, after having acknowledged the existence of the requirement of legal or natural persons as controllers, this part will focus on two possible interpretations of the element of control. In particular, this part will focus on the relationship between owners of smart speakers and the producers. Subsequently, the household exemption will also be discussed. Since both natural and legal

[39] The latter case can be seen as similar to that of a guest asking to use the Wi-Fi connection at someone's house. In both cases the owner of, respectively, the smart speaker or the Internet connection makes available to the guests technologies that collect their personal data. In the case of the Wi-Fi access then the processing would relate to the activities of the ISP as well as any other service the guest would make use of while online. In the case of smart speakers, the processing would entirely be carried out by the provider of the assistant (Amazon, Google) and/or the third parties that manage the skills or apps.

persons qualify to be controllers, this constituting element of control is easy to match in the case of an owner of a smart speaker. As per the second element, the possible plurality of actors, the complexity of AI and the IoT, especially when combined, makes the existence of separate and joint control particularly common.[40] It might, therefore, happen that, besides the producers of a smart speaker, and apps/skills developers, other subjects might be considered controllers. However, which part of the processing does the owner or the user of a smart speaker have *actual* control over? The less likely hypothesis is that the control of the owner is on the entirety of the processing, with a congruence of his/her purposes and means with the purposes and means of, for instance Amazon, Google, or the third parties providing the apps and skills. Due to the way these devices work, in fact, it is almost impossible for the owner to have control over the purposes of the processing. The technologies behind smart speakers are owned by the companies providing the goods and services, and are often protected by Intellectual Property or other rights. The only part on which the owner might have a form of control is whether activating the device, instead of using the mute button to prevent the device from listening, once the guests are in the house. This, however, could be interpreted in an extensive manner as to integrate the first stage of the processing: the data collection. The devices record and store every sound happening within the range of their sensors for the entire duration of a task, including background noises and conversations. In the case of Google Home, it has been explained before how it even keeps the recordings of non-identified users in a separate log. Furthermore, even if a task isn't ordered, they constantly scan the environment looking for the wake word, immediately

[40] Jenna Mäkinen, "Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things" (2015) 24(3) *Information & Communication Technology Law* 262-277, p. 272.

deleting the sounds scanned, but nevertheless initially collecting and processing them even if for very short fractions of time. These circumstances imply that the voice or other personal data of guests are collected and, sometimes, even further elaborated. This constitutes processing. Similarly to the *Wirtschaftsakademie* case, therefore, it could be argued that the owner works as a 'facilitator' that triggers the collection by activating and not muting the device (which would be a way to prevent or interrupt the processing).[41] It should also be reminded at this point how, in order to be a controller, a subject needs not have access to the personal data processed.[42]

Having established that there is a stage which the owner of smart speakers can have control on, whether said control includes some or all of the purposes and means of the processing constitutes the third element. With regard to the means, an extensive interpretation of the provisions of the GDPR could consider that the choice of the means occurs when the owner chooses the smart speaker. In this interpretation, the smart speaker would represent the means for the collection stage of the processing. Obviously, the means for the stages of the processing occurring in Cloud would be under the sole control of the producers/providers. These latter, similarly to Facebook in the *Wirtschaftsakademie* case, would be the primary controllers due to the extensive decisional power they exercise.[43] This, however, leaves room to the possibility that the owner of the smart speaker is not a controller. It has been explained above that the decisional power over the means only qualifies as integrating control when it concerns the "essential elements", such as which data are processed, and for how long. It can be debated whether deciding simply which

41 *Wirtschaftsakademie*, Opinion of AG Bot, para. 56.
42 *Ibid.*, para. 38.
43 *Ibid.*, para. 73.

device is in use, and when, can count as an essential element of the means. With regard to the purposes, it is worth repeating that their determination is enough, in any case, to appoint the role of controller on a subject.

One interpretation, also quite extensive, could be that the purposes are decided by the owner based on which task and, therefore, which skill or app is activated. This reconstruction does not seem to match with the reality of the processing, however. Let's take the case of guests being accidentally recorded as background noise. If the owner of a smart speaker wants to play some music, the owner does not want to process the conversation happening in the background. The recording is not connected nor functional to the purpose of playing a song. It is, as said, accidental and does not serve any purpose of the owner. Let's consider instead the other possible option, that the guests are recorded for the fraction of a second while the device searches for the trigger word. This function is not activated by the owner and it might require a stretch to consider the purpose of finding the wake word as a purpose established by the owner. On the opposite, it is undebatable that the producers of the smart speakers and their apps determine the purposes for the processing, and determine how the technology works. It can be debated whether the owner has a factual (actual) decisional power over them, to the point of become a controller.[44]

Even considering the extensive interpretations of the requirements necessary for the owners of smart speakers to become separate controllers, for

[44] This approach appears in line with that adopted by other scholars with regard to users of social network platforms abiding to these latter's terms and conditions and the qualification as controllers. See the abovementioned Brendan van Alsenoy et al., "Social networks and web 2.0: are users also bound by data protection regulations?" (2009) 2(1) *Identity in the Information Society* 65–79; Patrick van Eecke, and Maarten Truyens, "Privacy and social networks" (2010) 26(5) *Computer Law & Security Review* 535–546.

the mere collection stage and, possibly, only with regard to the means, it should be verified whether the household exemption applies.

There are, currently, thousands of apps or skills available for Amazon Echo and Google Home.[45] The capabilities of these devices range from activating other devices inside the home, such as light switches, appliances, locks, or indeed security cameras, to reading the news, telling the weather forecast, reading aloud emails and messages, taking photographs, sending email and messages, finding recipes, keeping a list of the groceries, playing songs, buying online, or posting content on Social Networks. The vast majority of these capabilities can be reasonably catalogued as personal, family, or household related activities. With regard to activities carried out online or on Social Networks, according to Recital 18 of the GDPR they would also fall within the household exemption. The exception would be if they are carried out for commercial,[46] political, or charitable purposes or the Social Network profile of the owner is open. In the latter case the actions of the owner would be considered as making information available freely on the Internet. Doubts could also arise based on the number of contacts of the owners on the Social Network platforms used.

A particularly grey area might be the data of personnel hired to work inside the house, for instance for cleaning or maintenance. Whether the accidental collection of their data might fall within the household and personal affairs, remains unclear.

---

45 Greg Sterling, "Google Action vs. Alexa Skills is the next big App Store battle" (*Search Engine Land*, 19 February 2019), available at https://searchengineland.com/google-actions-vs-alexa-skills-is-the-next-big-app-store-battle-312497 (accessed 11 July 2019).

46 A hypothesis which is not particularly remote. Imagine the case of a fashion blogger using Echo Look, a device made to organize the closet and take pictures of outfits, to take the picture of a certain outfit and post it on his/her Instagram account, through which most of his/her revenues come from.

Furthermore, based on the *Ryneš* case it could be argued that the household exemption would not apply if the collection of the data does not occur within the house, but outside, in a public space such as the outside street or communal areas of an apartment building. It shall be pointed out in this regard that, while the devices are in most cases located inside the house of the owners (according to Google in the 75% of cases in the living room of the owners),[47] their sensors could be also located on the outside (such as security cameras, which would integrate a case extremely similar to the abovementioned *Ryneš*). The sensors could be powerful enough to catch sounds from outside the house of the owner (for instance from neighboring apartments or the hall outside the entrance of the house).

In the latter cases, the fact that the collection would occur outside of the household environment could be enough to exclude the application of the household exemption, making the owner a separate controller liable under the GDPR (if the extensive interpretation of the means and purposes is applied too).

5 Conclusions: a plea against the extensive interpretation of art. 4(7) GDPR

As it frequently happens, especially in the field of Data Protection, the question of whether the owner of a smart speaker should be considered, besides a Data Subject, also a controller vis-à-vis guests or other people temporarily in the house, should be answered on a case by case basis. As this paper has explained, there are several factors to be considered in order to appoint the role of controller and to assess the applicability of the household exemption.

---

[47] Sara Kleinberg, "5 ways voice assistance is shaping consumer behavior" (*Think with Google*, January 2018), available at https://www.thinkwithgoogle.com/consumer-insights/voice-assistance-consumer-experience/ (accessed 11 July 2019).

Some care should be taken in interpreting the requirements established to identify the controller. In this regard, particularly relevant is the way in which control over the means and purposes is interpreted. Doubts might arise on whether the choice of having and using the smart speakers *per se* constitutes control over the means through which the data are collected. It is also debatable whether the choice of which app to activate might constitute control over the purposes for which the collection is carried out.

In this regard, I want to put forward some arguments against the extensive interpretation of the definition of controller in the case of owners of smart speakers.

The overall premises, highlighted by both the ECJ and the Art. 29 Working Party with regard to control, are that the assessment shall be made based on the factual conditions of the processing, and the controller shall have actual decisional power over certain fundamental aspects of the processing. However, both the ECJ and the Art. 29 Working Party have often chosen not to consider as significant a very concrete and factual condition that can affect the autonomy of the prospective controller: the unbalance of power between certain providers of services or products, such as Facebook, Google, or Amazon, and smaller private parties. This unbalance is even bigger in the case of non-professional individuals. In Wirtschatfsakademie, the Court follows the idea of the late Advocate General Bot that once a person has accepted terms and conditions on which he or she has absolutely no negotiating power, then nevertheless the person "may always be regarded as a controller, given his actual influence over the means and purposes of the data processing."[48] Said influence merely being choosing to use the service instead than not using it. On the one hand, the primary role of certain providers

[48] *Wirtschaftsakademie*, Opinion of AG Bot, para. 60.

and producers is recognized. The impossibility of individuals to negotiate or affect any aspect of the service or product, is also acknowledged. On the other hand the *actual influence* on the processing, necessary to qualify the controller, is deemed to be all enclosed in the mere choice of not walking away from a service or product (which, in many cases, comes with significant social and peer pressure).[49] In the *Wirtschaftsakademie* case the position of administrators of a Facebook page, especially for a business, can make said reasoning in part justifiable. However, in the context of that case both the Court and the Advocate General affirm that the lack of power of individuals vis-à-vis the providers or producers does not exclude control in general. This is a dangerous formulation, and it should not be interpreted as opening the way to its application to other cases in which there is a power imbalance between potential controllers. To justify this extensive interpretation, the Advocate General affirms that holding more subjects liable, regardless of who those subjects are and what is their actual power on the processing, can have a positive ripple effect on big providers and producers. It could push them to a more careful compliance with the GDPR.[50] I don't find this justification very convincing. Besides being unsupported, it also fails to consider how holding multiple actors liable fragments the liability of these primary controllers, and creates the possibility for dangerous loopholes. Overall, it does not really add any particular benefit to a damaged party seeking for redress, at least from the monetary perspective, since individuals most likely have a limited patrimony if compared to companies and corporations.

If we consider the position of an individual owning a smart speaker, the unbalance of power vis-à-vis the producers and providers becomes even more

---

[49] Anabel Quan-Haase and Alyson L. Young, "Uses and Gratifications of Social Media: A Comparison of Facebook and Instant Messaging" (2010) 30(5) *Bulletin of Science, Technology & Society* 350-361, p. 357.

[50] *Wirtschaftsakademie*, Opinion of AG Bot, para. 74.

significant. Interpreting in an extensive manner the requirement for control and, consequently, deeming the owners of said devices controllers together with companies such as Amazon or Google with regard to guests (equating owning a product to being 'facilitators'), would mean to ignore the factual circumstances and ignore the necessity for actual decisional power. This is even more so if we consider average users might not even be fully aware of the functioning of the smart speakers. Considerations concerning the connection between effective decisional power and responsibility, which are already being discussed extensively with regard to consent in the GDPR, should be part of the discussion with regard to control too. It is, in this sense, comforting that a more moderate position is being taken by Advocate General Bobek in the context of the *Fashion ID* case. The case concerned the possible joint controllership between a website and Facebook due to the fact that the first has a plug-in on its website to automatically "like" the relating Facebook page of the company. In his Opinion the Advocate General has already taken a position against an extensive interpretation of the definition of controller, highlighting that attributing responsibility to a subject that is not in control of the processing would be unjust, and it would not help the Data Subject.[51] According to Advocate General Bobek, in fact, if the alleged co-controller does not have any actual control over the processing, the Data Subject cannot see his/her rights enforced. If, for instance, the Data Subjects exercises the right of access against a controller without actual control, this latter will not possibly be in the position to provide the Data Subjects with his/her personal data… because the controller does not even have availability of them.[52] It shall be pointed out that AG Bobek overall did not

---

[51] Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* [2018], Opinion of AG Bobek, para. 91.

[52] *Ibid*., para. 84.

exclude the existence of joint control for the specific case of *Fashion ID*. In its final decision the Court, following the path of the *Wirtschaftsakademie* decision, confirmed that Fashion ID is joint controller together with Facebook, but only for the initial stage of the processing.[53] However, the Advocate General appears to share the same concerns with regard to expanding the definition of control in an indiscriminate and generalized way.

Furthermore, in interpreting the requirements for the existence of pluralistic control, particular care should be put with regard to the sharing of purposes and means. In the case of the owners of a smart speaker, the purpose is using the device. As explained above, such use gives life, often accidentally, to the collection of data of the guests. However, the owner does not *need* nor *want* the data of the guests in order to achieve the purpose. This is a matter which, in other contexts, would be dubbed collateral damage. On the other hand, the producers and providers of the smart speaker do need all the data available in order for the device to properly function (and for other purposes, such as marketing, statistics, and so on). The possibility of separate, independent control could still be open, but in this regard the arguments made above with regard to the actual control of the individual owners and the power unbalance should be considered.

It should be noted how the very same Art. 29 Working Party has also held in the past, with regard to owners of Internet of Things devices, a more moderate position. In its Opinion on the matter, in fact, after having considered privacy and Data Protection implications of the IoT, the Working Party concluded that:

> Users of IoT devices should inform non-user data subjects whose data are collected of the presence of IoT devices and the type of collected data. They

[53] Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* [2019].

> should also respect the data subject's preference not to have their data collected by the device.[54]

This indication has been followed by Google, which on the website entirely dedicated to Google Home expressly recommends owners to inform their guests of the presence of the device and make avail of the mute button.[55]

From a systemic perspective, besides being more in line with the element of the factual evaluation of the position of a controller, the approach I propose is also consistent with the European system of data protection as a whole. The GDPR has, in fact, as purposes protecting individuals and fostering the internal market.

In terms of fostering the internal market, it could even be argued that making the owners of smart speakers controllers risks to have a chilling effect on the market, with some potential buyers opting not to purchase the devices to avoid the risk of being sued by angry friends or neighbors.

Contrary to the abovementioned opinion of Advocate General Bot in the *Wirtschaftsakademie* case, I believe that including the owners of smart speakers among the controllers does not grant a higher degree of protection to individuals. It does not offer higher protection to the guests, since the positive ripple effect has so far not been proved and appears to be more wishful thinking than reality. Following the *Wirtschaftsakademie* and *Fashion-ID* cases, in fact, so far no change appears to have occurred in the behaviour of the principal controller, Facebook. This latter has not modified the functioning of its like buttons or cookies. The additional responsibilities assigned to small, local enterprises which mostly

---

[54] Art. 29 Data Protection Working Party, "Opinion 8/2014 on Recent Developments in the Internet of Things" (WP 223, 2014).

[55] "Guests & Google Home" (*Google Nest Help*), available at https://support.google.com/googlenest/answer/7177221?hl=en (accessed 26 June 2019).

necessitate Facebooks' services in order to be visible and gain potential customers do not appear to have put pressure on Facebook. This approach actually risks to increase legal uncertainty,[56] due to the fragmentation of the liability that otherwise would entirely lay on corporations (and therefore would keep corporations fully accountable and act as a deterrent too). In the words of Advocate general Bobek:

> Making everyone responsible means that no-one will in fact be responsible. Or rather, the one party that should have been held responsible for a certain course of action, the one actually exercising control, is likely to hide behind all those others nominally 'co-responsible', with effective protection likely to be significantly diluted.[57]

It also does not protect the owners of smart speakers, which are individuals as well as (over-burdened)[58] data subjects, and would find themselves projected in a role that affirms them in control, while in reality they do not have any power vis-à-vis the companies providing the devices and the software. In the words of Advocate General Bobek: "no good (interpretation of the) law should reach a result in which the obligations provided therein cannot actually be carried out by its addressees."[59]

The paradoxical nature of this situation emerges more clearly if we draw a parallel with another institute of the law that is often associated with Data

---

56 Mahieu, van Hoboken, Asghari, para. 44.

57 Case C-40/17, Opinion of AG Bobek, para. 92.

58 Lilian Edwards et al., "Data subjects as data controllers: a Fashion(able) concept?" (*Internet Policy Review*, 13 June 2019), available at https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400 (accessed 14 June 2019). In their article, the authors focus on a different technology, namely personal data stores (PDS). Their argument being particularly PDS-specific, I consider them outside of the scope of this work.

59 Case C-40/17, Opinion of AG Bobek, para. 93.

Protection: product liability.[60] Imagine individual A being sued by another individual, named B, based on product liability. B has been damaged by A's domestic appliance, while B was a guest at A's house. Let's exclude that A has misused the domestic appliance, since the damage was entirely caused by a fault in the product. Within the regime of product liability such claim would have no basis, as it would not be enough that A, by buying and using the product, acted as an enabler or a facilitator of the damage. Why would, then, this reasoning be applied in the case of data processing by another, very evolved, form of domestic appliance?

The final argument in support of my position comes from the system of the law. In the relationship between the owner of smart speakers and the guest, in the case of damages deriving to this latter from the actions or functioning of the device, other legal protections still apply, therefore not leaving the damaged subject without remedies. Civil law protection, such as tort/extra-contractual liability or even criminal law would cover the relationship between the two

[60] I acknowledge that, while the product liability regime falls entirely within private law, Data Protection inherently possesses a double nature of both fundamental right and private law, as abundantly debated by privacy and data protection scholars in the past two decades. I believe, however, that the peculiar double nature of Data Protection does not render a parallel with consumer protection invalid; on the contrary, it makes such parallel possible due to the fact that both regimes can be used as tools to protect a weak party in a bi- or multi-lateral legal transaction and are deployed to regulate horizontal asymmetrical relations (even though the fact that Data Protection insists on a fundamental right makes it apt to be deployed in vertical relations too). As an example, a comparison between Data Protection and institutes of private law (including product liability) has been carried out by M. Paun in "Legal Protection in Consumer Financial Services: Source of inspiration for data protection?" (*Amsterdam Privacy Conference*, Amsterdam, 5-7 October 2018). It could be argued that, unlike product liability, the processing of personal data creates risks for the fundamental rights of individuals, which could be reason enough to grant a strong protection via an extensive interpretation of the role of the controller. Considering, however, that product liability is a tool created having as a starting point situations in which individuals are damaged in their possession or even in their bodily integrity, the underlying and implicit protected interests appear in both data protection and product liability of great importance.

besides the regime of the GDPR.[61] In other words, the system of the law already has it covered, at least with regard to the remedies for damages.[62]

Regardless of the qualification of the owner as controller, it has been pointed out how the qualification of online and Social Network activities as purely personal or domestic, as well as the positioning within the domestic environment, make it reasonable to apply the household exemption in most cases. However, circumstances such as the openness of the Social Network profile or of other platforms on which the data might be published via the smart speakers, the number of contacts the owner has on a Social Network, or possible commercial, political or charitable purposes, might exclude the application of the household exemption. Similarly, if some of the sensors of the smart speakers collect data from outside of the house, from public spaces or spaces belonging to other individuals (such as the neighbors), the household exemption would likely not apply. In most of these cases, however, (the only exception possibly being the carrying out of commercial, political, or charitable activities) the arguments against an extensive interpretation of the notion of controller still stand.

In conclusion, while an extensive application of the GDPR can help tackling the challenges that arise from new, complex technologies, the expansion

---

[61] As stated by the Art. 29 Working Party for the case of damages deriving from Social Networking activities. See Opinion 5/2009, pp. 6-7.

[62] In this regard it shall be noted how the regime of joint and several responsibility of GDPR's joint control might appear to offer an easy point of contact to a data subject. By activating the remedies vis-à-vis the owner of a smart speaker, a data subject might appear to have an advantage: starting a procedure in a familiar language, in one's own country. This, however, is valid in any case, since art. 77 GDPR gives data subjects the right to start a procedure before the Data Protection Authority of the country they belong to, or the country of habitual residence, or in which the workplace is located, or where the violation of the rights has occurred, in the official language of said country. Indeed, I acknowledge that the procedure would then be not against a faceless company but against an individual. I do not believe this is a reason good enough to burden individual data controllers who own and use a smart speaker but, as I explain in the article, have limited to no control over its functioning, with a responsibility so big as the one of data controller.

should be done reasonably and carefully. In the case of the extensive interpretation of the concept of controller, careful consideration should be given to *all* factual circumstances, including the palpable unbalance of power between the parties involved, especially to avoid undesired consequences which would result in not obtaining the highest possible degree of protection of individuals, *all* the individuals involved (included the individual owning a smart speaker and using it for private and household purposes only). The case of the owner of a smart speaker is, in this sense, a perfect example in which the role of (joint)controllers should be left only for those actors, such as the producers and providers of the hardware and software, within which lies the real and concrete decisional power concerning means and purposes.

So far the case law concerning joint control has seen peculiar actors being appointed controllers side-by-side with big corporations providing the very service which originated the processing. In the above-mentioned Wirtschaftacademie and Fashion-ID, in fact, the joint controllers were all small and mediums businesses. While the unbalance of power could be understandably disregarded in the case of companies/businesses being joint controllers, there are additional elements that differentiate an individual owning a smart speaker. *In primis,* the individual owner most frequently uses the smart speaker for private and family life. From the perspective of the technological and commercial reality, most non-professional individual users lack the knowledge, expertise and (legal and material) capability to affect the processing and the technology that is in a sense imposed on them. I believe these factual elements can guide the courts and, possibly, the European legislator in separating individual owners from producers of smart speakers. In other words: let's not make the owner of an Echo or Home a controller for the mere fact of putting guests within the range of their sensors.