Exploring the limits of joint control: the case of COVID-19 digital proximity tracing solutions

by **Stephanie Rossello and Pierre Dewitte**[*]

Abstract: Referring to the judgment of the CJEU in Fashion-ID, some scholars have anticipated that, "at this rate everyone will be a [joint] controller of personal data". This contribution follows this arguably provocative, but not entirely implausible, line of thinking. In the first part of the article, we highlight the ambiguities inherent to the concept of "joint control" and confront them with those pertaining to the notion of "identifiability". In the second part, we investigate the effects of the broad legal test for joint control on the role of the individual user of BLE-based COVID-19 digital proximity tracing solutions. This offers the possibility to examine, at a theoretical level, whether the impact of the broad notion of joint control differs depending on the architecture of the system (i.e. centralized or decentralized). We found out that the strict application of the joint controllership test could lead to unexpected and, most likely, unintended results. First, an app user could, in theory, qualify as a joint controller with a national health authority regardless of the protocol's architecture. Second, an actor could, again in theory, be considered as a joint controller of data that is not personal from that actor's perspective.

Keywords: Joint control; personal data; identifiability; COVID-19; digital proximity tracing; GDPR; decentralisation; centralisation

Recommended citation: Stephanie Rossello and Pierre Dewitte, Exploring the limits of joint control: the case of COVID-19 digital proximity tracing solutions, 12 (2021) JIPITEC 342 para 1

A. Introduction

1 In its opinion in *Fashion-ID*, Advocate General Bobek foresightedly stated that: "When pushed to an extreme, if the only relevant criterion for joint control is to have made the data processing possible, thus in effect contributing to that processing at any stage, would the internet service provider, which makes the data processing possible because it provides access to the internet, or even the electricity provider, then not also be joint controllers potentially jointly liable for the processing of personal data?".[1] Referring to the judgment of the Court of Justice of the European Union ("CJEU") in

[*] Stephanie Rossello is a researcher at the KU Leuven Centre for IT & IP Law, where she is involved in the European Union's Horizon 2020 research and innovation program under grant agreement No 824988 "Machine learning to augment shared knowledge in federated privacy preserving scenarios" (MUSKETEER); Pierre Dewitte is a researcher and PhD candidate at the KU Leuven Centre for IT & IP Law, where he is involved in the KU Leuven-C2 research project "Privacy by design Regulation in Software Engineering" (PRiSE). The authors wish to thank Marie Beudels, Ilaria Buri, Ivo Emanuilov, César Augusto Fontanillo López, René Mahieu and the two peer-reviewers for their insightful feedback on draft versions of this article.

[1] Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV joined parties: Facebook Ireland Limited* [2018], Opinion of Advocate General Bobek ECLI:EU:C:2018:1039, para 74.

Fashion-ID, some scholars, similarly, anticipated that, “at this rate everyone will be a [joint] controller of personal data”.[2] This contribution follows this arguably provocative, but not entirely implausible, line of thinking.

2 More specifically, in the first part of the article, we focus on the legal framework on joint control, by combining the ambiguities inherent to the notion of joint control with those pertaining to the notion of “identifiability” of personal data (section B). Next, we briefly describe and evaluate the scope of the household exemption (section C). In the second part of the contribution, we investigate the effects of the broad legal test for joint control on the role of the individual user of Bluetooth Low Energy (“BLE”)-based digital proximity tracing solutions used in the fight against the COVID-19 outbreak (“COVID-19 apps”).[3] This case-study was chosen because it offers the possibility to examine, at a theoretical level, whether the broad notion of joint control has different consequences depending on the architecture of the software system, i.e. whether it is centralized or decentralized. In relation to a case-study concerning security/privacy preserving edge computing solutions adopted in a smart home with Internet of Things, scholars have argued that the current broad notion of joint control, coupled with the narrow interpretation of the household exemption, may end up “unfairly burdening certain stakeholders in smart homes”,[4] including the smart home user, and “disincentivise uptake”[5] of security/privacy preserving edge computing solutions. We are interested in knowing whether this conclusion could, in theory, also hold true in the case of privacy-preserving decentralized solutions such as those applied in COVID-19 digital proximity tracing. Therefore, after having set out the hypothesis, methodology, objective and limitations of the case-study (section D), we provide an overview of both the centralised and decentralised COVID-19 app ecosystems (section E), and subsequently apply the legal framework sketched out in sections B and C to the said case-study (section F). We then summarise our findings (Section G) and conclude the paper (Section H).

3 Notwithstanding the specific use case, we wish to stress from the outset that the present paper by no means provides a definitive answer as to the allocation of responsibilities for concrete digital proximity tracing solutions adopted in the fight against COVID-19. Neither does it attempt to confirm or deny an existing claim as to the potential role of COVID-19 app users as (joint) controllers. Rather, the analysis aims at illustrating how the lack of a coherent interpretation of key concepts delimiting the material and personal scope of application of EU data protection legislation, such such as the notions of “identifiability” of personal data and “joint controllership”, may have arguably unintended consequences. Consequently, this contribution intends to pinpoint the concepts that need further clarification from the European Data Protection Board (“EDPB”), National Supervisory Authorities, the CJEU and domestic courts.

B. The ambiguous notion of joint control

I. Joint control under the GDPR

4 Article 4(7) General Data Protection Regulation (“GDPR”) provides that 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* […]” (emphasis added). This definition is the same as the one provided in the GDPR predecessor, Article 2 (d) of the Directive 95/46 (“DPD”). The latter provision has been further clarified by the Article 29 Working Party (“WP29”) in its opinion 1/2010 on the concepts of controller and processor[6]—now replaced by the EDPB’s guidelines 07/2020 on the concepts of controller and processor in the GDPR[7]—

[2] Christopher Millard and others ‘At This Rate, Everyone Will Be a [Joint] Controller of Personal Data!’ (2019) 9 (4) International Data Privacy Law 217 <https://academic.oup.com/idpl/article/9/4/217/5771498> accessed 21 April 2021.

[3] The development of these apps in Europe has indeed followed two main technical approaches, the so-called “centralised” versus “distributed” or “decentralised” approach. The technical protocols and accompanying security and privacy risks analyses of some of these COVID-19 apps have been made publicly available and easily understandable to a non-technical audience, including the authors of this contribution. The existence of this publicly available technical documentation rendered this legal analysis possible.

[4] Jiahong Chen and others, ‘Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption’ (2020) 10 (4) International Data Privacy Law 293 <https://academic.oup.com/idpl/article/10/4/279/5900395> accessed 21 April 2021.

[5] ibid.

[6] Article 29 Working Party, ‘Opinion 1/2010 on the concepts of “controller” and “processor” ’(2010) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> accessed 21 April 2021.

[7] European Data Protection Board, ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR’

and by the CJEU in its judgments in the *Fashion ID*, *Wirtschafstakademie* and *Jehovah's Witnesses* cases. We start our analysis by investigating the object of joint control, *i.e.* the processing of personal data. Then, we examine the remaining building blocks of that definition and map the ambiguities surrounding the concept of joint control.

II. The notion of personal data as a gatekeeper

1. The legal test for identifiability

5 Before proceeding with the allocation of responsibilities, it is crucial to identify whether there is a processing of "personal data". Article 4(1) GDPR defines personal data as "any information relating to an identified or identifiable natural person [...]". Data that do not relate to an identified or identifiable individual will be considered anonymous and fall outside the scope of the GDPR. While other elements of this definition can also potentially pave the way for an extensive interpretation of personal data,[8] we limit the scope of our analysis to the controversial notion of "identifiability".

6 Recital 26 GDPR provides that "to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly". In turn, according to Recital 26 GDPR, "to ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors such as the costs of and amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". As already discussed at length by several authors,[9] there is considerable legal uncertainty on the standard of identifiability set forth by the GDPR. This uncertainty concerns, among others, the perspective from which the nature of the data is to be assessed (the so-called "absolute" versus "relative" approach to personal data)[10] and the risk of (re-)identification that can be tolerated without data being considered as relating to an "identifiable individual" (the so-called "zero-risk" versus "risk-based" approach).[11]

2. Absolute and zero-risk versus relative and risk-based approach

7 Under the absolute approach, if *anybody* is theoretically able to identify a data subject on the basis of the data at issue (potentially combined with auxiliary information), that data would qualify as personal data.[12] Under the relative approach, the likelihood of re-identification would only be assessed from the perspective of a more *limited* number of parties, *i.e.* the controller or a third party that is reasonably likely to approach or be approached by

<https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf> accessed 13 July 2021. It is worth noting that the final version of these guidelines have been issued at the very end of the publication process. In light of the above, we have done our best to reflect the modifications and refinements implemented following the public consultation period.

[8] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 (1) Law, Innovation and Technology, 48–59 <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> accessed 21 April 2021.

[9] See for a recent overview of the uncertainties surrounding the identifiability test set out in Recital 26 GDPR: Michele Finck and Frank Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 (1) International Data Privacy Law, 14–19 <https://academic.oup.com/idpl/article/10/1/11/5802594?login=true> accessed 21 April 2021; Purtova (n 8) 46-48 <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176>; Manon Oostveen, 'Identifiability and the Applicability of Data Protection to Big Data' (2016) 6 (4) International Data Privacy Law 299, 304–306 <https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipw012> accessed 21 April 2021; Worku Gedefa Urgessa, 'The Protective Capacity of the Criterion of "Identifiability" under EU Data Protection Law' (2016) 4 European Data Protection Law Review 521 <http://edpl.lexxion.eu/article/EDPL/2016/4/10> accessed 21 April 2021.

[10] Finck and Pallas (n 9) 17–18; Gerald Spindler and Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 (2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 165-166 <https://www.jipitec.eu/issues/jipitec-7-2-2016/4440> accessed 21 April 2021.

[11] Finck and Pallas (n 9) 14–16; Sophie Stalla-Bourdillon, 'Anonymous Data v. Personal Data a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016) 34 Wisconsin International Law Journal 286 ff < https://repository.law.wisc.edu/s/uwlaw/media/77051> accessed 21 April 2021; Sophie Stalla-Bourdillon, 'Anonymising Personal Data: Where Do We Stand Now?' (2019) 19 (4) Privacy & Data Protection Journal 5 <https://www.immuta.com/anonymizing-personal-data-where-do-we-stand-now-2/> accessed 21 April 2021.

[12] Spindler and Schmechel (n 10) 165.

the controller.[13] Under a zero-risk approach, data would be personal as soon as there is a risk of re-identification, no matter how negligible, whereas, under a risk-based approach, this would be the case only if identification is considered to be reasonably likely in light of the efforts it would require in terms of factors such as costs, time, technological means and expertise.[14] Although the reasonably likely means of identification standard set out in recital 26 GDPR seems to imply a risk-based approach to personal data, the interpretation of the identifiability criterion by the relevant authorities does not unequivocally point in this direction.[15] Below, we present a selection of the main interpretative guidance on identifiability.[16]

8 In its 2007 opinion on the concept of personal data, the WP29 stated that the "mere hypothetical possibility to single out the individual is not enough to consider the person as 'identifiable'" and stressed that the possibility of identification should be (re-)assessed on a continuous basis, throughout the expected lifetime of the data.[17] What is to be considered "reasonable" is context-dependant.[18] This seems to plead in favour of a risk-based approach. The WP29 also stressed that identifiability should be assessed not only from the perspective of the controller but from the perspective of "any other person".[19] While this might appear as advocating for an absolute approach—and therefore in contradiction with the above—the WP29 clarified that statement in an example related to key-coded personal data used for clinical trials, where the re-identification of patients is explicitly envisaged in the scope of the trial. According to the WP29, key-coded data would be considered personal data for the controllers involved in re-identification, but not for "any other data controller processing the same set of coded data [...], if within the specific scheme in which those other controllers are operating, re-identification is explicitly excluded and appropriate technical measures have been taken in this respect".[20] This, again, seems to favour a relative and risk-based approach.

9 In its later opinion on anonymization techniques, the WP29 appears to have adopted a more radical stance towards the identifiability threshold. There, it stated that the outcome of anonymization—*i.e.* the process through which data becomes anonymous and *a fortiori* non-identifiable—should be" as permanent as erasure" with the aim to "irreversibly" prevent re-identification.[21] Like in 2007, the WP29 stressed that identifiability must be judged from the viewpoint of the controller or any other third person.[22] In a much criticized example,[23] however, it clarified that if a controller provides a dataset with individual travel patterns at event level to a third party after having removed or masked the identifiable data, such a dataset would still qualify as personal data "for any party, as long as the data controller (or any other third party) still has access to the original raw data".[24] Here, the absence of any reference to the likelihood of such re-identification happening seems to imply an absolute and zero risk approach to personal data.[25]

10 Later, the CJEU interpreted the notion of "reasonably likely" means of identification in the *Breyer* case, where it held that a dynamic IP address held by a

[13] See for an example: Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016], Opinion of Advocate General Campos Sánchez-Bordona ECLI:EU:C:2016:339, para 67-68; For further explanation on these approaches see: ibid 165-166; Finck and Pallas (n 9) 17-18.

[14] Finck and Pallas (n 9) 14–16.

[15] ibid. 15-20.

[16] The interpretative guidance presented above relates to recital 26 of the DPD, which contains an identifiability test similar to the one set out in recital 26 of the GDPR and, more specifically, provides that: "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person". Considering the similarity between the test of the DPD and the GDPR and the fact that recital 26 of the GDPR has not been interpreted yet by the EDPB or CJEU, the interpretation provided under the DPD is still relevant at the time of writing.

[17] Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal data' (2007) 15 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 21 April 2021

[18] ibid. 13.

[19] ibid. 19. This mirrors the wording of recital 26 of the DPD which referred to "any other person", not "another person" as recital 26 GDPR.

[20] Article 29 Working Party (n 17) 20.

[21] Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) 6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 21 April 2021.

[22] ibid 9.

[23] Finck and Pallas (n 9) 15; Stalla-Bourdillon, 'Anonymising Personal Data: Where Do We Stand Now?' (n 11) 2.

[24] Article 29 Working Party (n 21) 9.

[25] Finck and Pallas (n 9) 15.

content provider was personal data, even if that provider was not able, by itself, to link the address to a particular individual. The Court considered that, since German law allowed the content provider to combine the dynamic IP address with the information held by the internet service provider under specific circumstances such as cyberattacks, the content provider had a legal possibility to identify the data subject. This legal possibility was considered a "reasonably likely" means to be used. Conversely, the likelihood test would not have been met if identification was "prohibited by law or practically impossible on account of the fact that it requires disproportionate efforts in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant".[26] As such, it seems that the CJEU has embraced a risk-based approach to personal data, since it investigated the actual means of re-identification that were at the disposal of the content provider.[27]

11 As to the perspective from which "identifiability" should be assessed, the opinion of Advocate General Campos Sánchez-Bordona in *Breyer* points to a relative approach. According to him, a reference to "any third party" must be understood as referring to third parties "who, *also in a reasonable manner*, may be approached by a controller seeking to obtain additional data for the purpose of identification".[28] Otherwise, "[...] it would always be possible to imagine the hypothetical contingency of a third party who, no matter how inaccessible to the provider of services on the Internet, could — now or in the future — have additional relevant data to assist in the identification of a user".[29]

12 Like others,[30] we believe that the relative and risk-based approach is the only sensible way to interpret the identifiability criterion. In light of the increasing amount of publicly available information which could potentially be used to re-identify a data subject and the growing body of research disputing the possibility to irreversibly anonymize data,[31] favouring an absolute and zero-risk approach to personal data could *de facto* amount to admitting that almost all data could potentially qualify as personal. This would lower legal certainty and increase the burden on controllers to make sure that the data they collect do not, at any point in time, lead to the potential re-identification of individuals.[32]

III. The components of joint control

1. The notion of controller: a necessary first step

13 As highlighted by the EDPB, "the assessment of joint controllership should mirror the assessment of 'single' control [...]".[33] Before analysing the criteria used to establish joint control, it is therefore crucial to first identify which entities qualify as controllers in their own right. Only then is it possible to examine whether they would qualify as joint, or rather sole, controllers vis-à-vis certain processing operations. As such, the EDPB breaks down the definition of controller into the following building blocks.[34] A controller is the:

- "natural or legal person, public authority, agency or other body" that;
- "determines";
- "alone or jointly with others";
- "the purposes and means";
- "of the processing of personal data".

14 The first building block is self-explanatory for the purposes of this contribution. What needs to be highlighted is that a natural person can also qualify as a controller under the GDPR. As detailed

[26] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779 para 46.

[27] See similarly: Finck and Pallas (n 9) 18; Daniel Groos and Evert-Ben van Veen, 'Anonymised data and the rule of law' (2020) 6 (4) European Data Protection Law, 1-11 < http://edpl.lexxion.eu/article/EDPL/2020/4/6> accessed 21 April 2021.

[28] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016], Opinion of Advocate General Campos Sánchez-Bordona (n 13), para 68.

[29] ibid.

[30] See for authors similarly arguing in favour of a risk-based approach to personal data: Finck and Pallas (n 9) 34–36; Groos and van Veen (n 27); Stalla-Bourdillon, 'Anonymising Personal Data: Where Do We Stand Now?' (n 11).

[31] See authors quoted in Oostveen (n 9) 306, who correctly points out that, due to the recent social and technical developments, the categorization of data as "identifiable" and "non-identifiable" has become more difficult.

[32] See for authors taking a similar stance: Groos and van Veen (n 27); WK Hon, C Millard and I Walden, 'The Problem of "personal Data" in Cloud Computing: What Information Is Regulated?--The Cloud of Unknowing' (2011) 1 (4) International Data Privacy Law 211-228 <https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipr018> accessed 21 April 2021.

[33] European Data Protection Board (n 7) 19.

[34] ibid 9-10.

in section C, this also opens up the possibility for natural persons to rely on the so-called "household exemption" to avoid falling under the Regulation's scope of application.

15 Second, the capacity to "determine", stresses the EDPB, refers to "the controller's *influence* over the processing, by virtue of an *exercise of decision-making power*".[35] As already clarified by the WP29,[36] the EDPB emphasises that such influence can stem from either legal provisions or an analysis of the factual elements surrounding the circumstances of the case. In the case of legal provisions, where a piece of domestic legislation lays down the purposes and the means of a specific (or set of) processing operation(s), the legislator can also appoint the controller or the criteria for its nomination (Art. 4(7) GDPR). This seems to suggest that the possibility for the legislator to allocate responsibilities is conditional upon the determination of the purposes and means of the processing. Those purposes must be explicitly and legitimately specified (Art. 5(1)b GDPR). However, the legislator also has the possibility to add specific provisions for the type of data to be processed and the data subjects concerned, where the processing is based on the performance of a task carried out in the public interest (Art. 6(3) second indent GDPR). Collectively, this prevents the legislator from allocating responsibilities in a vacuum. It also means that the legal designation only covers the processing operations that pursue a set of pre-defined purposes.

16 In the case of contextual analysis, where the law does not explicitly or implicitly allocate responsibility to a certain entity, a factual assessment is required "in order to reach a conclusion as to whether a particular entity exercises a determinative influence with respect to the processing of personal data in question".[37] The wording used by the EDPB therefore seems to suggest that such a factual assessment is not necessary where the controller or the criteria for its determination have been laid down by law.[38] In that case, the EDPB underlines that the legal designation "will be determinative for establishing who is acting as controller".[39] Nonetheless, the EDPB also states that the designation of the controller by law presupposes that the appointed entity "has a genuine ability to exercise control".[40] This seems to be a safeguard against overly artificial schemes allowing to challenge the allocation of responsibilities put in place by the legislator, should there be major discrepancies between the factual reality and the legal fiction.

17 Third, it appears from the wording of Art. 4(7) GDPR—"alone or jointly with others"—that more than one entity can determine the purposes and the means of the processing operations. This can lead to a situation of joint control, which will be extensively discussed below.

18 Fourth, as already pointed out by the WP29,[41] the EDPB states that determining the "purposes and means" amounts to "deciding respectively the 'why' and the 'how' of the processing."[42] It is necessary to exert influence over both those elements to qualify as a controller, although "some margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing".[43] In short, one should distinguish between the essential means—which have to be determined by the controller—and the non-essential means—which can, to a certain extent, be delegated to another entity without shifting (or sharing) the burden of control to or with that entity. The essential elements of the means concern matters such as which data shall be processed, which third parties shall have access to the data or how long the data shall be processed.[44] The non-essential elements relate to more "practical aspects of implementation" such as which software or hardware to use.[45]

19 Fifth, when detailing the notion of "processing**"**, the EDPB emphasises that control is to be allocated with regard to specific processing operations. In other words, the assessment described above "may extend to the entirety of the processing at issue, but may also be limited to a particular stage in the processing".[46] In that sense, the EDPB accommodates both a macro and a micro-perspective when it comes to the identification of the relevant processing

[35] ibid 11.

[36] Article 29 Working Party (n 6) 8-10.

[37] European Data Protection Board (n 7) 11.

[38] ibid 11. The EDPB indeed states that "*in the absence of* control arising from legal provisions, the qualification [...] must be established on the basis of an assessment of the factual circumstances surrounding the processing" (emphasis added).

[39] ibid 11.

[40] ibid.

[41] Article 29 Working Party (n 6) 14.

[42] European Data Protection Board (n 7) 14.

[43] ibid.

[44] ibid 15

[45] ibid.

[46] ibid 17.

operations.[47] It fails, however, to provide any specific guidance as to the criteria to be used to identify the relevant set or stages of the processing operations. Moreover, as will be detailed below, the EDPB does not consider access to the data being processed as a determining factor when qualifying an entity as a controller.[48]

2. The notion of joint control in the CJEU case law

20 In its latest *Fashion ID* judgment, the CJEU was asked by the referring court whether the operator of a website like Fashion ID could qualify as a controller under the DPD when embedding a Facebook 'like' plug-in on its website. The plug-in caused the visitor's browser to transmit personal data to Facebook, regardless of whether that visitor had a Facebook account and whether they had clicked on the 'like' button or not. The personal data at issue consisted of the visitor's IP address and the browser string to which Fashion ID did not have access. The CJEU was not asked to rule on whether the data at issue were personal. Like Advocate General Bobek, who delivered the opinion in that case,[49] the Court probably took it as a given that they were. The Court did, however, specify that "joint responsibility of several actors for the same processing [...] does *not* require each of them to have *access* to the personal data concerned" (emphasis added).[50] When it comes to identifying the relevant processing operations in relation to which control has to be assessed, the Court stated that "the processing of personal data may consist in one or a number of operations, each of which relates to one of the *different stages* that the processing of personal data may involve" (emphasis added).[51] The Court deemed the "collection and disclosure by transmission"[52] of the website visitors' personal data by Fashion ID to Facebook as the relevant processing operations in relation to which Fashion ID's controller role should be assessed. Subsequent stages in the processing were, by contrast, deemed irrelevant.

21 After having stressed that the concept of controller is to be defined broadly in order to ensure "effective and complete protection" [53] of data subjects, the CJEU held that a "natural or legal person who exerts influence over the processing of personal data, *for his own purposes*, and who participates, as a result, in the *determination of the purposes* and *means* of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46" (emphasis added).[54] As to the means, the Court concluded that Fashion ID, by embedding the social plugin on its website, while being fully aware that it served as a tool for collection and transmission of personal data to Facebook, "exerts a decisive influence over the collection and transmission of the personal data of visitors to that website" to Facebook, "which *would not have occurred without* that plugin" (emphasis added).[55] As to the purposes, the CJEU considered that the collection and transmission of personal data to Facebook were "performed in the *economic interests* of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own *commercial purposes* is the consideration for the benefit to Fashion ID" (emphasis added).[56] The CJEU concluded that Fashion ID can be considered to be a joint controller with Facebook in respect of the "collection and disclosure by transmission of the personal data of visitors to its website".[57]

22 Earlier, in the *Wirtschafstakademie* case, the CJEU had to determine whether the administrator of a Facebook fan page, *i.e.* Wirtschafstakademie, could be considered a joint controller with Facebook in relation to the processing of personal data of the visitors of that fan page. When considering the role of the administrator of the fan page in relation to that processing, the Court attached importance to the fact that, by creating the fan page, the administrator "*gives* Facebook the *opportunity*" to carry out such processing (emphasis added).[58] It further held that the fan page administrator "contributes to the

[47] European Data Protection Board (n 17) 17. This mirrors the approach taken earlier by the WP29, as also mentioned by Van Alsenoy in Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (KU Leuven Centre for IT and IP Law, 1st edn, Intersentia, 2019) 69.

[48] European Data Protection Board (n 7) 17.

[49] Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV joined parties: Facebook Ireland Limited* [2018], Opinion of Advocate General Bobek (n 1), para 58.

[50] Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629 para 69.

[51] ibid para 72.

[52] ibid para 76.

[53] ibid para 50.

[54] ibid para 68.

[55] ibid para 78.

[56] ibid para 80.

[57] ibid para 84.

[58] Case C210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] ECLI:EU:C:2018:388 para 35.

processing of the personal data of visitors to its page" by defining the criteria in accordance with which the statistics of the visits of the fan page were to be drawn and designating the categories of persons whose personal data would be made use of by Facebook.[59] The CJEU therefore considered that the fan page administrator was taking part in the determination of the purposes and the means of the processing of personal data of visitors of that fan page, "by its *definition of parameters* depending in particular on its target audience and the *objectives of managing* and *promoting its activities*" (emphasis added).[60] Like in *Fashion ID*, the CJEU stressed that it was not necessary for each controller to have access to the relevant personal data and that various operators may be involved at different stages of the processing of personal data and to different degrees.[61]

23 Similarly, in *Jehovah's Witnesses*, the CJEU confirmed that access to the personal data was not a necessary prerequisite for an actor to qualify as a (joint) controller.[62] Concretely, the CJEU considered that, although the Jehovah's Witnesses Community did not have access to the personal data and did not know the specific circumstances in which its members collected and further processed such data, it nonetheless "organized, coordinated and encouraged" the preaching activities in the framework of which the processing was taking place.[63] Moreover, "the collection of personal data relating to the persons contacted and their subsequent processing" was carried out to "help achieve the objective of the Jehovah's Witnesses Community, which is to spread faith".[64] The CJEU considered this to be sufficient to conclude that the Jehovah's Witnesses Community determined, jointly with its members, "the purposes and means of processing of personal data of the persons contacted [...]".[65]

3. The notion of joint control in the EDPB Guidelines 07/2020

24 Compared to the assessment of control in general (see section B.III.1), when it comes to assessing joint control, the EDPB appears to stress more the importance of a factual, rather than a formal analysis. Indeed, in the case of joint control, states the Board, it might be that "the formal appointment [laid down by the law or in a contract] does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to 'determine' the purposes and means of the processing".[66]

25 According to the EDPB, "the overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation".[67] The EDPB further states that two or more entities can be seen to jointly participate in the determination of the purposes and the means of a given (or set of) processing operation(s), when they take "common" or "converging" decisions.[68] A common decision means "deciding together and involves a common intention in accordance with the most common understanding of the term 'jointly' referred to in Article 26 of the GDPR".[69] Converging decisions, on the other hand, "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 the means of the processing".[70] Echoing the CJEU's finding in *Fashion ID*, the EDPB adds that an important criterion to determine that the entities take converging decisions, is "whether the processing *would not be possible* without both parties' participation in the sense that the processing by each party is inseparable, *i.e.* inextricably linked" (emphasis added).[71] Moreover, like the CJEU in *Fashion- ID*,[72] the EDPB stresses that the "existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal

[59] ibid para 36.

[60] ibid para 39.

[61] ibid para 38, 43.

[62] Case -25/17 *Tietosuojavaltuutettu intervening parties: Jehovan todistajat — uskonnollinen yhdyskunta*, [2018] ECLI:EU:C:2018:551 para 69.

[63] ibid para 70.

[64] ibid para 71.

[65] ibid para 73.

[66] European Data Protection Board (n 7) 19.

[67] ibid.

[68] ibid.

[69] ibid.

[70] ibid.

[71] ibid 19-20.

[72] Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* [2019] (n 50) para 70.

data."[73] As correctly remarked by other scholars,[74] there are, however, no clear criteria according to which responsibility should be apportioned among joint controllers.

26 The EDPB subsequently clarifies the meaning of a jointly determined purpose, *i.e.* a purpose that is either identical, common, closely linked or complementary to the purpose pursued by another entity.[75] Echoing the reasoning developed in both *Fashion ID* and *Wirtschafstakademie*, the EDPB states that this could be the case "when there is a mutual benefit arising from the same processing operation, provided that each entity involved participates in the determination of the purposes and means of the relevant processing operation".[76] At the same time, however, the EDPB also specifies that "the mere existence of a mutual benefit (for ex., commercial)" is not sufficient to establish joint control, as the entity involved in the processing must "pursue [a] purpose of its own".[77]

27 The EDPB moreover points out that jointly determining the means does not imply that the entities need to determine the means to the same extent. With reference to the abovementioned *Fashion ID* and *Wirtschafstakademie* cases, the EDPB clarifies that the joint determination of means can follow from a situation in which a given entity makes use of a technology developed by another entity for its own purposes. In that sense, "the entity who decides to make use of [the means provided by another entity] so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing".[78]

IV. From one ambiguity to another: towards a broad notion of joint control

1. The relevant processing operations

28 The processing operation in relation to which joint control should be assessed could be defined at a micro-level, looking at one specific processing operation, or at a macro-level, with respect to a set of processing operations. As mentioned above, the EDPB's opinion seems, like the earlier WP29 opinion it replaces,[79] to accommodate both approaches. By contrast, as already noted in literature, the CJEU appears to have adopted a micro-level and so-called "phase-oriented"[80] approach to joint control in its recent case-law, and most recently in *Fashion ID.*

29 Remarkably, as noted by other scholars in relation to the CJEU's ruling in *Fashion ID*,[81] both the CJEU and the EDPB fail to provide any objective criterion on the basis of which the relevant phases of the processing should be identified. According to some commentators,[82] the key element to define the relevant processing operation would be the unity of purposes.[83] As explained below, this introduces an

[73] European Data Protection Board (n 7) 20.

[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 (1) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 91, 95-96 < https://www.jipitec.eu/issues/jipitec-10-1-2019/4879> accessed 21 April 2021.

[75] ibid 19.

[76] ibid.

[77] ibid.

[78] ibid 20.

[79] Van Alsenoy (n 47).

[80] Rene Mahieu and Joris van Hoboken, 'Fashion ID: Introducing a Phase-Oriented Approach to Data Protection?' 30 September 2019 European Law Blog <https://europeanlawblog.eu/2019/09/30/Fashion ID-introducing-a-phase-oriented-approach-to-data-protection/> accessed 21 April 2021; Mahieu, van Hoboken and Asghari (n 74).

[81] Mahieu and van Hoboken (n 80).

[82] Serge Gutwirth, *Privacy and the information age* (Lanham, Rowman & Littlefield Publ., 2002) 97, as quoted in Van Alsenoy (n 47) 69-70.

[83] This approach was also adopted by the Advocate General Bobek in his opinion in *Fashion ID*, in which he highlights that "both the Defendant and Facebook Ireland seem to pursue commercial purposes in a way that appears to be mutually complementary". "In this way", he adds, "although not identical, there is unity of purpose: there is a commercial and advertising purpose". Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV joined parties: Facebook Ireland Limited* [2018], Opinion of Advocate General Bobek (n 1), para 105; The 'unity of purpose' approach has also been recognised by the EDPB in the final version of its guidelines 07/2020, where it states that 'it is necessary to double check whether at 'macro-level' these processing operations should not be considered as a 'set of operations' pursuing a *joint purpose* using jointly defined means (emphasis added). See European Data Protection Board (n 17) 17.

additional layer of uncertainty as to the level of detail with which the purposes should be defined. Indeed, the degree of precision with which the purpose is scoped will directly impact the granularity of the processing operations, and *vice-versa*. Intuitively, the more general the purpose, the higher the likelihood to find that several processing operations share the same purpose and the larger the set of the processing operations in light of which control is to be assessed. Conversely, the more specific the purpose, the lower such likelihood.[84] The EDPB did not provide any explanation on this point in its recent guidelines. The WP29 did, however, briefly touch upon this issue in its Opinion 03/2013 on purpose limitation, where it stated that the purpose "must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied. For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will – without more detail – usually not meet the criteria of being 'specific'".[85] It remains uncertain, however, whether a consideration made in relation to the principle of purpose limitation also applies to the definition of purposes when delineating the relevant processing operation for assessing control.[86] As a consequence, the delineation of the relevant processing operations and consequent allocation of responsibilities might end up being an arbitrary, fluid exercise, as will be further illustrated in the second part of this paper.

2. Identifiability and access to data

30 Another key question emerging from the findings outlined above is whether the perspective through which identifiability is assessed under Article 4(1) GDPR predefines the candidates for the role of controller. In other words, whether the assessment as to the existence of "personal data" happens independently from the one conducted to identify the entity that "determines" the "purposes" and the "means" of the processing.

31 Since access to the data at stake is a *de facto* requirement for an entity to be able to "reasonably likely" (re-)identify the individuals, by clarifying that access is not a prerequisite for "joint responsibility" (which in the cases at hand, implied joint control), the CJEU seems to have (at least implicitly) accepted that a party may qualify as a joint controller of data that from that party's perspective, are in fact anonymous. Interestingly—although they were not issued under the GDPR—the European Data Protection Supervisor's ("EDPS") Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 seem to endorse this approach. Indeed, the EDPS states that: "The fact that a party only has access to information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or not longer identifiable [...] does not influence the joint controllership situation."[87] However, the EDPS adds, "this may nonetheless matter when establishing the degree of responsibility of the parties involved".[88]

32 To the contrary, if one were to adopt a relative approach to personal data and consider that the perspective from which identifiability is assessed predetermines the potential candidates for the role of controller, it would not even be necessary to assess the role of the parties lacking access to the data as possible (joint) controllers. In that case, the data at stake would not be personal to these parties, as, by lacking access, they would *a fortiori* lack the means reasonably likely to be used to identify the individual.

33 An alternative explanation could be that, by stating that access to data is not a prerequisite for joint control under the GDPR, the CJEU meant *actual* access to data at the time of the processing, as opposed to *potential* and reasonably likely future access. This interpretation would reconcile the CJEU's statement on access to personal data when assessing joint control with the relative and risk-based approach to personal data. However, it would still be incompatible with the less nuanced position of the EDPB on the topic, which, as already mentioned, stated that "someone who outsources a processing

[84] See similarly: Frank Robben, 'Toepassingsgebied en begripsdefinities', in Jos Dumortier and Frank Robben, *Persoonsgegevens en privacybescherming. Commentaar op de wet tot bescherming van de persoonlijke levenssfeer* (Brugge, Die Keure, 1995) 28, as quoted in Van Alsenoy (n 47) 256-257.

[85] Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013) 15–16 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 21 April 2021.

[86] See similarly: Charlotte Ducuing and Jessica Schroers, 'The recent case law of the CJEU on (joint) controllership: have we lost the purpose of 'purpose'?' (2020) 6 Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht 429.

[87] European Data Protection Supervisor, 'Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' 24 <https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf> accessed 21 April 2021.

[88] ibid.

activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing [...] is to be regarded as controller even though *he or she will never have actual access* to the data" (emphasis added).[89] Thus, the question that remains unanswered is whether lacking potential—as opposed to actual—access could preclude an entity from being regarded as a controller.

34 The analysis carried out in section F illustrates a major implication of this loophole: potentially, an actor could qualify as a (joint) controller of data that, from that actor's perspective, are not personal.

3. The meaning of (participating in) the determination of purposes and means

35 Next to assisting in the delineation of the relevant processing activities in light of which control is to be assessed, identifying the "purpose" of the activity is also necessary to determine whether the entity(ies) at issue can be said to jointly participate in their determination. As seen above, determining the purposes means ascertaining "why" data is processed. In *Fashion ID,* the key criterion to conclude that the entities at issue jointly determined the purposes seems to have been that the processing operation commercially benefitted both entities. Fashion ID benefitted from an "increased publicity for its goods" and Facebook was able to use the data collected for "its own commercial purposes".[90] The EDPB, however, clarified that mutual (commercial) benefit is only an example of, but not a sufficient condition for, two or more entities to be said to jointly determine the purpose. According to the EDPB, what is required is that each entity pursues a "purpose of its own", which is defined negatively: an entity which is "merely being paid for the services rendered" would not pursue a purpose of its own and hence be a processor, not a joint controller.[91] This explanation seems to suggest that "own purpose" is to be interpreted as the motivating factor driving the entity to engage in a certain processing activity. This interpretation could, again, leave the door open to a wide array of situations where a party could qualify as a joint controller. Indeed, depending on how granularly the purpose is defined, it would in theory always seem possible to attribute a distinctive commercial or other purpose to the entities involved in the processing operations at stake.

36 As to the "means", whereas the EDPB makes a clear distinction between essential and non-essential means when discussing sole control and unambiguously states that the controller must determine the essential elements of the means, this clear-cut demarcation seems to become less relevant in the case of joint control.[92] With reference to *Fashion ID*, the EDPB indeed states that the joint determination of the means could follow from an entity's choice to use a tool developed by another entity for "its own purposes". Again, this raises the same interpretative questions and ensuing potential broad interpretation as to the meaning of processing for "its own purpose" as set out in the preceding paragraph.

37 Finally, the meaning of "determining" also suffers from a lack of clarity in at least two ways. First, it is unclear whether the legal designation of a controller should supersede factual reality. On the one hand, when assessing control (in general), the EDPB seems to imply that a factual analysis should only be performed in case of major discrepancies between the law and the fact. On the other hand, as mentioned above in section B.III.3, when assessing joint control, the EDPB seems to be more nuanced, by presumably requiring a higher degree of factual scrutiny when analysing whether two or more entities could act as joint controllers. This raises the specific question analysed in section F as to whether a situation of joint control is possible between a legally designated controller, on the one hand, and a factual controller, on the other. More specifically, the question is whether the designation of one controller by law as such excludes a situation of joint controllership between that legally designated controller and a factual controller. Again, although not applicable to the case at hand, the aforementioned EDPS' Guidelines can provide some partial guidance in this respect. They indeed state that "joint controllership may also occur between an EUI [European Union Institution] and an external actor (such as an external provider of a management portal or a national public authority etc.)." [93] Nevertheless, the EDPS discourages this scenario and encourages EUIs to make sure that private companies act as processors.[94]

[89] European Data Protection Board (n 7) 17.

[90] Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* (n 50) para 80.

[91] European Data Protection Board (n 7) 21.

[92] ibid. The fact that a joint determination of the essential means is necessary to qualify as joint controllers nonetheless transpires from the examples mentioned in pp. 20-22 of the EDPB's guidelines.

[93] European Data Protection Supervisor (n 87) 22-23.

[94] Since Regulation 2018/1725 on the "protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data" explicitly leaves room (in article 28.1) for a situation of joint control between EUIs and

38 Second, if we perform a factual assessment, what seemed to have played a crucial role in the aforementioned CJEU case law, particularly *Fashion ID*, was not as much the capacity to determine "why" and "how" personal data were processed, but merely "if" personal data were processed at all. This approach, focusing on enabling the processing of personal data by another party,[95] is confirmed in the EDPB guidelines, which stress that joint determination arises in the case of converging decisions or, in other words, when the "processing would *not be possible* without both parties' participation" (emphasis added) (see section B.III.3). The perils inherent to such a broad interpretation of the term "determining" are eloquently explained by Advocate General Bobek in its opinion in *Fashion ID.* There it states that, if one looks at the joint control test critically, "it seems that the crucial criterion after *Wirtschafstakademie Schleswig-Holstein* and *Jehovah's Witnesses*" seems to be "that the person in question '*made it possible*' for personal data to be collected and transferred, potentially coupled with some input that such a joint controller has on the parameters (or at least where there is silent endorsement of them)". "If that is indeed the case", he adds, "then in spite of a clearly stated intention to that effect to exclude it in *Wirtschafstakademie Schleswig-Holstein*, it is difficult to see how normal users of an online (based) application, be it a social network or any other collaborative platform, but also other programmes would not also become joint controllers".[96]

(arguably public and private) non-EUIs entities, it is disputable whether and, if yes, to which extent, this answer also applies to situations of joint control between a public and private entity/ individual falling under the GDPR. We therefore do not further consider this document for the purposes of the case-study presented below.

[95] Chen and others (n 4) 284 refer to this approach as "joint-controllership by technical configurations".

[96] Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV joined parties: Facebook Ireland Limited* [2018], Opinion of Advocate General Bobek (n 1) para 73.

Component of the definition of joint controller		**Ambiguity**	
#1	Relevant processing operation	Unity of purpose as a criterion to circumscribe the relevant processing operation? If so, how to define purpose (see also **#3**)?	
		Stage of the processing operation as a criterion to circumscribe the relevant processing? If so, how to identify the relevant stage?	
#2	Personal data	Identifiability	Risk based and relative or zero-risk and absolute approach to the notion of personal data?
			Does the perspective from which identifiability is as-sessed when defining personal data (under Article 4(1) GDPR) predefine the candidates for the role of controller (under Article 4(7) GDPR)?
#3	Joint determination of purposes and means	Purposes	Each actor to pursue its "own purpose"? If so, how to define purpose (see also **#1**) ?
			What is the meaning of (i) identical, (ii) common, (iii) closely linked or (iv) complementary" purposes?
		Means	Each actor to pursue its "own purpose", when using technology developed by other entity? If so, how to define purpose (see also **#1**) ?
		Determinations	Does the legal designation of one controller exclude per se joint controllership between the legally designated controller and a factual one?
			When it comes to the notion of "converging decision", how extensively should the criteria of "making the data processing possible" be interpreted?

C. The household exemption: a way out?

39 The so-called "household exemption" exempts a natural person processing personal data "in the course of a purely personal or household activity" from the GDPR's scope of application (Article 2(2)c GDPR). It applies to processing operations that have no connection to "a professional or commercial activity", which could include, for instance, "correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities" (Recital 18 GDPR). Both the WP29 and the CJEU have had the opportunity to clarify the contours of that exemption, the scope of which has not drastically changed since the DPD (Article 3(2), second indent and Recital 12 DPD).

40 In its judgment in the *Lindqvist* case, the CJEU held that the household exemption was to be interpreted narrowly as "relating only to activities which are carried out in the course of [the] private or family life of individuals".[97] As pointed out by the Advocate General at the time, this would only cover "confidential activities that are intended to be confined to the personal or domestic circle of the persons concerned".[98] The household exemption, the Court added, would then clearly not apply to the "processing of personal data consisting in publication on the internet so [they] are made accessible to an indefinite number of people".[99] This was later reiterated by the Court in the *Satamedia* case.[100]

41 More recently, the CJEU also clarified that video surveillance, if partially "covering a public space" and therefore "directed outwards [...] the private setting of the person processing the data" would not fall within the scope of the household exemption.[101] In its detailed opinion, Advocate General Jääskinen discussed the distinction between personal activities—"which are closely and objectively linked to the private life of an individual and which do not significantly impinge upon the personal sphere of others" and "may take place outside the home"—and household activities—"that are linked to family life and normally take place at a person's home or in other places shared with family members, such as second homes, hotel rooms or private cars".[102] While both types of activities fall within the scope of the household exemption, he also highlighted that the processing operations at stake must "exclusively" relate to either personal or household activities in order to benefit from the exemption.[103] The CJEU recently applied the above-mentioned criteria in its *Jehovah's Witnesses* judgment to exclude the taking of notes by Jehovah's Witnesses during door-to-door preaching from the scope of the household exemption.[104]

42 In its Opinion 5/2009 on online social networking, the WP29 detailed additional elements that should be taken into account when determining whether end-users of social network services ("SNSs") could rely on the household exemption. Among others, it stated that when "an SNS user acts on behalf of a company or association, or uses the SNS as a platform to advance commercial, political or charitable goals", the said exemption should not apply. Echoing the reasoning developed by the CJEU in *Lindqvist* and *Satamedia*, the WP29 also held that, "when access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS [...]", it goes beyond the personal or household sphere.[105] Same goes for a user who takes the "informed decision to extend [such] access beyond self-selected 'friends'".[106]

43 As already remarked by other scholars,[107] there is a tendency to interpret the household exemption

[97] Case C-101/01 *Bodil Lindqvist v* Åklagarkammaren *i* Jönköping [2003] ECLI:EU:C:2003:596 para 47.

[98] Case C-101/01 *Bodil Lindqvist v* Åklagarkammaren *i* Jönköping [2003], Opinion of Advocate General Tizzano ECLI:EU:C:2002:513, para 34.

[99] Case C-101/01 *Bodil Lindqvist* (n 97) para 47.

[100] Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy* [2008] ECLI:EU:C:2008:727 para 44.

[101] Case C-212/13 *František Ryneš v* Úřad *pro ochranu osobních* údajů [2014] ECLI:EU:C:2014:2428 para 33.

[102] Case C-212/13 *František Ryneš v* Úřad *pro ochranu osobních* údajů [2014], Opinion of Advocate General Jääskinen ECLI:EU:C:2014:207, para 51.

[103] ibid para 53. This, he added when discussing whether the collection of video footages could qualify as 'purely' household activities, would not be the case 'when the processing involves 'persons who have no connection with the family in question and who wish to remain anonymous' (ibid para 56).

[104] Case -25/17 *Tietosuojavaltuutettu intervening parties: Jehovan todistajat — uskonnollinen yhdyskunta* (n 62) para 41-45.

[105] Article 29 Working Party, 'Opinion 5/2009 on online social networking' (2009) 6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf> accessed 21 April 2021.

[106] ibid.

[107] Chen and others (n 4) 279-293.

increasingly narrowly. As will be seen below, this can lead to an increase of situations where a natural person qualifies as (joint) controller under the GDPR.

D. The case study: hypothesis, objective, methodology and limitations

44 One of the distinctive features of a decentralised architecture is to distribute the processing of personal data across multiple devices, rather than centralizing everything through the use of a single server. Decentralised systems are often presented as more privacy-friendly alternatives to centralised solutions since they eliminate the need to trust a single entity.[108] Yet, such systems also scatter the processing operations across multiple parties, therefore raising the issue as to the role and qualification of these actors under EU data protection law. More specifically, as will be seen below, one of the main differences between centralized and decentralized COVID-19 proximity tracing solutions is that under the decentralized protocol more processing operations take place at the edge, i.e. on the app user's mobile phone, rather than on a central (back-end) server. As hinted above, in relation to a case-study concerning security/privacy preserving edge computing solutions adopted in smart home Internet of Things, scholars have already argued that the current broad notion of joint control, coupled with the narrow interpretation of the household exemption, may end up "unfairly burdening certain stakeholders in smart homes", [109] including the smart home user, and "disincentivise uptake" [110] of security/privacy preserving edge computing solutions. We inquire whether this conclusion could, in theory, also hold true in the case of privacy-preserving decentralized solutions such as those applied in COVID-19 digital proximity tracing.

45 We postulate that the more actors involved in the processing of personal data, the more parties are likely to bear a certain degree of responsibility under the GDPR including, potentially, end-users themselves. Applied to the case of COVID-19 apps, the hypothesis is hence that end-users will be considered joint controllers with the national health authority for certain processing operations in a decentralised approach. To understand whether the architecture of the protocol has an impact on the outcome, we also analyse the role of the app user under centralized solutions. We investigate this by applying the broad legal framework for joint control emerging from the analysis presented in sections B and C of the paper to the following use-cases: the ROBust privacy-presERving proximity Tracing ("ROBERT") protocol, which is an instance of a centralised COVID-19 app, and the Decentralised Privacy Preserving Proximity Tracing ("DP-3T") protocol, which adopts a decentralised approach. These publicly available protocols[111] and accompanying privacy and security impact analyses[112] were used to illustrate the main features of the centralised and decentralised approaches.

46 In light of the above, the following main research question is examined: given the broad interpretation of joint control, could app users qualify as controllers under the GDPR, jointly with the legally designated controller (*i.e.* in most cases, the national health authority), with regard to the processing of other app users' personal data? If the answer is positive, we examine the following additional questions. First, does the answer to the first question differ depending on the centralised or decentralised nature of the tracing solution? Second—given that, as mentioned above (section B), we believe that one should first assess whether the data at issue is personal (and more specifically, identifiable) in order to allocate (joint) control—do the processing operations with respect to which the (joint) controller exercises control always qualify as operations on personal (hence identifiable) data from the perspective of that controller?

47 The study admittedly suffers from the following limitations. First and foremost, we do not intend to cover the full spectrum of responsibilities arising

[108] Primavera de Filippi, 'The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies' (2016) 9 Journal of Peer Production 4 < https://hal.archives-ouvertes.fr/hal-01382006/document> accessed 21 April 2021.

[109] Chen and others (n 4) 293.

[110] ibid.

[111] PRIVATICS team INRIA and AISEC FRAUNHOFER, 'ROBERT: ROBust and Privacy-PresERving Proximity Tracing v.1.1' (2020) <https://github.com/ROBERT-proximity-tracing/documents/blob/aa1921f0006fcebd35bc30eeb765b22e45027a62/ROBERT-specification-EN-v1_1.pdf> accessed 21 April 2021; Carmela Troncoso and others, 'Decentralised Privacy-Preserving Proximity Tracing - Version 25 May 2020' (2020) < https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf > accessed 21 April 2021.

[112] PRIVATICS team INRIA, 'Proximity Tracing Approaches Comparative Impact Analysis v1.0' (2020) <https://github.com/ROBERT-proximity-tracing/documents/blob/master/Proximity-tracing-analysis-EN-v1_0.pdf> accessed 21 April 2021; DP-3T Project, 'Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems' (2020) <https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf> accessed 21 April 2021.

from concrete digital proximity tracing solutions adopted in the fight against COVID-19. Indeed, we did not delve into any concrete implementation of the two abovementioned protocols by States. Similarly, the specific design features of each protocol were left out of the scope of the analysis. Our analysis focuses on the main differences between two distinct architectures, rather than on a specific app, and aims at highlighting the challenges and, at times potentially paradoxical consequences, stemming from the rigorous application of the criteria of joint control to the specific case of the app user in the two protocols under consideration. Second, we qualified the data as "personal" and allocated control on the basis of a selected list of processing operations on other app users' EphIDs and the assumption that the backend server is operated by the same public entity (*i.e.* the national health authority) that operates the overall application. Third, we do not have an academic or professional background in software engineering nor cryptography. The reasoning and findings presented in this paper are therefore entirely based on the documentation made available by the two consortia behind the selected protocols.

E. Centralized v. decentralized approach to digital contact tracing

48 Broadly speaking, COVID-19 apps work as follows. When two individuals cross each other's path, both apps (i) broadcast their own Ephemeral Identifiers ("EphIDs")—that is, the piece of information generated by either the backend server or the end-user's device to allow proximity tracing—and (ii) collect and store the EphIDs of nearby app users. If app users are tested positive to COVID-19, they have the possibility to inform the backend server that they are infected and, in a centralised approach, to share their recent encounters. This information is then used to (i) calculate the risk that someone has been infected following an encounter with an infected user and (ii) should that risk reach a certain threshold, inform that person of the procedure to follow. Below, we outline the necessary technical details that support the assessment performed in section F.

I. Who? The actors involved in BLE-based digital proximity tracing solutions

49 From an architectural point of view, the analysed COVID-19 apps rely on two main components: a terminal equipment (*i.e.* the app user's mobile device) and the back-end server.[113] In the present paper, we start from the postulate that the national health authority is operating the backend server, as part of the app system.[114] For the legal analysis deployed in section F, we therefore assimilate the national health authority with the app operator and the backend server, and consistently refer to the latter, as its role is extensively detailed in the documentation of both investigated protocols. The exact relationship between the national health authority, the backend and app operator(s) and other actors such as for example the app developer is, therefore, excluded from the scope of the present contribution. Instead, we focus on the following actors.

50 First, the *app users*, *i.e.* all the individuals who have downloaded and installed the app. For the purpose of our analysis, they can be further divided into the following categories:[115] (i) the *diagnosed* users, who are infected with COVID-19 and have been diagnosed positive to it; (ii) the *at risk* users, who have been in the proximity of a diagnosed user in the period during which the latter was contagious; (iii) the *exposed* users, who have been notified that they have been in the proximity of a diagnosed user.

51 Second, the *national health authority*, *i.e.* the entity that, in each country, is tasked with the implementation and supervision of the policies related to public health. According to the EDPB's Guidelines 04/2020, national health authorities could potentially be regarded as the controllers for the deployment of digital proximity tracing apps, although "other controllers may also be envisaged".[116] As highlighted

[113] It is worth noting that both the centralised and decentralised approaches to digital proximity tracing described in this paper rely on a backend server. Its role within the functioning of the tracing system as well as the amount of information that transits through it, however, significantly differs depending on the approach.

[114] This seems to be the approach adopted in Switzerland, where the backend(s) are "under the direct control of the Federal Office of Public Health (FOPH) and are operated technically by the Federal Office of Information Technology, Systems and Telecommunications (FOITT)". See FOPH, 'Data Protection Statement of the Federal Office of Public Health FOPH in connection with the use of the "SwissCovid app"' (2020) <https://www.bag.admin.ch/dam/bag/en/dokumente/cc/kom/swisscovid-app-datenschutz.pdf.download.pdf/FOPH_SwissCovid_Data_Protection_Statement_24_June2020.pdf> accessed 21 April 2021.

[115] This taxonomy is mainly based on: PRIVATICS Team INRIA (n 112) 4.

[116] European Data Protection Board, 'Guidelines 04/2020 on the use of location data and proximity tracing tools in the context of the COVID-19 outbreak' (2020) 7 <https://edpb.europa.eu/

above, we assimilate the national health authority with the *backend server*, *i.e.* the entity that manages the server used to support the functioning of digital proximity tracing, be it in a centralised or a decentralised solution.

II. How? The functioning of BLE-based digital proximity tracing solutions

52 Broadly speaking, the functioning of the digital proximity tracing solutions under consideration can be broken down into four distinct phases.[117] The decentralised and centralised approaches are illustrated in Figure 1 and Figure 2, respectively.

- *Phase 1 – Installation of the app.* In this initial stage, the users download the app on their mobile phone from an official app store. In the centralised protocol, the app users register with the backend servers which then generates a permanent identifier that does not, as such, reveal the identity of the individual.[118] On the basis of that identifier, the backend server then creates and pushes several EphIDs to the app user's device using its own, periodically renewed global key.[119] In a centralised scenario, the backend server uses its own rotating global key to derive the EphIDs from the permanent identifier created when the app user registered with the backend server for the first time. In the decentralised protocol, the EphIDs are generated pseudo-randomly by each app user's mobile phone on the basis of its own periodically changing secret key.[120]

- *Phase 2 – Broadcasting of the app user's own EphIDs and collection of other app users' EphIDs.* In this phase, each app user's phone broadcasts its own EphIDs and collects and subsequently stores the EphIDs of other app users in the vicinity. This process is identical under the centralised and decentralised approach.

- *Phase 3 – Testing and declaration of infection.* If users test positive to COVID-19, their phone transmits the information necessary for phase 4 to the backend server. The type of information provided differs depending on the nature of the tracing solution. Under the centralised protocol, the diagnosed users transmit the EphIDs of at-risk users collected during phase 2. Under the decentralised approach, however, the diagnosed users only upload their own EphIDs broadcasted during the infectious time window.[121]

- *Phase 4 – Matching and computation of the risk score.* The backend server then processes the information obtained in phase 3 in order to notify at-risk users. Again, this process differs depending on the nature of the app. Under the centralised approach, the matching of a diagnosed user and at-risk users and the computation of the risk-score are performed on the backend server.[122] Under the decentralised protocol, the matching and calculation occur on the phone of the at-risk users.[123]

sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf > accessed 21 April 2021.

[117] Carmela Troncoso and others, 'Decentralized Privacy-Preserving Proximity Tracing – Overview of Data Protection and Security' (2020) 11 <https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf> accessed 21 April 2021; PRIVATICS team INRIA and AISEC FRAUNHOFER (n 111) 4.

[118] The permanent identifier is defined by the ROBERT consortium as a "permanent and anonymous identifier associated to each registered user". See PRIVATICS team INRIA and AISEC FRAUNHOFER (n 111) 15.

[119] ibid 4.

[120] Troncoso and others (n 117) 6–7. In a decentralised scenario, the key on the basis of which the EphIDs are created is assigned by the app user's device itself, with no intervention from the backend server.

[121] More specifically, under the DP-3T protocol, the diagnosed user provides the backend server with the secret key corresponding to the first day in which he was considered infectious. The backend server will then be able to retrieve all EphIDs broadcasted by the diagnosed user's phone during the contagious window. See Troncoso and others (n 111) 16–17.

[122] More specifically, the backend server retrieves the permanent identifiers of the at-risk users whose EphIDs have been uploaded by the diagnosed user during phase 3. On the basis of several parameters such as the amount of time they were exposed to the diagnosed user, the backend server then calculates the risk-score of the at-risk users. If that risk reaches a given threshold, the backend server notifies them that they have been exposed to a diagnosed user and informs them of the procedure to follow.

[123] Here, each app user's phone periodically downloads the diagnosed users' EphIDs from the backend server and verifies whether those EphIDs appear in the records of EphIDs collected and stored during phase 2. If this is the case, the at-risk user's phone computes the risk score on the basis of a number of parameters and, should the risk reach a certain threshold, notifies the app users that they have been in contact with a diagnosed user, together with further instructions.

Table 2 - Explanation of the pictograms used in the various figures

👤📱	📱👤+	☁↑	🔑	🎚⚙
App user	Diagnosed app user	Backend server	Secret key used to generate EphIDs	Matching and computation of the risk score

Figure 1 - Decentralised approach to digital proximity tracing

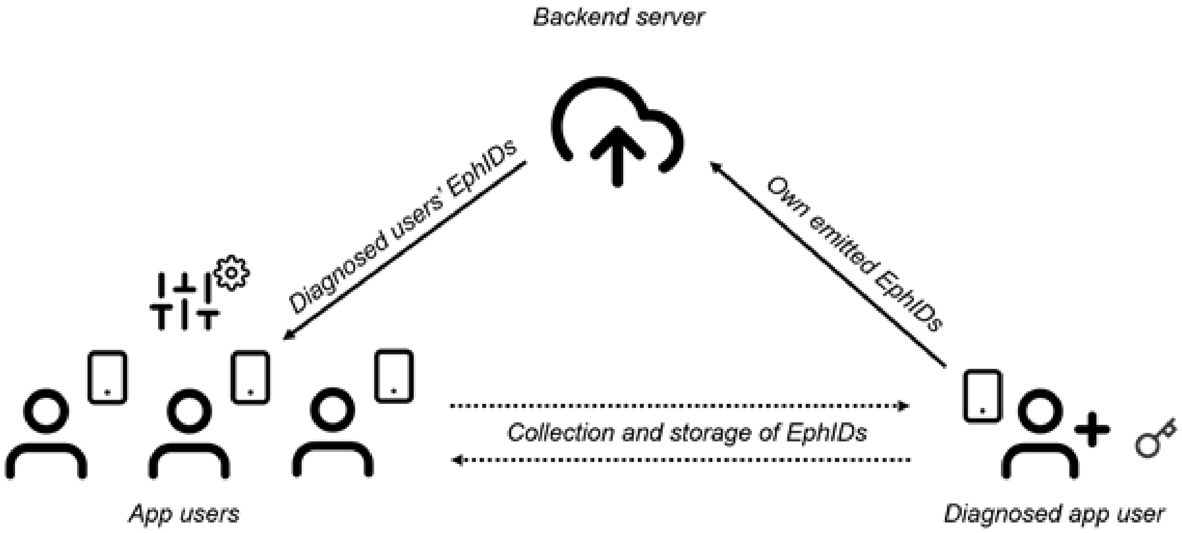
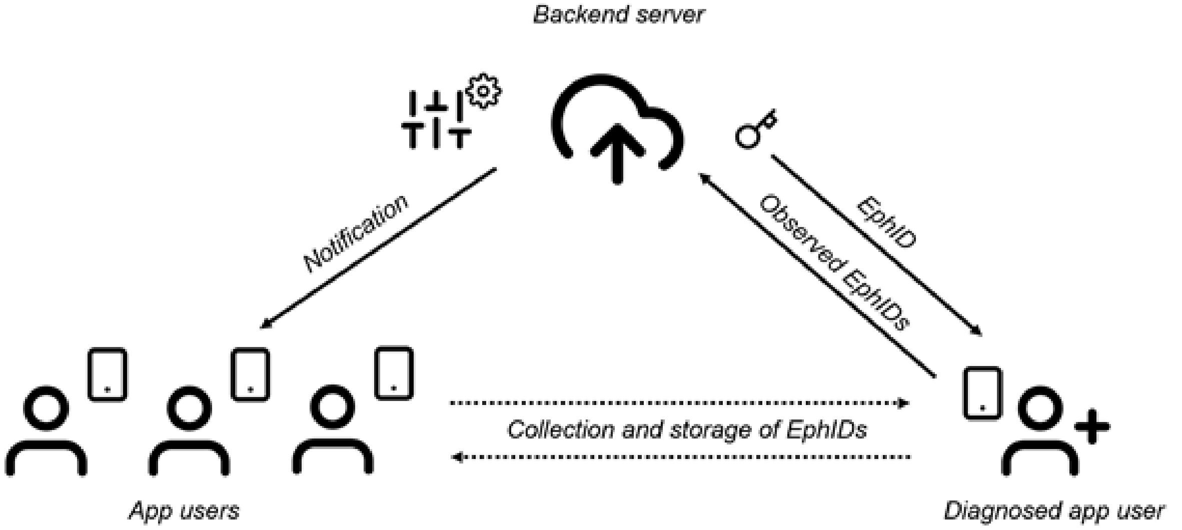


Figure 2 - Centralised approach to digital proximity tracing



F. The app user as joint controller ?

53 In the following section, we illustrate the complexities of the legal test for joint control, by focussing on the role of the app user under the GDPR in the ROBERT and DP-3T protocols. Although the appointment

of the controller is done by law in most European countries[124] (and coincides with the national health authority), we look at whether the app user could qualify as joint controller with the legally appointed controller, when it comes to the processing of other app users' EphIDs. Where pertinent (see section F.I.4 below), we also go beyond the legal fiction, to illustrate (as announced above, see in section B.IV.2) one of the implications of combining the assessment concerning the "identifiability" of personal data with the one relating to (joint) controllership. Namely, an actor could potentially qualify as a (joint) controller of data that, from that actor's perspective, are not personal.

54 Before delving into the following paragraphs, it is necessary to emphasise once again that the present contribution does not intend to confirm or deny any pre-existing claim as to the qualification of end-users as joint controllers in the context of COVID-19 digital proximity tracing apps. Rather, this eventually emerged from the application of the current regulatory framework and available guidance on the notion of joint control to the two protocols at stake.

I. The processing of other app users' personal data

1. Step 1: the relevant processing operations

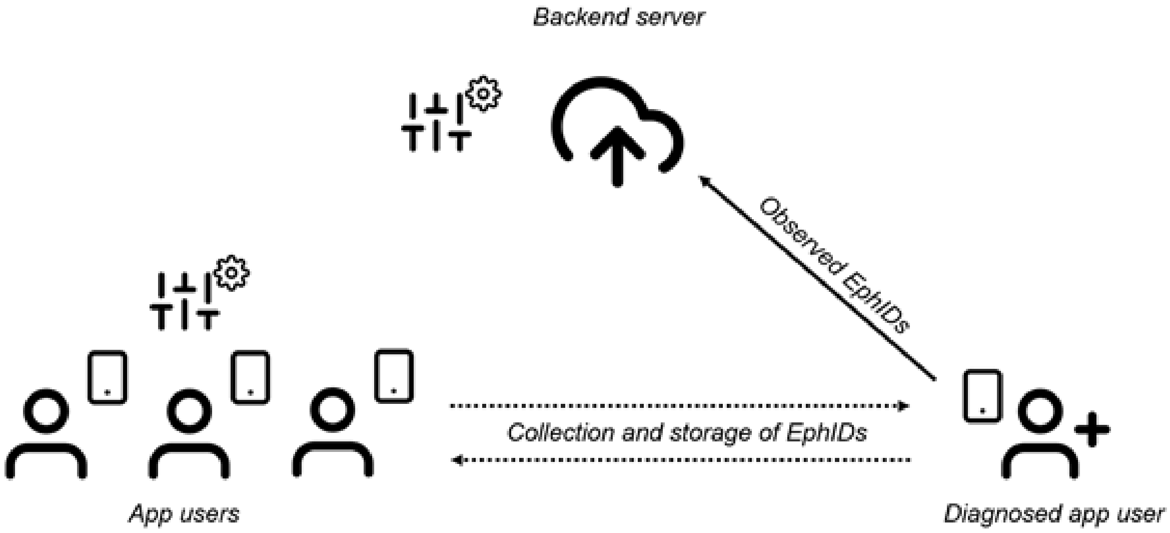
55 As a preliminary step, it is necessary to identify the processing operations in light of which the allocation of responsibilities is to be performed. Article 4(2) GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". To keep the scope of the investigation manageable, and since we want to assess the role of the app user in relation to the processing operations on other app users' personal data (not their own personal data), we limit ourselves to considering the processing operations that are performed on the other app users' EphIDs.[125] This narrows the scope of the analysis down to the following processing activities (Figure 3):

- In both the centralised and decentralised scenarios: the collection and storage by a given app user's phone of EphIDs of other app users (phase 2);
- In the centralised scenario: the transmission by the diagnosed app-user of EphIDs of at-risk app users to the backend server (phase 3) and the subsequent use of these EphIDs by the backend server to compute the at-risk users' risk-score (phase 4);
- In the decentralised scenario: the use by each app user's phone of the diagnosed user's EphIDs in order to match these EphIDs with the observed ones and the use by the at-risk app user's phone of the diagnosed user's EphIDs, in order to compute the app user's risk-score (phase 4).

[124] Belgium, for example, has appointed Sciensano, the public institution tasked—at the federal, community and regional levels—with various missions related to public health, as the controller for the processing operations relating to the Coronalert app (Arrêté Royal n° 44 du 26 juin 2020, art. (14,§3,3°)). Switzerland, for instance, has designated the Federal Office of Public Health (Office Fédéral de la Santé Publique) to act as the controller with regard to the SwissCovid app (Ordonnance 818.101.25 sur le système de traçage de proximité pour le coronavirus SARS-CoV-2 du 24 juin 2020, art. 4). In France, the Health Ministry bears the controllership of the StopCovid app (Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé "StopCovid", Art. 1). In Italy, the Ministry of Health is the controller for the processing operations happening in the context of the Immuni app (Decreto-Legge 30 aprile 2020, n. 28. Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19, Art. 6.1).

[125] Therefore, we discarded the following processing operations as irrelevant for the analysis: the generation of an app user's own EphIDs (and permanent identifiers in the centralised protocol) which occurs during the installation of the COVID-19 app (phase 1 above); the processing operations occurring during the upload of the diagnosed user's own EphIDs on the backend server (phase 3 of the decentralised protocol).

Figure 3 - Processing operations relevant for the analysis



56 It is crucial to determine whether all these processing operations are relevant when assessing control. This shows a first difficulty stemming from the application of the criteria for joint control mentioned above. On the one hand, if we approach the individual processing operations from a *macro-perspective* and adopt the unity of purpose as a criterion for identifying the relevant processing operations, it is plausible to argue that these operations all share the same purpose, namely notifying the app user of an exposure to a diagnosed user. This is the case in both the centralised and decentralised approaches. Such purpose serves both a public interest (*i.e.* preserving public health) but also a private one (*i.e.* preserving each individual user's health). As a result, all these processing operations would be considered as a set of operations and, provided they concern personal data, would all be relevant to assess the role of the app user under the GDPR.

57 On the other hand, it would be equally plausible to define the purpose of the processing operations more granularly, at a *micro-level*. For instance, in a centralised scenario, the purpose of the collection and storage of other app users' EphIDs (phase 2) is the transmission of these EphIDs to the backend server, should the user at issue become infected (phase 3). Similarly, in a decentralised protocol, the use by an app user's phone of the diagnosed user's EphIDs aims at matching these EphIDs with the observed ones and, should a match occur, calculating the risk-score (phase 4).

58 In short, it always seems possible to reduce the purpose of each processing operation to the subsequent stage of the processing that that operation is intended to enable, thereby losing sight of the overall purpose that connects each stage of the processing.[126] This exemplifies the problem identified in section B.IV.1 and table 1 above as to the level of granularity with which the purpose(s) of the processing should be defined.

59 The identification of the relevant processing operations is likely to become even more unpredictable if we abandon the unity of purpose as a criterion and adopt a "phase-oriented"[127] approach to identify the relevant processing operations, like the CJEU seems to have done in *Fashion ID*. In that case, limiting the relevant processing operations to any phase of the processing runs the risk of leading to an artificial representation of the processing operations that lacks any objective rationale.

2. Step 2.1: the qualification of other users' EphIDs as personal data - criteria

60 Next, it is crucial to determine whether the processing activities identified in the preceding paragraph are performed on "personal data". For the purposes of this contribution, we only focus on the identifiability criterion and hence assume that EphIDs can qualify as "any information relating to a natural person" (Article 4 (1) GDPR). Since, as

[126] See similarly: Mahieu and van Hoboken (n 80).

[127] ibid.

highlighted in section B.II.2, we consider the relative and risk-based approach as the most sensible approach to personal data, we assess the nature of the EphIDs under this approach. We do so on the basis of the criteria provided by the privacy and security risks analyses performed by the members of the ROBERT and DP-3T consortia, namely:

- The likelihood of re-identification threats assessed by the members of the ROBERT consortium under a centralised and decentralised approach on the basis of (i) their feasibility (which "depends on the weaknesses of the system and the technical means and expertise of the risk-source") and (ii) motivation of the attacker.[128] When the ROBERT consortium rated such likelihood as "significant" or "maximal", we considered that the EphIDs at issue could qualify as personal data. Moreover, when such likelihood was also implicitly assessed by the members of the DP-3T consortium, their assessment was also taken into account.[129]
- The risk source,[130] which refers to the actor that could pose the relevant threat, as identified by the members of the ROBERT consortium. When the source of the risk is another (tech-savvy or regular) app user, we considered that the EphIDs at issue could be personal data from the perspective of the app-user.[131] When such actor coincides with the operator of the back-end server or a person that could be deemed reasonably likely to be approached by the backend server, such as another State authority, we considered that the EphIDs at issue could qualify as personal data from the perspective of the backend server.

61 Based on these criteria, and without questioning the exactitude of the findings of the two consortia, the following EphIDs could qualify as personal data for the purposes of this analysis (see Table 3 below).

3. Step 2.2: the qualification of other users' EphIDs as personal data – perspective of the app user

62 Since we are interested in knowing whether the app user could qualify as a joint controller with the legally designated controller, we first consider the perspective of the app-user.

63 From this perspective, the diagnosed users' EphIDs could qualify as personal data. The ROBERT and DP-3T consortia point out that, in both the centralised and decentralised protocols, diagnosed users' EphIDs are vulnerable to re-identification attacks performed by *other app users*. The ROBERT consortium lists the following risks.[132] First, there is a risk that a "tech-savvy user" identifies "all infected individuals among encounters", which occurs "when the adversary is able to find diagnosed users among all persons he has encountered during [the] contagious period".[133] In this scenario, the attacker proceeds "by collecting pseudonyms of each person encountered, and then correlating this list of pseudonyms with the list of infected users' pseudonyms published by the authority to determine when she was in contact with an infected person and use this information to reveal the identity of the infected".[134] This attack, the members of the ROBERT consortium add, "only concerns the decentralised approach and is not possible in the centralised approach".[135] Second, there is a risk that a "regular user" identifies "a targeted infected individual".[136] This risk is materialised "by turning on the Bluetooth interface when in presence of the targeted individual, alone, then turning it off".[137] It is described as being "also possible in centralised approaches when the set of encounters of the user is limited to the target only"[138] or in other more costly scenarios, such as when the attacker creates "an instance of the application (registered on the server) for each encountered person".[139]

[128] PRIVATICS Team INRIA (n 112) 5.

[129] We specifically refer to the evaluation by the members of the DP-3T consortium of the nature of EphIDs as pseudonymous data vis-à-vis the backend server in a centralised scenario (DP-3T Project (n 112) 18).

[130] PRIVATICS Team INRIA (n 112) 5.

[131] The legality criterion as put forward in the *Patrick Breyer v Bundesrepublik Deutschland* case (see section B.II.2) is not taken into account for the purposes of this assessment, since it requires a knowledge of the national legal context in which the COVID-19 app is implemented, which is beyond the scope of this analysis.

[132] PRIVATICS Team INRIA (n 112) 7–8.

[133] ibid 7.

[134] ibid. 7-8.

[135] ibid 8.

[136] ibid.

[137] ibid.

[138] ibid.

[139] ibid 7,8.

64 Similarly, although they do not explicitly assess the likelihood of this attack and define it as a risk inherent to proximity tracing systems that notify users that they are at risk, the members of the DP-3T project state that there is a risk that a "motivated attacker identifies the infected people that he has been physically near".[140] This could be done by "combining two pieces of information: (1) who [he] interacted with at each time, and (2) that [he was] in close proximity to an infected person at a specific time".[141] To learn who he interacted with, "the attackers keep a log of personal interactions. To learn "at which time he interacted with an infected person, the attacker proceeds in two steps: first, [he] creates multiple accounts in the proximity tracing system and uses them only for a short time [...]; second, if a notification arrives, he examines the corresponding account. Since the account was only used during a fixed time window, the attacker now knows that he was in close proximity to an infected person during that period".[142] Then, "by combining information from multiple time windows, the attacker can narrow down their list to a small group of people and, in some cases, single out infected individuals".[143] In some cases (such as for example when the user had contacts with a very limited number of people), re-identification of the infected individual is even possible "without additional data gathering" .[144]

65 Since the ROBERT consortium rates the aforementioned attacks as "significantly likely" to be performed,[145] the diagnosed users' EphIDs could be considered as personal data from the perspective of both the *exposed* and the *at risk app users*, under both a centralised and a decentralised approach. *Exposed app users*, as discussed in relation to the *Breyer* case in section B.II.2, are actually able to perform the re-identification attacks outlined above given that they have received a notification of exposure. *At risk app users*, in turn, could potentially be notified of an exposure, thereby becoming an exposed app user and thereby acquiring the means to identify diagnosed users on the basis of their EphIDs. The functioning of digital proximity tracing indeed makes the latter possibility "reasonably likely" to happen, even though the EphIDs of diagnosed users would only actually become identifiable to the at-risk app users after they have received that notification (Table 3 below).

66 By contrast, since both the re-identification attacks described above can only be performed once an individual has been diagnosed positive to COVID-19,[146] the EphIDs of other app users would not qualify as personal data from the perspective of the app user.

67 It follows that, from the perspective of the app user, the following processing operations would qualify as processing operations on personal data:

- *in both the centralised and decentralised protocol: the collection[147] and storage by an at-risk or exposed app user's phone of diagnosed users' EphIDs (phase 2);*
- *in the decentralised protocol: the use by an at-risk or exposed app user's phone of the diagnosed users' EphIDs in order to (potentially) match these EphIDs with the observed ones, and, subsequently, for purposes of risk-score computation (phase 4).*

4. Step 2.3: the qualification of users' EphIDs as personal data – perspective of the backend server

68 While the backend server (as explained above) is usually appointed by law as the controller, and the rest of the analysis considers the backend server's role as a controller as a given, in this paragraph we go beyond that legal fiction, to assess whether the users' EphIDs would also qualify as personal data from the backend server's perspective. We do so to illustrate one of the implications of combining the assessment of the "identifiability" of personal data with the one concerning (joint) controllership: potentially, an actor could qualify as a (joint) controller of data that, from that actor's perspective, are not personal.

69 We first consider the diagnosed users' EphIDs. When it comes to the centralised approach, it

[140] DP-3T Project (n 112) 5.

[141] ibid.

[142] ibid.

[143] See, for a fictional example: ibid.

[144] ibid 6.

[145] PRIVATICS Team INRIA (n 112) 7–8.

[146] ibid.

[147] If, as argued by some authors such as Finck and Pallas (n 9) 17, one assumes that "data becomes personal [only] at the moment that identification becomes possible", then we would have to discard collection as a relevant processing operation since, at that stage EphIDs are not identifiable yet but become identifiable only once the at risk app user has received the exposure notification (which means that - by definition - there is no collection of relevant EphIDs anymore). However, to avoid further complicating the already complex analysis, we considered collection as a relevant processing operation for the purpose of this contribution.

seems that the two consortia disagree on whether the backend server would be reasonably likely to re-identify the diagnosed individuals. According to the authors of the DP-3T protocol, the backend server can associate the EphIDs with their corresponding permanent identifiers, which could then "easily be related back" to their real identities.[148] Although the DP-3T members do not assess the likelihood of this event occurring, it follows that diagnosed users' EphIDs would qualify as personal, albeit pseudonymous, data.[149] The ROBERT consortium does not specifically discuss the likelihood of such re-identification attacks in a centralized protocol. However, it estimates the likelihood of attacks that could potentially lead to indirect re-identification (e.g. linkability of identifiers on the server or location tracing through access to the sever) as "limited",[150] in which case the diagnosed users' EphIDs would not qualify as personal data. By contrast, while this contribution does not intend to assess the exactitude of the claims made by both consortia, it seems that, in a decentralised approach, the backend server is not in a position to link the diagnosed users' EphIDs back to their identifiable form, since those are generated pseudo-randomly using the secret key created and stored on the app user's phone itself.[151] As such, they would not qualify as personal data vis-à-vis the backend server.[152] While, one might argue that such a conclusion has been implicitly endorsed by the recent case law of the CJEU according to which access to the personal data is not a prerequisite to qualify as a controller, this nonetheless raises the issue as to the relationship between the entities through which the risk of re-identification must be assessed and the ones that determine the purposes and the means of the processing. As hinted in section B.IV.2, the findings of the CJEU and the EDPB seem to indicate that the question of the allocation of responsibilities should be dissociated from the one related to the existence of a processing of personal data. As a result, one might end up in a situation—like here—where a given entity determines the purposes and the means, and therefore acts as controller, of a processing of data that qualify as personal from the perspective of another entity, but not its own.

70 Second, the other app users' (*i.e.* the non-diagnosed users') EphIDs could qualify as personal data from the perspective of the *backend server*. Indeed, the conclusion drawn above as to the qualification of diagnosed users' EphIDs would be equally applicable to other app users' EphIDs.

Table 3- EphIDs as data relating to an identifiable individual

Data	Perspective	Centralised COVID-19 app	Decentralised COVID-19 app
Diagnosed users' EphIDs	Backend server	Yes (DP-3T) / No (ROBERT)	No
	At risk and exposed app user	Yes	Yes
Other app users' EphIDs	Backend server	Yes (DP-3T) / No (ROBERT)	No
	App-user	No	No

II. Step 3: the joint participation in the determination of the purposes and means

71 As stated above, we take it as a given for this part of the analysis that the backend server, which we assimilate with the national health authority, acts as a controller by virtue of its legal appointment. The question that we intend to answer is whether the app user can be said to determine the purposes and the essential means of the processing *jointly* with the authority and, hence, act as joint controller with the latter in relation to the relevant processing operations identified in section F.I.3. above.

72 As mentioned above, when it comes to assessing joint controllership, each entity must first pursue a purpose "of its own"[153] and, hence, qualify as a controller in its own right. Only then is it possible to analyse whether the entities might *jointly* exercise influence on the purpose and means of such processing and hence qualify as joint controllers. As argued in section B.IV.1 and B.IV.3, the definition

[148] DP-3T Project (n 112) 18.

[149] ibid.

[150] See more specifically "LR2: Linkability of identifiers on the server" and "SR7: location tracing through access to a central server" in PRIVATICS Team INRIA (n 112) 12, 13.

[151] Troncoso and others (n 117) 7. See similarly: "SR 11: Re-identification of all infected users [new]" in PRIVATICS Team INRIA (n 112) 11.

[152] This conclusion is supported by the Data Protection Impact Assessment carried out on the DP-3T protocol: "Therefore, it must be considered, in line with the principles laid down above, and the test set out in Breyer (C-582/14, § 43), that the information stored on the backend server cannot be characterised as personal data from the point of view of the operator of the backend server." Id-Est avocats, 'Data protection impact assessment report" (2020) 17 < https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf> accessed 21 April 2021.

[153] European Data Protection Board (n 7) 21.

of "purpose" and "determining" will significantly impact the outcome of that assessment. The purpose of the processing operations could be defined as notifying at risk app users of a potential exposure to the virus. It could be argued that, by merely engaging in the aforementioned processing operations, the app users simply participate to the functioning of a system that was designed and adopted by somebody else to achieve that goal.[154] In that sense, the app user would not exercise any influence on the said purpose.

73 However, "determining" could also be defined more broadly as in materially contributing to certain processing operations and, consequently, allowing them to take place. In that sense, it can be argued that digital proximity tracing, and more specifically, the abovementioned processing operations, "would not be possible"[155] without the participation of the app user, who needs to install the app and turn it on when they are in the presence of other app users. Moreover, instead of merely looking at the objective purpose of the processing operations at issue, the purpose could be interpreted as the motivating factor driving each entity involved in the processing, as suggested by the relevant case law of the CJEU and the EDPB (see section B.IV.3 above). In this case, the app users could be said to pursue a purpose "of [their] own", *i.e.* preserving their own health or limiting the spread of the disease across their private circle of friends and relatives. This purpose can be regarded as "closely linked" or "complimentary" to the purpose arguably pursued by the legally designated controller, *i.e.* containing the virus and/or protecting the public healthcare system from saturation. Consequently, the processing operations at issue appear to mutually benefit the app users and the legally designated controller.

74 When it comes to the joint determination of the essential means, it has been argued that, since the app user does not have any configuration option, they cannot determine the "how" of the processing.[156] In other words, and to establish a parallel with the decision of the CJEU in *Wirtschafstakademie*, the app user does not have a say regarding the criteria (*i.e.* in the context of digital proximity tracing, the type of data collected, the retention period or the elements used to calculate the risk score, for instance) surrounding the functioning of the proximity tracing solution. Again, while this may be true under a strict interpretation of "determining the means", it may be at odds with the approach put forward in *Fashion ID* and the EDPB's Guidelines. That approach indeed indicates that the joint determination of the means could follow from an entity's choice to use a tool developed by another entity for its "own purposes".[157] By analogy, it could be said that app users jointly determine the means of the processing, by choosing to use a proximity tracing tool which was developed by another entity and which triggers the processing of other individuals' personal data for their *own* (private) purpose.

75 To conclude, if we look at the processing operations identified in section F.I.3 as a set of operations and consider the backend server and the app user as pursuing distinctive "own" purposes, they could be said to take "converging decisions" within the meaning of the EDPB's guidelines. Indeed, the processing operations at stake "would not be possible"[158] without, besides the participation of the legally designated controller, the participation of the app user, who needs to install the app and turn it on when they are in the presence of other app users.

III. Step 4: the "household exemption"?

76 Since, given the outcome of the analysis performed in sections F.I and F.II, app users could potentially qualify as joint controllers in relation to certain processing operations on other users' personal data, it is necessary to verify whether they could benefit from the so-called "household exemption".

77 First, it is worth noting that the processing operations detailed in section F.I.3 are unlikely to fall within the scope of "household" activities since they extend far beyond the app user's home or other places shared with his family members.[159] This is inherent to the functioning of digital proximity tracing solutions that are based on an app designed to be used on the go and holds true under both a centralised and decentralised scenario.

78 Second, the same could be said when it comes to their qualification as "personal" activities, although following a different line of thinking. As

[154] See, for instance: Kirsten Bock and others, 'Data Protection Impact Assessment for the Corona App' (2020) SSRN Electronic Journal 48 <https://www.ssrn.com/abstract=3588172> accessed 21 April 2021.

[155] European Data Protection Board (n 7) 19.

[156] Bock and others (n 154) 48.

[157] European Data Protection Board (n 7) 21.

[158] ibid.

[159] Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014], Opinion of Advocate General Jääskinen (n 102) para 51.

highlighted in section F.II, the collection, storing and, in a centralised solution, transmission of at risk app users' EphIDs serves both a general, public health-related and a private, more individualistic purpose. For that reason, one could argue that those processing operations do not "purely" relate to personal activities, regardless of their qualification as "personal". Given the privacy risks stemming from the use of both centralised[160] and decentralised[161] solutions, it is also difficult to argue that those processing operations do not "impinge upon the personal sphere of others",[162] even though the EphIDs of at-risk app users transmitted by the diagnosed app users to the backend server in a centralised scenario are not made accessible to an indefinite number of people. While irrelevant given the dual nature of those purposes, the question as to whether the interference is "significant" enough as to rule out the applicability of the household exemption remains subject to a case-by-case analysis.[163] Given the above, it is fairly reasonable to assume that the app user would not be able to rely on the household exemption.

G. The patchwork of answers

79 The first research question of this case-study was whether, given the broad interpretation of joint control, app users could qualify as controllers under the GDPR jointly with the legally designated controller (*i.e.* the national health authority, in most cases), with regard to the processing of other app users' personal data. If, as argued under section F.II, we take the view that app users pursue a purpose of their "own" when using the COVID-19 app (*e.g.* preserving their own individual health), and consider this purpose as being closely linked or complimentary to the one pursued by the national health authority (*e.g.* preserving public health), app users could qualify as *joint controllers* with the national health authority with respect to the processing operations identified in section F.I.3 (Tables 4 and 5 below). In that case, it is unlikely that these users would be able to rely on the household exemption laid down in Article 2(2)c GDPR. By contrast, if we consider that the app users do not pursue a purpose of their "own", the national health authority would qualify as a *sole controller* vis-à-vis the relevant processing operations by virtue of its legal designation (Tables 4 and 5 below). In essence, a lot will depend on the interpretation of open-ended notions such as "purpose" and "determining".

80 Second, and since the answer to the first research question can, at least in theory, be positive, we also wanted to know whether that outcome could be affected by the centralized or decentralized architecture of the proximity tracing solution. This does, *prima facie*, not seem to be the case. In other words, a situation of joint control between the legally designated entity and the app user seems, in theory, to be possible not only in (privacy preserving) decentralized solutions but also in the centralized protocol.

81 Third, we were interested in knowing whether the data processed by the (joint) controller(s) always qualify as "personal data" from the perspective of those entities. In other words, whether the perspective through which identifiability is assessed under Article 4(1) GDPR predefines the candidates for the role of controller. The answer seems to be negative. As highlighted in Tables 4 and 5 below, there are indeed situations where the actor that qualifies as a controller does not overlap with the actor for which the data at stake are to be regarded as personal. Only considering the actors for which the data are to be regarded as personal as potential candidates for the controller role could, therefore, lead to situations where the controller designated by law does not qualify as a controller in fact. This would create a mismatch between the legal fiction and the factual reality. In the decentralized protocol for example, the backend server (alone or together with the app user) could qualify as (joint) controller with respect to the collection and storage of diagnosed users' EphIDs, even though these EphIDs would not qualify as personal data from the perspective of the backend server (see Table 5 below). Conversely, treating the risk of re-identification independently from the allocation of responsibility could, especially in situations where (unlike in this specific use-case) there is no legally designated controller, result in an entity being qualified as a controller of data which, from its perspective, are non-personal, without even being aware of it. Both situations fail to meet the standard of legal certainty.

H. Time to close Pandora's box?

82 As mentioned in the beginning, this analysis was conceived as a thought provoking experiment. It does not provide a definitive answer to the

[160] PRIVATICS Team INRIA (n 112).

[161] DP-3T Project (n 112).

[162] Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014], Opinion of Advocate General Jääskinen (n 102) para 51.

[163] In our view, the mere risk for a diagnosed app user to be re-identified by an exposed app user following a unique notification should suffice to exclude the applicability of the household exemption.

question of the allocation of responsibilities under the GDPR in concrete digital proximity tracing solutions adopted in the fight against COVID-19. The purpose is rather to illustrate the complexities and ambiguities of the legal test for joint control under the GDPR. Following some scholars' line of thinking that "at this rate, everyone could be considered a [joint] controller of personal data",[164] we illustrated how, under a legally plausible interpretation of the existing test for joint control under the GDPR, even app users in the ROBERT and DP-3T COVID-19 proximity tracing protocols could, in theory, qualify as joint controllers. Considering the limitations of this study, further research, based on the concrete application of COVID-19 proximity tracing solutions in a specific national context is needed, in order to investigate whether this conclusion could hold true also in real life COVID-19 app use-cases. If that were the case, we would not consider this as a desirable outcome. First, it is difficult to imagine how an app user would be able to comply with all the obligations incumbent upon joint controllers. Second, Article 82 (4) GDPR suggests that that, in a case of joint controllership, both the national health authority and the app user could be held liable *vis-à-vis* the data subject for the entire damage caused by a possible infringement of the Regulation. The possibility (even if only theoretical) of facing liability claims under the GDPR might deter individuals from using the COVID-19 app and ultimately undermine the efficacy of the proximity tracing solution in combating the spread of the disease. This would be precisely the opposite of what countries deploying a COVID-19 app intended to achieve.

83 Unlike what we had hypothesized, the risk of running into joint-controllership situations seems to apply both to centralized and (so-called privacy-preserving) decentralized software architectures. As already argued by other scholars,[165] such risk may, however, discourage the adoption of privacy-preserving decentralized solutions.

84 Finally, and most importantly, the analysis revealed a fundamentally incoherent approach to key concepts delimiting the material and personal scope of application of the GDPR, such as the meaning of "identifiability" of personal data, "determining the purposes and means" and "access" to personal data when assessing (joint) control. We believe it is time for National Supervisory Authorities or, preferably, the EDPB, to start providing unequivocal and uniform guidance on these notions. If not, the lack of legal certainty, may end up endangering the credibility of the EU data protection system.

[164] Millard and others (2).

[165] Chen and others (n 4) 293.

Table 4- Outcome of the analysis – centralized protocol

Processing operation	**Joint determination of the purposes and means**	**Re-identification risk as assessed by the DP-3T consortium**	**Re-identification risk as assessed by the ROBERT consortium**
Collection and storage by an at risk or ex-posed app user of diag-nosed users' EphIDs	**Purposes:**“own”, closely linked/complimentary **Means:** use of means devel-oped by another entity for own purposes	*Joint control*	*Joint control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server)
	Purposes: the app user does not pursue his “own” pur-pose	*Sole control* (even though diagnosed users' EphIDs also qualify as personal data from the perspective of the app user)	*Sole control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server, whereas they do from the perspective of the app user)

Table 5- Outcome of the analysis – decentralized protocol

Processing operation	**Joint determination of the purposes and means**	**Re-identification risk as assessed by the DP-3T consortium**	**Re-identification risk as assessed by the ROBERT consortium**
Collection and storage by an at risk or ex-posed app user of diagnosed users' EphIDs	**Purposes:** “own”, closely linked/complimentary **Means:** use of means devel-oped by another entity for own purposes	*Joint control* (even though diagnosed users' EphIDs do not qualify as personal data from the perspective of the backend server)	*Joint control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server)
	Purposes: the app user does not pursue his “own” pur-pose	*Sole control* (even though diagnosed users' EphIDs do not qualify as personal data from the perspective of the backend server, whereas they do from the perspective of the app user)	*Sole control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server, whereas they do from the perspective of the app user)

Use by an at risk or exposed app user of the diagnosed users' EphIDs for matching and risk score compu-tation	**Purposes:** "own", closely linked/complimentary **Means:** use of means devel-oped by another entity for own purposes	*Joint control* (even though diagnosed users' EphIDs do not qualify as personal data from the perspective of the backend server)	*Joint control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server)
	Purposes: the app user does not pursue his "own" pur-pose	*Sole control* (even though diagnosed users' EphIDs do not qualify as personal data from the perspective of the backend server, whereas they do from the perspective of the app user)	*Sole control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server, whereas they do from the perspective of the app user)