University of New South Wales Law Research Series

WHEN A 'LIKE' IS NOT A 'LIKE': A NEW FRAGMENTED APPROACH TO DATA CONTROLLERSHIP

MONIKA ZALNIERIUTE AND GENNA CHURCHES

Forthcoming (2020) *The Modern Law Review*
[2020] *UNSWLRS* 7

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

forthcoming THE MODERN LAW REVIEW 2020

WHEN A 'LIKE' IS NOT A 'LIKE': A NEW FRAGMENTED APPROACH TO DATA CONTROLLERSHIP

MONIKA ZALNIERIUTE[*] AND
GENNA CHURCHES[†]

Abstract

In Fashion ID, the Court of Justice of the European Union ('CJEU') held that an operator of a website featuring a Facebook 'Like' button is a data controller under EU Directive 95/46 ('Directive') jointly with Facebook in respect of the collection and transmission of the personal data of website visitors to Facebook, but Facebook alone is a data controller for any subsequent data processing. While the CJEUs expansive interpretation of joint controllership aims to leave 'no gaps' in the protection of individuals, we question whether the proposed solution to 'fragment' controllership into different stages of processing helps to achieve that goal. We argue that CJEUs 'fragmented' approach is incompatible with the GDPR, as it does not reveal the intended purposes of data processing, and thus negates informed and specific consent. We suggest that such 'fragmentation' undermines the consistency, predictability and transparency of EU data protection law by obscuring the pervasiveness of data commodification in the digital economy.

[*] Fellow and Leader of 'Technologies and Rule of Law' Research Stream, Allens Hub for Technology, Law, & Innovation, Faculty of Law, UNSW Sydney, Australia.
[†] PhD Candidate, Member, Allens Hub for Technology, Law, & Innovation, Faculty of Law, UNSW Sydney, Australia. The authors are grateful for insightful comments and constructive feedback that anonymous reviewers provided on earlier drafts.

INTRODUCTION

Political and legal institutions, as well as the mainstream public, are beginning to grasp the enormous power so-called 'big tech' — or more accurately, 'big advertising' — exercise over our social, political and economic lives through data commodification and manipulation. Facebook, Google, Amazon, and a range of other companies are under intensifying pressure to ensure their data collection and processing complies with data privacy protections and is not used for unethical purposes.[1] These heightened levels of public engagement on data privacy issues and increased scrutiny of advertising and tech companies began after the Snowden revelations in 2013, and was recently re-energized by the Cambridge Analytica and 2016 US Election interference scandals.[2] Even the US seems to be shifting with California enacting a comprehensive data privacy law.[3] Meanwhile the CJEU continues to exert its prominent role in ensuring high levels of protection for personal data of individuals. Recently, it delivered several high-profile decisions

---

1 Many recent enforcement actions brought by the US and EU regulators illustrate this trend, see, eg, European Commission Press Release, 'Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising' (IP/19/1770, 20 March 2019); *Federal Trade Commission v Google LLLC and Youtube LLC*, [2019] FTC Case No 1:19-Cv-02642, Federal Court: District of Columbia; *Federal Trade Commission v Facebook Inc*, [2019] Case No 19-cv-2184, Federal Court: District of Columbia.

2 See, eg, UK House of Commons, *Digital, Culture, Media and Sport Committee*, 'Disinformation and 'fake news': Final Report', Eighth Report of Session 2017–19 (14 February 2019); United States Senate, *Select Committee On Intelligence*, 116th Congress, 1st Session Senate, 116-Xx 'United States Senate on Russian Active Measures Campaigns and Interference in the 2016 US Election' (2019).

3 California Consumer Privacy Act of 2018 § 1.81.5. [Cal. Civ. Code § 1798.100–1798.199].

on platforms' responsibility for removing harmful content,[4] the passivity and specificity of consent required for cookies,[5] and even revisited the geographical scope of the (in)famous 'right to be forgotten'.[6]

The prominence of data privacy issues in political and judicial agendas has been described as a constitutional moment for data privacy in the EU and USA.[7] In this rapidly evolving environment, on 19 January 2017, the Higher Regional Court of Düsseldorf ('Higher Regional Court') requested the EU judicature to ascertain whether an online retailer website with an embedded Facebook 'Like' plug-in, was a data controller for the purposes of the Directive.[8] The *Fashion ID* ruling,[9] delivered on

---

4 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (*Case* C-18/18) [2019] ECLI:EU:C:2019:821 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1965965>.

5 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* (Case C-673/17) [2019] ECLI:EU:C:2019:801 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2027422> ('*Planet49*').

6 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (Case C-507/17) [2019] ECLI:EU:C:2019:772 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1103956>.

7 See, eg, M. Zalnieriute, 'An international constitutional moment for data privacy in the times of mass-surveillance,' (2015) (23(2) *International Journal of Law and Information Technology* 99; N.M. Richards and W. Hartzog, 'Privacy's Constitutional Moment' (August 23, 2019) at <https://ssrn.com/abstract=3441502>.

8 Pursuant to Article 267 of the Consolidated Version of the Treaty on European Union [2008] OJ C115/13 ('TFEU'); see Oberlandesgericht Düsseldorf, Beschluss vom 19.01.2017 - I-20 U 40/16, <https://openjur.de/u/2157759.html>; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 ('Directive').

9 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* (C-40/17) [2019] ECLI:EU:C:2019:629

29 July 2019 by the Grand Chamber of the CJEU in response to this request, represents a powerful clarification of the contours of joint data controllership, with significant implications for website operators, social media platforms, the digital economy as well as the rights of individuals.

It is impossible to discuss all aspects of this judgment in the limited space provided. Instead, we focus on the implications of novel jurisprudence developed in *Fashion ID* — the 'staged' allocation of responsibility or what we term a 'fragmented' approach to joint data controllership. While the CJEUs expansive interpretation of joint controllership in *Fashion ID* aims to leave 'no gaps' in the protection of individuals, we question whether the Court's solution ultimately achieves that goal. We argue that limiting the responsibility of joint controllers by 'fragmenting' controllership into different stages of data processing is incompatible with the GDPR, as it does not reveal the *intended* purposes of data processing, and thus negates *informed* and *specific* consent. That is, such limited responsibility fails to account for the 'bigger picture' of data commodification and Fashion ID's *intended* purpose in permitting Facebooks further processing of the data — to create marketing and advertising opportunities for Fashion ID based on Facebooks extensive data pools, personal profiles of its users, and data-driven marketing techniques.[10] Limited responsibility does not require disclosure of the further data processing and its intended purposes. We therefore suggest that a 'fragmented' approach, developed by the Court in Fashion ID, undermines the consistency, predictability and transparency of EU data

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1973704> ('*Fashion ID*').

[10] A similar, albeit somewhat different, argument is also developed by R. Mahieu and J. van Hoboken, 'Fashion-ID: Introducing a phase-oriented approach to data protection?' *European Law Blog*, 30 September 2019.

protection law by obscuring the pervasiveness of data commodification in the digital economy.

Part I of this note provides the background of the *Fashion ID* dispute. Part II outlines the opinion of Advocate General ('AG') M. Bobek, while Part III focuses on the CJEUs judgment and its reasoning. Part IV analyses the expansion of the concept of 'data controllership' and its application under the *General Data Protection Regulation* ('GDPR').[11] Part V considers *Fashion ID* and 'fragmented' approach implications for the effectiveness of the EUs data protection regime to protect individuals in a digital economy, founded on data commodification.

FACTUAL AND LEGAL BACKGROUND

Fashion ID is a German fashion retailer with an online presence.[12] On its website, Fashion ID like many businesses, embedded a 'social plug-in'[13] provided by Facebook Ireland Ltd ('Facebook'). This plug-in enabled visitors to 'Like' Fashion IDs services but also transferred visitor information, including IP addresses, to Facebook even when visitors did not have a Facebook account or did not physically click the 'Like' button.[14]

---

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

[12] Fashion ID website <https://www.fashionid.de/> (last accessed 10 October 2019).

[13] Opinion of Advocate General Bobek: *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* (C-40/17) ECLI:EU:C:2018:1039 [2018] <http://curia.europa.eu/juris/document/document.jsf?docid=209357&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=1990380> (last accessed 10/10/2019) ('*Fashion ID*, AG') [70].

[14] *Fashion ID*, n 9 above, [27], [75], [83]; for an explanation of the session and permanent cookies involved see Landgricht Düsseldorf, Urteil vom 09.03.2016 - 12 O 151/15, <https://openjur.de/u/877553.html> [22].

A German consumer protection group, Verbraucherzentrale NRW, sought an injunction against Fashion ID in the District Court of Germany.[15] In particular, Verbraucherzentrale NRW alleged that Fashion ID failed to disclose the collection and use of personal data, to obtain and advise on the ability to revoke consent; and to inform users of social media how to avoid their data being collected.[16] The defendant, Fashion ID, claimed a lack of knowledge with respect to the collection and use of the data because it did not have access to the personal data transmitted to Facebook via the plug-in.[17]

The District Court largely agreed with Verbraucherzentrale NRW, imposing a 250,000 EUR fine on Fashion ID.[18] The Court did not accept that Fashion ID had a duty to inform social media users on how they can avoid their data being collected and linked to the users' own Facebook account.[19] Fashion ID appealed to the Higher Regional Court with Verbraucherzentrale NRW, cross-appealing the rejected plea.[20]

In the appeal proceedings, Fashion ID, with Facebook Ireland as intervenor, claimed consumer protection groups were not entitled to bring claims under the Directive.[21] Further, the scope of Fashion ID's and Facebook's obligations in connection with the data processing, such as the duty to inform consumers that their data was being collected and/or require their consent, depended on whether the online retailer was considered a 'data

---

15 Landgricht Düsseldorf, n 14 above.

16 *Fashion ID*, AG, n 13 above, [18]; Landgricht Düsseldorf, n 14 above, [26]-[32].

17 *Fashion ID*, n 9 above, [82]; note the Article 29 Data Protection Working Party had already stated that access to the data is not a precondition to being a controller, Article 29 Data Protection Working Party Opinion 1/2010 on the concepts of 'controller' and 'processor', Adopted on 16 February 2010, 00264/10/EN WP 169, 22 ('WP Opinion Controller and Processor').

18 Landgricht Düsseldorf, n 14 above.

19 Ibid.

20 *Fashion ID*, n 9 above, [31].

21 *Fashion ID*, n 9 above, [52].

controller' under the Directive.[22] The Higher Regional Court decided to stay the proceedings and, on 19 January 2018, referred these questions to the CJEU, requesting a preliminary ruling under Article 267 TFEU.[23]

OPINION OF ADVOCATE GENERAL

The AG delivered his opinion on 19 December 2018. He first reasoned organisations protecting consumer interests such as Verbraucherzentrale NRW were not prohibited from bringing legal action on behalf of data subjects under the Directive.[24] The AG argued the objective of the Directive to ensure 'effective and complete protection of the fundamental rights and freedoms of natural persons', endorsed national laws seeking 'to ensure a higher level of protection in the community'.[25]

The AG then provided a wide-ranging analysis on Fashion ID's status as a 'data controller'. Under the Directive, a 'controller' is a party 'which alone or jointly with others determines the purposes and means of the processing of personal data'.[26] Given recent CJEU jurisprudence in *Wirtschaftsakademie*[27] and

---

22 Oberlandesgericht Düsseldorf, n 8 above, [13]-[17], under German national law, if Fashion ID were not data controllers, they may have been a 'disturber' ('*Störer*') — a person who does not infringe a right, 'but has created or increased the risk of a third party infringement' and may be 'required to do what is reasonable and reasonable to prevent an infringement. If one rejects the defendant's own responsibility, the preconditions would lie here, since the defendant in any case created the danger through the integration of the plug-in that [Facebook] processes personal data'.

23 Ibid; *Fashion ID*, n 9 above, [42].

24 *Fashion ID*, AG, n 13 above, [23]-[49].

25 Ibid, [31].

26 Directive, n 8 above, art 5(d); note the examples provided in WP Opinion Controller and Processor, n 17 above, 14.

27 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, (C-210/16) ECLI:EU:C:2018:388 [2018] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543

Jehovan todistajat,[28] the AG opined that finding Fashion ID a data controller could be a forgone conclusion or a *'causa finita*'.[29] Nonetheless, the he proceeded to apply the jurisprudential test, first introduced in *Wirtschaftsakademie*,[30] for establishing joint controllership, which focuses on the ability of the party to determine the 'means and purpose' of the data processing.[31] In *Wirtschaftsakademie*,[32] the CJEU held that the administrator of the Facebook 'fan page' of a German education provider was a joint controller with Facebook, as the page administrator was able to set parameters on the target audience, defining other criteria and statistics thereby 'influencing' data processing.[33] In contrast, *Fashion ID* claimed it did not even have access to the data and was therefore unable to determine the 'means and purposes' of processing.[34]

The AG distinguished the 'influence' *Fashion ID* exerted from that of the page administrator in *Wirtschaftsakademie*. He reasoned that by its use of the Facebook plugin, Fashion ID set *some* parameters,[35] and that there was no requirement for the joint data controller to have access to the data or the 'fruits of joint labour'.[36] The AG highlighted that while Fashion ID and Facebook had a mutual or complimentary purpose for the

&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1087378> ('*Wirtschaftsakademie*').

28 *Tietosuojavaltuutettu (Data Protection Supervisor, Finland) with Jehovan todistajat — uskonnollinen yhdyskunta as Intervenor* (C-25/17) EU:C:2018:551 [2018] ('*Jehovan*').

29 *Fashion ID*, AG, n 13 above, [66].

30 *Wirtschaftsakademie*, n 27 above.

31 Opinion of the Advocate General Bot in *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, (Case C-210/16) ECLI:EU:C:2017:796 [2017] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=195902&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1087378#Footref7> [56], [73], [124]; *Wirtschaftsakademie*, n 27 above, [18], [36].

32 *Wirtschaftsakademie*, n 27 above.

33 Ibid, [36].

34 *Fashion ID*, n 9 above, [82], [69].

35 *Fashion ID*, AG, n 13 above, [69].

36 Ibid, [70], referring to *Jehovan*, n 28 above.

commercial use of the personal data,[37] the co-determining of the 'means and purposes' of data processing by *both* controllers was limited solely to the initial collection and transmission of the data to Facebook.[38] Thus, the AG recommended that Fashion ID should be found a joint controller with Facebook under Article 2(d) of the Directive, with Fashion ID's joint controllership responsibility limited to the initial collection and transmission of the data to Facebook.[39]

The referring Court also asked whose 'legitimate interests' for processing personal data are to be considered — Fashion ID's or Facebook's — where processing occurs without consent of the individual.[40] A 'legitimate interest' is one of several possible legal bases on which data controllers can rely for lawful processing, and can include workplace safety, security, research, including market research, enforcement of legal claim or marketing — the only limiting factor is that the reason be 'acceptable under the law'.[41] In response to the question, the AG noted the definition of 'legitimate interest' is 'elastic and open-ended', and could include 'advertising optimisation'.[42] He opined that both Fashion ID and Facebook's interests must be considered under Article 7(f) of the Directive because they act as joint controllers for the data processing.[43]

Finally, the AG addressed the scope of obligations arising from joint controllership, specifically who has a duty to inform,[44] and obtain consent from the data subject.[45] Consistent with his

37 Ibid, [105].
38 Ibid, [106].
39 Ibid, [106].
40 Ibid, [21].
41 Article 29 Data Protection Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, 844/14/ENWP 217, 24-25.
42 *Fashion ID*, AG, n 13 above, [123].
43 Ibid, [124], [127].
44 Directive, n 8 above, under Article 10.
45 Ibid, Articles 2(h) and 7(a); *Fashion ID*, AG, n 13 above, [21], referring to questions 5 and 6.

approach in determining the extent of joint data controllership, the AG recommended Fashion ID's obligations covered all aspects of the *joint* data processing operations, but not the *subsequent* stages of data processing performed by Facebook.[46] He suggested that in the interests of 'efficient and timely protection of data subjects' rights',[47] Fashion ID should receive consent,[48] and bear the duty to inform, but only to the extent of the collection and transmission of the information to Facebook.[49]

JUDGMENT OF THE COURT

On 29 July 2019, the CJEU issued its judgment that the operator of the website with an embedded Facebook plug-in is a data controller *jointly* with Facebook for the collection and transmission of personal data of website visitors. However, Facebook *alone* is a data controller for any subsequent processing. The Court noted the Directive was replaced by the GDPR on 25 May 2018, however, the Directive was applicable in this case as the proceedings in German Courts began in 2015.[50]

The CJEU commenced by rejecting Fashion ID's claim that consumer associations lacked legal standing to bring action against controllers under the Directive. Citing its earlier precedent, the Court recalled that the Directive did not fully

46 *Fashion ID*, AG, n 13 above, [131].
47 Ibid, [132].
48 Ibid, [132].
49 Ibid, [141].
50 Verbraucherzentrale NRW notified Fashion ID by letter on 1 April 2015 that the collection violated competition and telemedia law, Landgricht Düsseldorf, n 14 above, [20].

harmonise national laws in Member States, thus it did not preclude national legislation permitting such standing. [51]

The CJEU then focused on the core issue of the dispute — joint controllership. Citing earlier decisions in *Google Spain*[52] and *Wirtschaftsakademie*,[53] it reiterated that a broad definition of the concept of 'controller' was needed for the effective and complete protection of data subjects.[54] The Court highlighted that Article 2(d) of the Directive expressly contemplated the concept of a 'controller' relating to an entity 'which "alone or jointly with others" determines the purposes and means of the processing of personal data'.[55] The CJEU built on its earlier case-law in *Wirtschaftsakademie*[56] and *Jehovan*[57] in assessing who determined the 'purposes' and 'means' of the processing of personal data.[58]

In addressing Fashion ID's claims that it did not have access to the data in question, the Court affirmed the AG's opinion that, 'the joint responsibility of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned'.[59] Significantly, the Court delivered what could be considered the most important part of the judgment — the allocation of responsibility in controllership by 'fragmenting' data processing into different stages. This is the first time the CJEU has attempted to assign responsibility based

---

51 See *Fashion ID*, n 9 above, [57], [54], citing, to that effect, judgments of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito*, (C-468/10) and (C-469/10) EU:C:2011:777, [29] and of 7 November 2013, IPI, (C-473/12) EU:C:2013:715, [31].

52 *Google Spain and Google*, (C-131/12) EU:C:2014:317, judgments of 13 May 2014, [34].

53 *Wirtschaftsakademie*, n 27 above, [28].

54 *Fashion ID*, n 9 above, [66].

55 Ibid, [67].

56 *Wirtschaftsakademie*, n 27 above.

57 *Jehovan*, n 28 above, [69].

58 *Fashion ID*, n 9 above, [65]-[70].

59 Ibid, [69]; see, to that effect, *Wirtschaftsakademie*, n 27 above, [38]; and *Jehovan*, n 28 above, [69]; see also, WP Opinion Controller and Processor, n 17 above, 22.

on the 'stages' of processing, with great ramifications for the future interpretation of the GDPR:

> The existence of *joint liability* does not necessarily imply equal *responsibility* of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at *different stages* of that processing of personal data and to different degrees, with the result that the *level of liability* of each of them must be assessed with regard to all the relevant circumstances of the particular case.[60]

It thus found that Fashion ID had exercised influence over the initial collection of personal information and its transmission to Facebook, however, had no influence over any subsequent data processing by Facebook. The Court limited Fashion ID's controllership to the 'collection and disclosure by transmission of the personal data of visitors to its website'[61] because, the Court reasoned, it was 'impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter'.[62]

The Court then addressed Fashion ID's ability in determining the *means* of the data processing, finding that Fashion ID; 'embedded on its website the Facebook 'Like' button … while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website'.[63] As such, Fashion ID determined the 'means' of collection by exerting 'a decisive influence over the collection and transmission of the personal data of visitors … which would

---

60 *Fashion ID*, n 9 above, [70] (emphasis added), citing *Jehovan*, n 28 above, [66].
61 Ibid, [76].
62 Ibid, [76].
63 Ibid, [77].

not have occurred without that plugin.'[64] Therefore, Facebook and Fashion ID determined jointly 'the *means* at the *origin* of the operations involving the collection and disclosure by transmission of the personal data of visitors to Fashion ID's website'.[65]

Considering Fashion ID's ability to determine the 'purpose' of data collection and transmission, the CJEU emphasised that while the website has no control over the use of the transmitted data, the purpose of such collection is in part related to the website's benefit as it allowed better promotion of its products.[66] The Court concluded that Fashion ID did determine the purpose of the initial data collection, and further reasoned that Fashion ID's responsibility was even greater as it enabled 'Facebook to obtain personal data of visitors to its website' without them necessarily having any direct connection to the latter and irrespective of clicking the like button or the membership of Facebook.[67]

The Court then proceeded to assess whose 'legitimate interests' were to be balanced with those of data subject under Article 7(f) of the Directive in the case of joint controllership and absent individual consent. In this regard, the EU Commission has suggested that the e-Privacy Directive (which pursuant to Article 1(2) clarifies and supplements Data Protection Directive in the electronic communications sector) applies and requires the user's consent to be provided anyway, making the question about 'legitimate interests' irrelevant. [68] However, the CJEU held, agreeing with the AG, that the e-Privacy Directive only related to cookies, the use of which in this particular case was an

64 Ibid, [78].
65 Ibid, [79] (emphasis added).
66 Ibid, [80].
67 Ibid, [83].
68 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, 37–47.

issue for the referring Court to determine.[69] In the absence of such a finding, the CJEU proceeded to answer the question and held that 'each of those controllers should pursue a legitimate interest … through those processing operations in order for those operations to be justified in respect of each of them.'[70]

Finally, the Court turned to the obligations stemming from data controllership. It held Fashion ID had a duty to inform data subjects about the processing under Article 10 and to obtain consent under Articles 2(h) and 7(a) of the Directive. However, these obligations were again limited to the 'set of operations involving the processing of personal data in respect of which it [Fashion ID] actually determines the purpose and means'— the collection and transmission of the data to Facebook.[71] The Court reasoned that the collection of a data subject's consent by the plug-in operator would not be in line with efficient and timely protection of the individual rights, particularly as the plug-in operator, Facebook, is involved at a later stage of the processing, ruling the obligation fell to Fashion ID.[72]

Based on these arguments, the Court concluded that Fashion ID was a joint controller with Facebook, limited to the initial data collection and transmission to Facebook. Similarly, Fashion ID's obligations to obtain consent and duty to inform data subjects only extended to the collection and transmission of the data to Facebook.

---

69 See *Fashion ID*, AG, n 13 above, [90].

70 *Fashion ID*, n 9 above, [96].

71 Ibid, [100], the same language is also used at [99], [101], [102], [103], [105] and [106].

72 *Fashion ID*, n 9 above, [102].

EXPANDING THE CONTOURS OF DATA CONTROLLERSHIP

In *Fashion ID,* the CJEU extended its broad interpretation of a 'controller' to clarify the boundaries of the concept of 'joint responsibility' under EU data protection law. This expansive interpretation builds on the earlier CJEUs jurisprudence which extended joint responsibility to cases in which one party has very little control over the processing of personal data.[73] Importantly, such expansive interpretation is critical since many of the data protection obligations, now elaborated under the GDPR, apply only to data controllers.

CJEU's Concept of 'Joint Responsibility/Liability' vs GDPR's 'Joint Controllership'

The Court applied the now repealed Directive, under which controllers can 'jointly determine the purposes and means of processing', and further clarified the application of the CJEUs earlier developed concepts of 'joint responsibility' and 'joint liability'. While the Court has used these terms interchangeably in *Fashion ID,*[74] these concepts are different: 'liability' in general refers to answerability for legal obligations (in this case to data subjects),[75] whereas 'responsibility' refers to duties of the data controllers; to inform, obtain consents, and process data fairly. Such interchangeable use of these terms by the Court is

---

73 *Wirtschaftsakademie,* n 27 above; *Jehovan,* n 28 above.

74 Fashion ID, n 9 above, [69] refers to 'joint responsibility', [83] refers to 'responsibility', [70] refers to 'joint liability and liability', [85] refers to 'liability', [70] states: 'joint liability does not necessarily imply equal responsibility'; see also definitions provided in WP Opinion, *Controller and Processor,* n 17 above.

75 Black's Legal Dictionary defines the word 'liable' as 'bound or obliged in law or equity; responsible; chargeable; answerable; compellable to make satisfaction, compensation, or restitution'', see https://thelawdictionary.org/liable/, accessed 03 February 2020.

thus confusing, also stating that 'joint liability does not necessarily imply equal responsibility', without elaborating more precisely on the meaning of this phrase.[76] The Court did not address detailed provisions on responsibilities of 'Joint Controllers' under Article 26 of the GDPR, so the exact relevance of this decision to the GDPR remains uncertain. Some commentators and German Data Protection Authorities have previously interpreted the CJEUs concept of 'joint responsibility' as equivalent to the concept of 'joint controllership' under Article 26 of the GDPR, which states '*where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers*'.[77]

If the CJEUs concept of 'joint responsibility' or 'joint liability' is synonymous with the term 'joint controllership' under the GDPR, then the *Fashion ID* ruling suggests the threshold for joint controllership will also be low under the GDPR, and will not require equal responsibility or even access to data processed among joint controllers. Interestingly, since the GDPR came into effect, the market practice has been to interpret this concept of joint controllership narrowly in attempt to avoid any additional legal obligations flowing from such status.[78] Companies have instead preferred to characterise their relationships with other parties as either 'controller-processor', or 'independent controller-controller.[79] Such findings by the Court imply that joint controllership could be far more prevalent than previously

---

[76] *Fashion ID*, n 9 above, [70].

[77] GDPR, n 11 above, Article 26 (emphasis added); see, e.g, J. Paul, S. Assion, H. Niedenfuehr, 'What is next after the ECJ ruling on "Joint Control"', Bird & Bird, <https://www.twobirds.com/en/news/articles/2018/global/what-is-next-after-the-ecj-ruling-on-joint-control>.

[78] D. Tran and L. Adde, 'Joint Controller Relationships – More Prevalent Than Previously Thought?' (2019) *Privacy and Data Protection Journal*, 1 October 2019 <https://hsfnotes.com/data/2019/09/25/joint-controller-relationships-more-prevalent-than-previously-thought-article-published-in-privacy-and-data-protection-journal/>.

[79] Ibid.

thought and understood. Joint controllership could be found in wide range of circumstances: server hosting, peer-to-peer filesharing, even distributed ledger technologies such as blockchain.[80]

Duties of Website Operators and Plug-in Providers under Joint Controllership

While the exact applicability of 'joint liability/responsibility' jurisprudence to the GDPR is yet to be tested, the CJEUs clarification of an easily assumed joint controller relationship and associated duties stemming from it, matches well with those prescribed under Article 26 of the GDPR. Some suggest the GDPR has added unreasonable complexity for 'amateur' controllers. Arguably, a controllership arrangement with specific division of duties could reduce this complexity, however, this first requires a self-assessment of data controllership with obligations under the GDPR.[81]

Once aware of their status as controllers, website operators can: enter into joint controllership arrangements with social media plug-in providers to explicitly address responsibility and liability issues;[82] ask for consent and inform website visitors prior to sending their data for processing;[83] and, together with social media providers, designate a contact point to enable website visitors to exercise their data privacy rights against either the website operator or the social media plug-in

---

80 S. Wrigley, '"When People Just Click": Addressing the Difficulties of Controller/Processor Agreements Online' in M Corals et al, *Legal Tech, Smart Contracts and Block Chain, Perspectives In Law, Business and Innovation* (Springer Nature, Singapore, 2019), 223-228.

81 Ibid, 225.

82 GDPR, n 11 above, Article 26; the division or extent of liability was not addressed by the CJEU, despite using the term 'joint liability' in the judgment, *Fashion ID*, n 9 above.

83 GDPR, n 11 above, as required by Articles 4 and 13.

provider.[84] It is likely that website operators and social media plug-in providers will update their terms of use to include joint controllership agreements, similar to Facebook's action following the CJEUs *Wirtschaftsakademie* ruling.[85] However, due to an imbalance in bargaining power, larger players such as Facebook may seek to indemnify themselves from fines through the clauses in the agreements and terms of service with website operators. [86] The validity of the indemnifying clauses might not survive a legal challenge but smaller players in the market may not have much choice but to accept such clauses before a challenge occurs.[87]

LIMITING CONTROLLERHIP VIA FRAGMENTATION

The true significance of *Fashion ID* does not, however, end here. The Court did not stop at clarifying earlier jurisprudence and reaffirming the low threshold for joint controllership. Importantly, it also limited the reach of joint controllership, and — for the first time — articulated how controllers' responsibility should be divided based on the different 'stages' of data processing. The CJEU took the AG's recommendation to adopt and apply the approach first put forward (but not applied) in *Wirtschaftsakademie,*[88] and repeated it almost verbatim, holding that:

---

84 An issue mentioned in *Fashion ID*, AG, n 13 above, [135].

85 Paul, Assion, Niedenfuehr, n 77 above.

86 R. Mahieu, J. van Hoboken and H. Asghari, 'Responsibility for Data Protection in a Networked World' (2019) 1 *Jipitec* 39, 58.

87 Ibid 103-105.

88 *Fashion ID*, AG, n 13 above, [94], citing *Wirtschaftsakademie*, n 27 above, [44] (emphasis added): 'the existence of joint *responsibility* does not necessarily imply equal *responsibility* of the various operators involved in the

> existence of *joint liability* does not necessarily imply equal *responsibility* of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at *different stages* of that processing of personal data and to *different degrees*, with the result that the level of *liability* of each of them must be assessed with regard to all the relevant circumstances of the particular case.[89]

The Court has replaced 'joint responsibility' in *Wirtschakademie* with the word 'joint liability' in *Fashion ID* — arguably to avoid potential conflicting interpretations around the term 'responsibility',[90] and bring it closer to 'joint control' under Articles 26 and 82 of the GDPR.

Limited Joint Responsibility: Solely Collection and Transmission

Despite the peculiarities around wording, the Court limited Fashion ID's responsibility to the fragments or 'stages' of the data processing — the initial data *collection* and *transmission* of the personal data to Facebook.[91] By adopting this approach, the CJEU has limited the boundaries of joint controllership by regarding two actors as joint controllers *only* for the *stages* of processing where they determine *common* purposes and means of processing. Therefore, joint controllership might exist for

---

processing of personal data... those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of *responsibility* of each of them must be assessed with regard to all the relevant circumstances of the particular case.'

89 *Fashion ID*, n 9 above, [70], citing *Jehovan*, n 28 above, [66].

90 Such conflicting interpretations were possible, see, analysis in Paul, Assion, Niedenfuehr, n 77 above.

91 *Fashion ID*, AG, n 13 above, [102].

activities, such as data collection, but not for further processing, where one party might by solely responsible.

It seems this limitation was the Court's attempt to address the AG's concern that by 'making everyone responsible means that no-one will in fact be responsible'.[92] A situation where no one is responsible is, of course, antithetical to achieving high levels of protection for personal data. However, we argue below that fragmenting controllership and compartmentalising responsibility into different stages ultimately fails to achieve high levels of protection for several reasons.

Fragmentation Diminishes Predictability and Consistency of Data Protection Law

Firstly, allocation of responsibility under joint controllership on the basis of different stages of processing does not align well with the core principles of EU data protection law and undermines its predictability and consistency. In particular, it is important to note that neither the GDPR nor its predecessor, mention 'stages' in the definition of 'processing', which is defined as 'any operation or set of operations which is performed on personal data'.[93] The GDPR provides examples of operations constituting data processing: 'collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[94] However, as Mahieu and Hoboken note, it does not seem to imply a framework for classification of different stages of data

92 Ibid, [92].
93 GDPR, n 11 above, Article 4(2).
94 GDPR, n 11 above, Article 4(2); a similar list exists under Article 2(b) of the *Directive*, n 8 above.

processing.[95] Therefore, the allocation of responsibility under joint controllership does not seem to have a systematic premise, and will require a careful analysis of each 'stage' of processing on a case by case basis. This arguably reduces the predictability and consistency of the EU data protection law.

Fragmentation Obscures *Intended* Purposes of Data Processing

Second, we argue that such fragmentation undermines the fundamental principle of transparency of data protection law, which requires that individuals be informed of the *intended* purpose of processing when personal data is collected. Article 13(1) of GDPR mandates the controller to provide the data subject with:

> … c) the purposes of the processing for which the personal data are *intended* as well as the legal basis for the processing.[96]

The Court noted that Fashion ID installed the plug-in, 'in order to benefit from the commercial advantage consisting in increased publicity for its goods,' and that; 'those processing operations are 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.'[97] Therefore, the Court acknowledged the 'purpose' *intended* by Fashion ID was for Facebook to process the data to enable targeted advertising; in particular the promotion of Fashion ID's own products to the data subjects visiting their website, the 'friends' of those who

95 Mahieu, van Hoboken, n 10 above.
96 GDPR, n 11 above, Article 13(1)(c) (emphasis added).
97 *Fashion ID*, n 9 above, [80].

have 'Liked' the page, and even those who fit the 'profile' of interest in Fashion ID.

In this light, it is doubtful whether transmission of personal data to Facebook was the *only* purpose Fashion ID *intended* when installing the plug-in. Such a limited purpose could exist if Fashion ID collected personal data it later provided, or sold, to an unrelated body it does not interact with in a commercial way. However, considering Fashion ID *enabled* Facebook to collect the data and process it for *both* Fashion ID and Facebook's commercial purposes,[98] we argue Fashion IDs *intended* purposes go beyond the fragments of 'collection and transmission' of the data to Facebook, and cover *all* stages of data processing. Such limitation by the Court, therefore, obscures the *intended* purposes of data collection and processing.

Interestingly, it is not obvious whether the limitation of Fashion ID's controllership to initial collection and transmission despite the bigger commercial purpose implies that the 'means' *and* 'purposes' are cumulative elements and that responsibility only extends to the *stages* where both of these elements overlap. In comparison, Article 29 Working Party noted in its 2010 Opinion on controllers and processor, that 'Determination of the "purpose" of processing is reserved to the "controller". Whoever makes this decision is therefore (de facto) controller. The determination of the "means" of processing can be delegated by the controller, as far as technical or organisational questions are concerned.'[99] Whether the requirement is this cumulative in the joint controllership is important because *Fashion ID* seemed to have little control over the actual *means* by which the data was collected and transmitted, as data was directly harvested via the plug-in provided by Facebook. It remains for future CJEU jurisprudence to clarify whether the overlap of means and purposes is necessary for controllership to extend to a particular

98 *Fashion ID*, AG, n 13 above, [104]-[105].
99 WP Opinion Controller and Processor, n 17 above.

stage of data processing. Irrespective of such clarification, fragmentation obscures the intended purposes of data processing and principles of transparency along with it.

Fragmented Consent Undermines Transparency of Data Protection Law

Moreover, fragmenting joint controllership into stages further undermines transparency and overall effectiveness of data protection law by negating an *informed* and *specific* consent. In *Fashion ID*, consent obtained by the website operator only extended to the 'collection and transmission' of the data to Facebook.[100] We argue that requiring consent which covers only a *fragment* of the *overall* processing, renders it *uninformed* and *not specific*. Article 4(11) of the GDPR states:

> 'consent' of the data subject means any freely given, *specific, informed* and unambiguous indication of the data subject's … agreement to the processing of personal data ...[101]

A *specific* and *informed* consent and Fashions IDs duty to disclose the *intended* purposes of data processing depends on Facebook disclosing sufficient information about the processing to Fashion ID in the first place.[102] Falling short of such full disclosure, individual consent is simply not *specific* and *informed* under the GDPR and in turn, such processing does not have a legal basis. As Mahieu and van Hoboken have suggested

100 *Fashion ID*, n 9 above, [85].

101 GDPR, n 11 above, Article 4(11) (emphasis added); see also Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018, 17/EN WP260.

102 *Fashion ID*, AG, n 13 above, [81].

that 'as long as such information is not provided it [data collection via plug-in] should simply not be permitted.'[103] If Facebook fails to disclose sufficient information to website operators about what it does with the data, then Fashion ID should '*unlike*' Facebook plug-ins — that is, it should not use them.

However, Fashion ID will not stop using plug-ins because it has a commercial purpose in installing them. Similarly, Facebook will not simply start providing the specific information voluntarily — such a duty must be imposed on it. Therefore, it seems the idea of attempting to regulate Facebook and other advertising giants indirectly via small 'amateur' controllers,[104] such as Fashion ID, would work better if such 'amateurs' would bear full responsibility for data processing rather than a small 'fragment' bearing little resemblance to the overall commercial processing. This is the only way the fundamental principle of transparency under EU data protection law can be maintained.

Fragmentation Ultimately Obscures the Pervasiveness of Data Commodification

Ultimately, *Fashion ID* does not challenge the pervasiveness of data commodification, even though it seemed to comprehend the pervasiveness of the data collected, collated, correlated matched and linked. It reasoned that while Fashion ID enabled such commodification in the first place, it should not be responsible for the overall commodification. We concur with scholars such as Mahieu and van Hoboken that this 'fragmentation' ultimately

103 Mahieu, van Hoboken, n 10 above.

104 J. Globocnik, 'On Joint Controllership for Social Plugins and Other Third-Party Content–a Case Note on the CJEU Decision in Fashion ID' (2019) *IIC-International Review of Intellectual Property and Competition Law* 1033.

jeopardies the ability to recognise the 'societal risks posed by complex, networked, personal data processing systems such as in the case of a service provider like Facebook'.[105] This is particularly so when the sum of the fragments simply do not equal the risks to the rights and freedoms of data subjects when observing these complex systems as a whole.

It is a widely shared view that individuals actively and voluntarily share their data with advertising companies like Facebook.[106] In other words, that individuals are aware of commercial surveillance and its implications. However, *Fashion ID* is a firm example that this belief is a myth — individuals visiting Fashion ID's website actually lacked specific knowledge about the *intended* purposes of Facebook processing and could not be fully aware of the extensive scope of data surveillance. In fact, *Fashion ID* demonstrates that Facebook will have your data even if you did not press the 'Like' button, don't have an account, and did not visit Facebook's website. While the decision may cause Fashion ID to implement *some form* of consent before the collection occurs, that consent and information will not reveal the true and *intended* commercial extent of processing. Not only the did the CJEU in *Fashion ID* fail to challenge the pervasiveness of data commodification, it obscured it.

105 Mahieu, van Hoboken, n 10 above.

106 For general public and media views, see, e.g., Thomas Frank, Facebook users 'don't seem to care' about data scandal, fake news. Analyst says buy on the dip, CNBC News, 22 August 2018, https://www.cnbc.com/2018/08/22/facebook-users-dont-seem-to-care-about-data-scandal-analyst-says.html, accessed 03 February, 2020; citing a survey of 1,300 U.S. Facebook and Instagram users, of whom two-thirds were logged on the Facebook and Instagram accounts at least as much as a year before Cambridge Analytica scandal of 2018.

CONCLUSION

Fashion ID presented the CJEU with an unmissable opportunity to further elaborate on the contours of joint controllership. The CJEUs expansive interpretation of this concept aims to leave 'no gaps' in ensuring high levels of protection of personal data for individuals. The AG warned in his opinion that 'when too many people are made responsible for something then, ultimately, no-one is responsible.'[107] Aiming to avoid this vacuum, the Court proceeded to make sure that *joint* responsibility was kept to a minimum. In this case note we questioned whether the proposed solution to fragment controllership into different stages ultimately helps achieve that goal. We argued that such an approach is incompatible with the GDPR, as it does not reveal the *intended* purposes of data processing, and thus negates *informed* and *specific* consent. We suggested that fragmentation undermines the consistency, predictability and transparency of EU data protection law by obscuring the pervasiveness of data commodification in the digital economy. This obscurity cannot be unravelled until full and frank disclosures to enable *informed* and *specific* consent are required from both joint controllers. This obscurity cannot be disentangled unless the organisations permitting the harvesting of personal data, or advertising giants, such as Facebook, take full responsibility for the protection of the data they collect and commodify, often completely without our knowledge.

[107] *Fashion ID*, AG, n 13 above, [92].