Essay

The Battle for the Soul of the GDPR: Clashing Decisions of Supervisory Authorities Highlight Potential Limits of Procedural Data Protection

By Jordan Francis†

INTRODUCTION

For privacy professionals, 2023 got off to a big start as the Irish Data Protection Commission (DPC) announced €390 million in fines against Meta Platforms Ireland Limited ("Meta") for General Data Protection Regulation (GDPR)[1] violations by its services Facebook and Instagram.[2] Meta is no stranger to GDPR enforcement, having accumulated over €1 billion in fines over

† Legal Research Fellow, Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis. J.D., 2022, University of Minnesota Law School. I would like to thank the wonderful editors of the *Minnesota Law Review*, Professor Woodrow Hartzog, Professor Neil Richards, Cordell Institute Associate Director Patti Hageman, and my Cordell Institute colleagues Emily Doster and Oliver Khairallah for their insight, feedback, and support.

1. Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) [hereinafter GDPR].

2. Press Release, Data Protection Commission, Data Protection Commission Announces Conclusion of Two Inquiries into Meta Ireland, DATA PROTECTION (Jan. 4, 2023), https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland [https://perma.cc/8R57-VCRL] [hereinafter DPC Press Release]; TSA v. Meta Platforms Ir. Ltd., *In re* Instagram Service, ¶ 418 (Ir. Data Prot. Comm'n Dec. 31, 2022) [hereinafter DPC Instagram Decision]; LB v. Meta Platforms Ir. Ltd., *In re* Facebook Service, ¶ 10.45 (Ir. Data Prot. Comm'n Dec. 31, 2022) [hereinafter DPC Facebook Decision]; *see also* Vincent Manancourt, *€390M Fine Strikes Blow to Meta's Ad-Fueled Business Model*, POLITICO (Jan. 4, 2023), https://www.politico.eu/article/meta-fina-ad-business-model [https://perma.cc/QWR8-KBST].

the last year alone,[3] but these two decisions are notable for more than just the size of their fines.

The decisions centered around whether Meta followed the correct procedures when processing personal data for the delivery of behavioral advertisements on Facebook and Instagram. Many are already heralding these decisions as the beginning of the end for behavioral advertising,[4] arguing that Meta now has no choice but to obtain consent from data subjects to deliver behavioral ads (no easy feat under the GDPR).[5] Such celebrations may be premature, given that we have yet to see how the appeal process will play out or how Meta will (or will not) adapt its practices.[6] However, notwithstanding that uncertainty, these decisions do represent an existential threat to the behavioral advertising ecosystem and therefore warrant significant attention moving forward.

These decisions also shine light on a conflict that has been quietly brewing between data protection regulators. A schism is forming between the DPC and other authorities who enforce the GDPR across Europe. Because Meta's European headquarters are located in Ireland, the DPC takes the lead on GDPR complaints against Meta.[7] In recent years, concerned parties[8] have criticized the DPC for being overly favorable to companies like Meta.[9] This growing divide came to a head when the European

3. Ross Kelly, *Latest Meta GDPR Fine Brings 12-Month Total to More than €1 Billion*, IT PRO (Jan. 5, 2023), https://www.itpro.com/policy-legislation/general-data-protection-regulation-gdpr/369806/latest-meta-fine-brings-12-month-total-more-than-1-billion [https://perma.cc/5QZL-SSD7].

4. *See, e.g.*, Morgan Meaker, *The Slow Death of Surveillance Capitalism Has Begun*, WIRED (Jan. 5, 2023), https://www.wired.com/story/meta-surveillance-capitalism [https://perma.cc/GU3X-XP7M].

5. *Infra* Part I.A.

6. In March 2023, Meta announced that it was switching its legal basis for the processing of personal data for the delivery of behavioral ads to the "legitimate interest" basis, thus prolonging the legal dispute as to whether Meta must obtain consent for such data processing. Sam Schechner & Jeff Horwitz, *Meta to Let Users Opt Out of Some Targeted Ads, but Only in Europe*, WALL ST. J. (Mar. 30, 2023), https://www.wsj.com/article/meta-to-let-users-opt-out-of-some-targeted-ads-but-only-in-europe-44b20b6d. For more context on legitimate interests, see *infra* note 22 and accompanying text.

7. *See infra* Part I.B.

8. Like Austrian data protection advocate Max Schrems, whose nonprofit NOYB represented the complainants in these decisions.

9. *See* Derek Scally, *Schrems Criticises Irish Data Regulator After Facebook Case Breakthrough*, IRISH TIMES (Jan. 13, 2021), https://www.irishtimes.com/business/technology/schrems-criticises-irish-data-regulator-after

Data Protection Board (EDPB), a representative body of other EU data protection authorities, disagreed with the DPC's preliminary draft decisions in these disputes and ordered the DPC to change its findings.[10] In a surprising move, the DPC publicly criticized the EDPB for its involvement.[11] The different conclusions reached by the two bodies represent competing normative visions of the GDPR. The DPC's analysis in its draft decisions is symptomatic of the kind of rigid procedural formalism that can lead data protection regimes to facilitate or normalize data processing. The EDPB decisions, in contrast, embrace substantive principles—such as relational vulnerability and the primacy of privacy rights over business interests—to animate GDPR enforcement, thereby prioritizing stronger privacy protections for individuals. Which view will win in the long run remains to be seen, but these decisions portend future hostility between regulators.

Meta has announced plans to appeal these decisions concerning Facebook and Instagram,[12] and privacy professionals around the globe should wait with bated breath as this process plays out. The future of behavioral advertising is murky, and there are many different ways this situation could yet unfold. It remains to be seen whether these decisions will stand and how Meta will respond.[13] But the substance of the decisions and the conceptual differences underlying the divergent views of regulators make this nothing less than a battle for the soul of the GDPR.

This Essay proceeds in three parts. Focusing on the aspects of the decisions concerning the lawfulness of the data processing

-facebook-case-breakthrough-1.4457728 [https://perma.cc/JF2B-SE89]; Lindsay Clark, *Max Schrems Hits Irish Data Protection Commissioner with Corruption Complaint*, REGISTER (Nov. 24, 2021), https://www.theregister.com/2021/11/24/max_schrems_files_corruption_complaint [https://perma.cc/D9X7-QRA7]; Max Schrems (@maxscrehms), TWITTER (Jan. 12, 2023, 4:43 PM), https://twitter.com/maxschrems/status/1613667938581504000?s=20&t=GRZ4pyccoIV9RlZVACYV7g (criticizing the DPC for "gifting" Meta millions or billions of dollars by how the DPC calculated the fine in question).

10. DPC Press Release, *supra* note 2.

11. *Id.*

12. Meta, *How Meta Uses Legal Bases for Processing Ads in the EU*, ABOUT FB (Jan. 4, 2023), https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu [https://perma.cc/E3MZ-F9V9] [hereinafter *How Meta Uses Legal Bases*].

13. Even if affirmed, Meta will still resist the calls to rely on consent, instead buying time while trying its luck with the "legitimate interests" basis.

in question, Part I briefly explains key GDPR concepts such as lawful bases and the Article 65 dispute resolution process. Part II then walks through the portions of the Instagram decision concerning whether Meta could rely on performance of a contract as the lawful basis for the delivery of behavioral ads, examining how the DPC and EDPB each analyzed the relevant issues. Finally, Part III contrasts the differing ideological approaches of the DPC and EDPB and explores the implications of this growing rift, arguing that the EDPB's embrace of substantive principles such as relational vulnerability further the GDPR's objectives and should serve as a guide for US policymakers.

I. GDPR FUNDAMENTALS: LAWFUL BASES AND THE EDPB'S ROLE IN ENFORCEMENT

The GDPR, seen as the gold standard for protecting privacy in the digital age, has been called "the toughest privacy and security law in the world."[14] Privacy and data protection are fundamental rights in the EU,[15] and the GDPR protects those rights through its comprehensive regulatory framework. Article 5(1)(a)—one of the GDPR's primary provisions—lays down the general principle that data must be "processed lawfully, fairly and in a transparent manner in relation to the data subject."[16]

Data protection models like the GDPR work to uphold an individual's right to control how data about them are used.[17] Whereas substantive privacy rules prohibit certain uses of data, data protection is largely procedural, focusing instead on ensuring that adequate safeguards surround any data processing. The

14. Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?*, GDPR, https://gdpr.eu/what-is-gdpr [https://perma.cc/P8BV-79H6].

15. The EU's Charter of Fundamental Rights guarantees "the right to the protection of personal data" as well as the requirement that "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned *or some other legitimate basis laid down by law*." DPC Instagram Decision, *supra* note 2, ¶ 65 (citing EU Charter of Fundamental Rights, Article 8) (emphasis added).

16. *Id.* ¶ 66 (citing GDPR art. 5(1)(a)). This principle is reinforced by GDPR recitals 39 and 40, which provide that "[a]ny processing of personal data should be lawful and fair," and that "[i]n order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law." *Id.*

17. Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 980 (2021) (citing WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 165, 257–58 (2016)).

GDPR accomplishes this through strong default protections, individual rights, and comprehensive, rule-based safeguards that ensure data processing is fair and transparent. Two aspects of the GDPR most relevant to these decisions are (1) its default prohibition on data processing without a lawful basis and (2) its dispute resolution mechanism for conflicts between regulators.

A. DATA PROCESSING PROHIBITED BY DEFAULT

One of the GDPR's defining features is its default prohibition on data processing.[18] Article 6 provides that data processing "shall be lawful only if and to the extent" that at least one of six lawful bases applies. This is a flexible, standards-based approach founded on the normative theory that data use is legitimate only in select situations, which entails that a data controller point to one of six statutory bases before processing personal data.[19] The GDPR also requires data controllers[20] be transparent as to which lawful basis they are relying on for their processing operations.[21] The two lawful bases most relevant[22] to these decisions are consent and performance of a contract:

18. The charter mandates that data processing occur only where there is a legitimate basis laid down by law. DPC Instagram Decision, *supra* note 2, ¶ 65.

19. *See* Mark MacCarthy, *What U.S. Policymakers Can Learn from the European Decision on Personalized Ads*, (Mar. 1, 2023) https://www.brookings.edu/blog/techtank/2023/03/01/what-u-s-policymakers-can-learn-from-the-european-decision-on-personalized-ads.

20. A data controller is a "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." GDPR art. 4(7). In simple terms, a data controller determines both *why* and *how* personal data are processed. *See* Eur. Comm'n, *What Is a Data Controller or a Data Processor?*, EUROPA, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en [https://perma.cc/F95M-NJ64].

21. Article 5 mandates that data be processed "lawfully, fairly and *in a transparent manner*." GDPR art. 5(1)(a) (emphasis added). Article 13 reinforces this by requiring controllers provide certain information to a data subject when personal data are collected, obtained, and processed. *See* GDPR art. 13. Two of the things that a controller must disclose are its purpose for processing personal data as well as the legal basis for doing so. GDPR art. 13(1)(c).

22. Although not raised in these decisions, "legitimate interests" is another lawful basis that many people expected Meta to try to rely on in the future if it opted against trying to rely on consent. As of March 2023, Meta has adopted this strategy. Schechner & Horwitz, *supra* note 6. Legitimate interests is framed as a balancing test, weighing the interests of a data controller in processing personal data against the "interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular

> (a) the data subject has given ***consent*** to the processing of his or her personal data for one or more specific purposes;
>
> (b) processing is necessary for the ***performance of a contract*** to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.[23]

Consent. Under the GDPR, consent means something very different than in American privacy law.[24] In the U.S., consent ties to the concept of "notice and choice" whereby a company gives consumers notice of its data practices via a privacy policy and by choosing to use that service, consumers "consent" to those data practices.[25] Consent under the GDPR is both more meaningful and less consequential. As one of six lawful bases, consent

where the data subject is a child." GDPR art. 6(1)(f). Social media juggernaut TikTok caused waves in July 2022, when it halted plans to switch the lawful basis that it relied on for the delivery of behavioral advertisements from consent to legitimate interests. Natasha Lomas, *TikTok 'Pauses' Privacy Policy Switch in Europe After Regulatory Scrutiny*, TechCrunch (July 12, 2022), https://techcrunch.com/2022/07/12/tiktok-pauses -privacy-policy-switch [https://perma.cc/7SD8-LUYQ]. In the lead-up to the pause on its plans, TikTok had been in dialog with the Irish DPC concerning the switch. *Id.* Italy's supervisory authority had also issued a warning to TikTok that the switch would violate the ePrivacy Directive, another EU privacy law. Eur. Data Prot. Bd., *TikTok: Italian SA Warns Against 'Personalised' Ads Based on Legitimate Interest*, EDPB EUROPA (July 7, 2022), https://edpb.europa.eu/news/national-news/2022/tiktok-italian-sa-warns-against-personalised-ads -based-legitimate-interest_en [https://perma.cc/6A46-ML9H]. While there is no decision formally prohibiting companies from relying on legitimate interests to justify the delivery of behavioral ads, there are serious doubts about whether such practices would satisfy the required balancing test, and TikTok's stalled switch from consent to legitimate interests reinforces that doubt. Lomas, *supra*. The GDPR also limits the use of legitimate interest as a basis for direct marketing, granting data subjects an absolute right to opt-out. GDPR art. 21. Mark MacCarthy, *The European Data Protection Board (EDPB) Goes After Tech's Personalized Ad Business Model*, BROOKINGS (Feb. 1, 2023), https://www.brookings.edu/blog/techtank/2023/02/01/the-european-data-protection-board-goes-after-techs-personalized-ad-business-model.

23. GDPR art. 6(1) (emphasis added).

24. *See* Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 107–09 (2021) (explaining how the GDPR is not a "consent" based regime as some Americans have stated).

25. Notice and choice has been criticized as being overwhelming, illusory, and ineffective. *See* Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423 (2018); ACLU of Mass., *Rise of the Surveillance State*, FREEDOM UNFINISHED (Sept. 26, 2022), https://www.freedomunfinished.com/1983514/11374637 [https://perma.cc/2YYZ-R3LZ]; *see also* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013); Neil Richards, Woodrow Hartzog

plays a limited role; a controller does not *have to* rely on consent to process personal data.[26] But consent is simultaneously more meaningful because it is harder to obtain[27]—it must be freely given, specific, informed and unambiguous.[28] With additional protections surrounding consent,[29] including the requirement that performance of a contract cannot be made conditional on consent to personal data processing that is not necessary for the performance of that contract,[30] the net effect is a heightened consent standard which makes it desirable for controllers to find an alternative lawful basis wherever possible.

Performance of a Contract. Where a controller enters into a contract with a data subject, the controller can process that data subject's personal data to the extent that doing so is necessary for the fulfillment of that contract.[31] This lawful basis has several critical ambiguities.[32] What is a contract? What is

& Jordan Francis, *Comment Submitted by Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis on the Prevalence of Commercial Surveillance and Data Security Practices that Harm Consumers* 47–59 (Nov. 21, 2022), https://papers.ssrn.com/abstract_id=4284020 [https://perma.cc/3G2A-HPX4] (Comment ID: FTC-2022-0053-1071) (describing the failures of notice and choice and an overreliance on consent).

26. Jones & Kaminski, *supra* note 24, at 109 ("When Americans characterize the GDPR as a solely consent-based law, they are wrong. Most businesses subject to the GDPR process personal data either under the individual consent ground or the legitimate interest ground.").

27. *See* Ben Wolford, *What Are the GDPR Consent Requirements?*, GDPR, https://gdpr.eu/gdpr-consent-requirements [https://perma.cc/V3GE-6K27].

28. Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." GDPR art. 4(11).

29. Article 7 provides further conditions for consent, namely that: (1) where consent is relied upon, the controller must be able to demonstrate that consent was given by the data subject; (2) a written request for consent must be "clearly distinguishable from the other matters," "in an intelligible and easily accessible form," and "using clear and plain language"; (3) consent can be withdrawn; and (4) "[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." GDPR art. 7.

30. *Id.*

31. Recital 44 adds little context: "[p]rocessing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract." GDPR rec. 44 (emphasis added).

32. For guidance on the contract basis, see Info. Comm'r's Off., *Contract*, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the

necessary for the full *performance* of a contract? To what degree is a supervisory authority, which is not a court, competent to pass judgment on substantive matters of contract law? The EDPB[33] previously issued guidance on how to apply the contract basis, but questions remain concerning its scope.

B. THE ARTICLE 65 DISPUTE RESOLUTION PROCESS PROMOTES CONSISTENT GDPR ENFORCEMENT

Supervisory authorities (SAs)[34] are independent public authorities responsible for enforcing the GDPR and upholding the fundamental right of data protection in their respective member states.[35] The DPC is Ireland's supervisory authority.[36]

Relying on SAs for enforcement creates problems for controllers who operate in multiple EU member states and engage in cross-border data processing.[37] For those controllers, it could be extremely burdensome to engage with more than two-dozen dif-

-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract [https://perma.cc/VD7R-LKDQ].

33. *See infra* Part I.B.

34. Sometimes called a data protection authority (DPA).

35. The GDPR requires every member state establish its own SA. GDPR art. 51. Chapter 6 addresses the basic role of SAs, including their purpose, features, tasks, and powers. GDPR ch. 6. *See also* Int'l Ass'n Privacy Pros., *Supervisory Authority*, IAPP, https://iapp.org/resources/article/supervisory-authority [https://perma.cc/P6X3-2T29].

36. The DPC was established by the Data Protection Act 2018, which implemented the GDPR in Ireland'. Data Protection Act 2018 (Act No. 7/2018) (Ir.), https://www.gov.ie/en/publication/65865-data-protection-act-2018 [https://perma.cc/ZNC6-57RB]; *see also* Ir. Data Prot. Comm'n, *Who We Are*, DATA PROTECTION, https://www.dataprotection.ie/en/who-we-are [https://perma.cc/UG54-SYDK].

37. Cross-border data processing means either: (a) "processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State"; or (b) "processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State." GDPR art. 4(23).

ferent SAs. The GDPR was built with a unique mechanism designed to address this: the "one-stop shop."[38] Article 56 introduces the concept of a "lead supervisory authority" (LSA).[39] LSAs are assigned based on geographic location of a controller's main establishment (when the controller is engaged in cross-border data processing).[40] For example, Meta engages in cross-border data processing and has its main establishment in the EU in Ireland, so the DPC (Ireland's SA) is Meta's LSA.[41] GDPR complaints across the EU are referred to a controller's LSA, relieving the controller of the burden of engaging with multiple SAs.[42]

Relying on SAs for enforcement within their respective member states creates another problem: inconsistent enforcement. That risk is heightened when a controller (especially one as consequential as Meta) is subject to an LSA, who thus has outsized influence on the data practices of a controller which implicate the rights of citizens in other member states. To combat that risk, GDPR chapter 7 addresses consistency and cooperation between SAs.[43] One key institution is the EDPB, an independent body composed of representatives from various SAs whose purpose is to foster consistent application of the GDPR.[44] LSAs are required to cooperate and exchange information with the various SAs, which entails "submit[ting] a draft decision to

38. The "one-stop shop" is a colloquial term for the GDPR's consistency mechanism. Int'l Ass'n Priv. Pros., *One-Stop Shop*, IAPP, https://iapp.org/resources/article/one-stop-shop [https://perma.cc/5HJB-HD97] [hereinafter *One-Stop Shop*].

39. GDPR art. 56.

40. *Id.* Determining which SA is a controller's LSA sometimes can be a challenging affair. Deirdre Kilroy, *Is It Possible to Choose Your Lead Supervisory Authority Under the GDPR?*, IAPP (Nov. 28, 2017), https://iapp.org/news/a/is-it-possible-to-choose-your-lead-supervisory-authority-under-the-gdpr [https://perma.cc/T7JV-4PGJ].

41. DPC Instagram Decision, *supra* note 2, app. 1, ¶ 12 ("The Investigator was also satisfied that the Commission was the lead supervisory authority (the 'LSA') as set out in the GDPR for the purposes of this matter on the basis that (i) Meta Ireland has its main establishment (for the purposes of the GDPR) in Ireland and (ii) that the processing at issue in the Complaint constitutes cross-border processing.").

42. *See* Int'l Ass'n Priv. Pros., *Lead Supervisory Authority*, IAPP, https://iapp.org/resources/article/lead-supervisory-authority [https://perma.cc/CH3V-M4ED]; *One-Stop Shop*, *supra* note 38.

43. *See generally* GDPR ch. 7 (covering "cooperation and consistency" between supervisory authorities).

44. GDPR art. 68; *see also Who We Are*, EDPB, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en [https://perma.cc/7B9T-CY3D].

the other supervisory authorities concerned for their opinion and tak[ing] due account of their views."[45] These concerned supervisory authorities (CSAs) act as a check on the LSA. If one or more CSAs object to the draft decision,[46] the LSA and CSAs enter a consultation process. If that fails, the dispute is referred to the EDPB, who can then make binding determinations by majority vote.[47] The LSA will then publish the Article 65 decision resolving the dispute. This process by which the EDPB issues a binding decision is the Article 65 dispute resolution process, which was invoked in these decisions concerning Meta.

II. CLASH OF THE SUPERVISORY AUTHORITIES

On the eve of the GDPR taking effect, Meta switched its legal basis for the delivery of behavioral ads on Facebook and Instagram from consent to performance of a contract.[48] NOYB, a data protection nonprofit, filed complaints on behalf of two data subjects against Facebook and Instagram respectively.[49] Focusing on the Instagram decision from here on out,[50] the factual basis of the dispute is that after Instagram updated its terms of

45. GDPR art. 60(3). A supervisory authority is concerned where "(a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority." *Id.* art. 4(22).

46. An objection must be "relevant and reasoned," *Id.* art. 60(4), which is defined as "an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union," GDPR art. 4(24). The EDPB has issued guidance on what constitutes a "relevant and reasoned" objection. *See* EUR. DATA PROT. BD., GUIDELINES 09/2020 ON RELEVANT AND REASONED OBJECTION UNDER REGULATION 2016/679 (Mar. 09, 2021), https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202009_rro_final_en.pdf [https://perma.cc/VM7N-XPVF].

47. GDPR art. 65.

48. Under the GDPR's predecessor law, Meta relied on consent as the legal basis for the delivery of behavioral advertisements, but the GDPR heightened the requirements for consent. *Id.*; DPC Instagram Decision, *supra* note 2, ¶ 8.

49. *See* DPC Instagram Decision, *supra* note 2, app. 1, ¶ 14; GDPR art. 80 (giving data subjects the right to have a non-profit file complaints on their behalf); *Our Detailed Concept*, NOYB, https://noyb.eu/en/our-detailed-concept [https://perma.cc/X2HP-3PZV].

50. The substance of the two decisions is the same, so this Essay chose to focus on the Instagram decision for the sake of readability.

use, users were met with an engagement flow which guided them through accepting the updated terms.[51] This included two pages entitled "Review and Agree."[52] The first contained a subheading "Changes to How We Manage Data" and linked to Instagram's Data Policy. Clicking "next" led users to a second page which asked for confirmation that they were over the age of 18, provided a high-level overview of changes to the terms, linked to the full text of the updated terms, and gave users a binary choice: "Agree to Terms" or "See other options."[53] Selecting the latter presented users with one choice: deletion of their account.[54]

NOYB took issue with both the "accept or delete" ultimatum and the lack of transparency regarding which lawful basis Meta relied on for processing.[55] The DPC distilled the complaint into three issues:

> **Issue 1** – Whether clicking on the "Agree to Terms" button constitutes or must be considered consent for the purposes of the GDPR and, if so, whether it is valid consent for the purposes of the GDPR.
>
> **Issue 2** – Whether Meta Ireland could rely on Article 6(1)(b) GDPR as a lawful basis for processing personal data in the context of the Terms of Use and/or Data Policy.
>
> **Issue 3** – Whether Meta Ireland provided the requisite information on the legal basis for processing on foot of Article 6(1)(b) GDPR and whether it did so in a transparent manner.[56]

51. DPC Instagram Decision, *supra* note 2, ¶ 9.

52. *Id.*

53. *Id.* ¶ 10. "Agree to Terms" was much more prominent than "See other options."

54. Reinforcing this "accept or delete" dichotomy, the updated terms specified that continuing to use Instagram required accepting the new terms, and users who did not wish to accept could delete their account. *Id.*

55. In NOYB's view: forcing users to choose between agreeing to terms or deleting their account meant that Meta was relying on consent as its lawful basis; such consent could not be valid because it was not freely given or informed; users were misled into thinking that some processing operations fell under Article 6(1)(b) (contract) rather than 6(1)(a) (consent); processing personal data for the delivery of behavioral advertisements was impermissible under Article 6(1)(b); and Meta was not transparent when it listed multiple lawful bases in its privacy policy without specifying which basis each processing operation relied upon. *Id.* ¶¶ 12–18.

56. The Investigator (who carried out the initial preliminary investigation on behalf of the DPC) identified four issues rather than three: (a) whether acceptance of the Terms of Use/Data Policy constituted consent under Articles 4(11) and 6(1)(a) to the processing of personal data; (b) whether Meta could rely on Article 6(1)(b) (contract) as a lawful basis for the processing of personal data in respect of the Terms of Use; (c) whether Meta misrepresented the legal basis for processing in a way that would lead the data subject to believe that Meta

The final decisions imposed fines[57] for incorrectly relying on contract as a legal basis for the delivery of behavioral advertising and failing to be transparent as to which lawful basis justified Meta's processing operations.[58] The transparency violations proved less controversial than other aspects of the decisions,[59] so this Essay will focus on the DPC and EDPB's divergent views regarding consent and contract.

A. WHETHER META OBTAINED (OR NEEDED) CONSENT

The DPC divided Issue 1 into two questions: (i) whether clicking on "Agree to Terms" constituted consent,[60] and (ii) whether Meta was *required* to rely on consent to process personal data to deliver the Terms of Service. After reiterating the high standards for obtaining consent,[61] the DPC summarized the

was relying on consent as its legal basis; and (d) whether Meta failed to provide information as to its legal basis in the Terms of use/Data Policy in violation of its transparency obligations. *Id.* at ¶ 23. The DPC Commissioner, however, viewed (c) and (d) as duplicative and hence combined the two into one inquiry. In her view, "both issues are components of the same question of whether Meta Ireland has complied with its transparency requirements in respect of processing carried out on the basis of Article 6(1)(b)," because "where a controller has not complied with its transparency requirements, it logically follows that a data subject may be misled, deliberately or otherwise, as to legal basis of any processing in this context." *Id.* at ¶ 26.

57. €210 million in the Facebook inquiry and €180 million in the Instagram inquiry. DPC Press Release, *supra* note 2.

58. DPC Press Release, *supra* note 2; *see also* Jennifer Bryant, *Irish DPC Fines Meta 390M Euros Over Legal Basis for Personalized Ads*, IAPP (Jan. 4, 2023), https://iapp.org/news/a/irish-dpc-fines-meta-390m-euros-over-legal-basis-for-personalized-ads [https://perma.cc/3VDX-YXMW].

59. In short, DPC and EDPB agreed that the engagement flow created the impression that the lawful basis for processing was consent, but Meta was actually relying on contract, thereby violating the principles of transparency embodied in Articles 5(1)(a), 12(2), and 13(1)(c). DPC Instagram Decision, *supra* note 2, ¶ 199.

60. The DPC viewed this as two issues: whether clicking "Agree to Terms" actually constitutes consent and whether clicking "Agree to Terms" *necessarily* must be considered consent for such purposes. *Id.* ¶ 34. The distinction is not relevant to the main point of this Article.

61. Consent must be a "freely given, specific, informed and unambiguous indication" of the data subject's agreement to data processing; it can take many forms, such as ticking an unchecked box or some other action that "clearly indicates" agreement, but it does not extend to "[s]ilence, pre-ticked boxes or inactivity"; a request for consent must be clearly distinguishable from other matters; consent can be withdrawn; and the performance of a contract cannot be made conditional on consent to data processing that is not necessary for the performance of that contract. *Id.* ¶¶ 36–38 (citing GDPR arts. 4(11), 38, & rec. 32).

parties' arguments.[62] NOYB argued that by requiring users to accept terms or delete their accounts, Meta was asking individuals to consent to the data policy bundled alongside the Terms of Use but that any such consent would be invalid because it is not freely given and informed.[63] Meta maintained that it was not relying on consent and that clicking "Agree to Terms" amounted to a contractual agreement. The DPC's draft decision largely agreed with Meta. It concurred that Meta did not consider clicking "Agree to Terms" as consent;[64] it viewed the text of the Data Policy as merely explaining Meta's data practices and as a clear statement that Meta did not "intend to rely on consent for all data processing in the context of the Instagram service";[65] and it stated that all parties agreed that "acceptance of the Terms of Use was not valid consent."[66] The DPC thus proposed finding that clicking on the "Agree to Terms" button did not constitute consent under the GDPR. The EDPB, however, ordered the DPC to remove its proposed conclusion on Issue 1, rendering the DPC's finding on this first question non-binding.[67]

The DPC also expressed its view on NOYB's second argument—that consent is *the only* lawful basis that Meta could rely on to process personal data in connection with Instagram and any processing was therefore unlawful as consent had not been obtained.[68] NOYB argued that the applicability of Article 6(1)(b) should depend on the nature of the contract. In NOYB's view, contracts which are "primarily [for] data processing" must rely on consent, whereas contracts which concern "primarily some other contractual service" can rely on Article 6(1)(b).[69] Otherwise, a controller could circumvent consent requirements by presenting declarations of data practices as contractual provisions. The DPC disagreed, stating that Article 6(1) does not "require

62. *Id.* ¶ 36 (citing GDPR art. 4(11)). For clarity, when this Essay says "NOYB argued" or "Meta argued," it is referring to how the DPC summarized and characterized those arguments in its decision, not necessarily how those arguments may have appeared in either party's submissions.

63. *Id.* ¶¶ 15–17. NOYB also alleged that the deceptive design of the user engagement flow misled data subjects and "forced" consent. *Id.* ¶ 40.

64. *Id.* ¶ 45.

65. *Id.* ¶ 45.

66. *Id.* ¶ 45.

67. *Id.* ¶ 46.

68. *Id.* ¶ 47.

69. *Id.* ¶ 48.

that certain processing . . . must necessarily be based on consent."[70] Such a distinction would create a hierarchy of legal bases, something the DPC sees as contradictory to the GDPR's language.[71]

Reiterating that there is a distinction between "the act of agreeing to a contract (even . . . where that contract concerns the processing of personal data) and the act of providing consent for the purpose of legitimatising the processing of personal data,"[72] the DPC viewed the second consent argument as an extension of Issue 2.[73] According to the draft decision, if reliance on Article 6(1)(b) "turns on the particular agreement entered into by the parties" rather than the type of contract,[74] then whether Meta *must* rely on consent depends on whether the processing was necessary for the performance of *this contract* under Article 6(1)(b). If not, then by process of elimination Meta might have no choice but to rely on consent.[75] Again, the DPC did not make binding findings on this issue because of the EDPB's decision.[76]

B. WHETHER PROCESSING WAS NECESSARY FOR THE PERFORMANCE OF A CONTRACT

NOYB's assertion that Meta was required to rely on consent for the processing of personal data for the delivery of behavioral advertisements flows from the presumption that Meta could not rely on Article 6(1)(b) (fulfillment of a contract) for such processing.[77] The DPC and EDPB took drastically different views on this issue, and their differing assessments represent alternative futures for the GDPR.

1. The DPC Draft Decision

If processing personal data is lawful where it is necessary for the performance of a contract to which the data subject is party,[78] then an SA must determine whether a contract exists, what it means to perform that contract, and what is necessary

70. *Id.* ¶ 54.
71. *Id.* ¶¶ 48, 51.
72. *Id.* ¶¶ 50, 55.
73. *Id.* ¶ 57.
74. *Id.* ¶ 55.
75. *Id.* ¶ 57.
76. *Id.*
77. *Id.* ¶ 64.
78. *Id.* ¶ 68. The DPC also stressed that parties have a right to contract in accordance with their national laws. *Id.* ¶ 71.

for performance. The DPC's analysis first determined the scope of the contract by examining the relationship between the updated Terms of Use and Data Policy,[79] concluding that acceptance of the former constituted acceptance of a contract but that it did not incorporate the latter.[80] The DPC then analyzed arguments concerning the concept of "necessity" in data protection law as applied to the Terms of Use.[81]

NOYB asserted that Meta could not rely on Article 6(1)(b) as the legal basis for processing personal data for the delivery of behavioral advertisements in connection with the Terms of Use. They argued that such processing was not "genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller," and that merely including processing in fine print did not make it necessary for the performance of that contract.[82] To NOYB, necessary meant a "core element of a social network" rather than terms regarding advertisements, sponsored content, and analysis and improvement.[83] NOYB also attempted to draw a line between "processing

79. *Id.* ¶ 72.

80. Despite the "ambiguous and unclear" nature of the engagement flow, the DPC believed that acceptance of the Terms of Use constituted acceptance of a contract. *Id.* ¶¶ 74–75. However, the DPC viewed the Data Policy as being an "information document" meant to comply with GDPR transparency requirements. *Id.* ¶ 76. Hence, when assessing Article 6(1)(b), the Terms of Use constituted the contract and the Data Policy merely shed light on Meta's processing operations. *Id.* With the scope determined, the DPC turned to the problem of defining necessity. *Id.* ¶ 78.

81. *Id.* ¶ 80.

82. *Id.* (quoting Opinion 06/2014 of the Article 29 Working Party).

83. *Id.* ¶ 81. Reliance on Article 6(1)(b) for purposes of service improvement was at issue in another recent contentious DPC decision regarding WhatsApp (another Meta subsidiary business). *See* Alex LaCasse, *Irish DPC Fines WhatsApp 5.5M Euros, Fissure with EDPB Continues*, IAPP (Jan. 19, 2023), https://iapp.org/news/a/irish-dpcs-whatsapp-fine-deepens-fissure-with-edpb-over-enforcement-jurisdictions [https://perma.cc/R5XQ-W2MC]. Despite prior EDPB guidance that 6(1)(b) could be relied upon for the personalization of content, NOYB maintained that such processing must be an "integral part" of the service for it to apply. NOYB's position relied on prior guidance from the EDPB that application of 6(1)(b) depended upon the scope of the contract and what data would be necessary for its performance. DPC Instagram Decision, *supra* note 2, ¶ 82. NOYB also maintained that the Terms of Use should be assessed by reference to Belgian contract law, and that none of the statements in the Terms of Use were contractual in nature. *Id.* ¶¶ 82–83.

necessary to provide the services of a social network" and "processing in the sole interest of [Meta]."[84] In contrast to NOYB's arguments, which draw substantive distinctions around the general nature and purpose of a contract from a data subject's perspective, Meta argued that the applicability of Article 6(1)(b) should be more dependent on the specific terms of the contract. In Meta's view, necessary does not mean "strictly essential to the performance of the contract" or "the only way to perform the underlying contract."[85] Rather, "processing which is necessary to perform the full agreement . . . can include optional or conditional elements of contract," which is "a matter for the parties to the contract."[86]

The DPC's draft decision again largely agreed with Meta.[87] Starting with the issue of performance, the DPC emphasized the importance of ascertaining the bargain struck in the contract, finding that "a contract is performed when each party to that contract discharges their contractual obligations by reference to the bargain struck between the parties."[88] Performance therefore should be assessed by whether "a requested service can be provided,"[89] and there "must be a nexus between the specific processing operations and the bargain struck."[90] Necessity is then defined in terms of performance: "what is necessary for the performance of a contract is anything which, if it is [sic] did not occur, would mean that the specific contract entered into would not have been performed."[91] Thus, mere inclusion of a term in the contract does not make it necessary.[92] Rather, "a functional assessment of the specific contract should take place" and the "controller should be able to demonstrate how the main subject-matter of the specific contract . . . cannot, as a matter of fact, be performed if the specific processing . . . in question does not occur."[93] Endorsing a broad interpretation of Article 6(1)(b), the

84. *Id.* ¶ 84. Meta did not share NOYB's view that a contractual provision must be in the interests of the data subject for it to be necessary. *Id.* ¶ 85.

85. *Id.* ¶ 85.

86. *Id.*

87. The Investigator, in their preliminary investigation, also found that Meta could rely on Article 6(1)(b) in this context. *Id.* ¶ 86.

88. *Id.* ¶ 88.

89. *Id.*

90. *Id.* (citing Guidelines 02/2019 ¶ 30).

91. *Id.* ¶ 89.

92. *Id.*

93. *Id.* The latter burden on the controller comes from EDPB guidance. *Id.*

DPC emphasized that "'necessity' does not require the most minimal processing possible," and "includes processing beyond the most minimal to meet the objective where the processing renders a lawful objective 'more effective.'"[94]

Under this capacious reading of "necessary," the DPC rejected NOYB's argument that advertising is not necessary to deliver a social network and reiterated that the question is whether such processing is necessary to perform the *specific contract* at issue.[95] Prior EDPB guidance had stated that, "as a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services."[96] The DPC interpreted this to mean that sometimes personal data processing for behavioral advertising *is necessary* for online services.[97] The DPC then identified the "core" functions of the contract,[98] highlighting two clauses from the Terms of Use related to personalization. The first explained that Instagram builds systems to offer personalized experiences,[99] and the second promised to connect users with "brands, products, and services in ways you care about."[100]

Believing that the Terms of Use set an expectation that Instagram includes behavioral advertising, the DPC concluded that "the core of the service offered is premised on the delivery

94. *Id.* ¶ 93. This statement by the DPC is illustrative of how procedural data protection can facilitate and normalize data processing. *See infra* note 129 and accompanying text.

95. *Id.* ¶ 103.

96. *Id.* ¶ 104.

97. *Id.* ¶ 105. The DPC's reasoning was that the "as a general rule" disclaimer meant that the inverse of the statement is true in limited circumstances. That view was buttressed by another EDPB acknowledgment that personalization of content may constitute an essential element of certain online services. *Id.*

98. *Id.* ¶ 94. The DPC sought to consider "the particular aim, purpose, or objective of the service" as well as the "bargain that was struck between the parties." *Id.* ¶ 95.

99. This includes "highlighting content, features, offers, and accounts you may be interested in, and offering ways for you to experience Instagram, based on things you and others do on and off Instagram." *Id.* ¶¶ 100–01.

100. This includes using data from Meta products and third-party partners "to show you ads, offers, and other sponsored content that [Instagram] believe[s] will be meaningful to you," to make that content "as relevant as all your other experiences on Instagram." *Id.* ¶¶ 100, 102.

of personalised advertising."[101] Despite NOYB's argument that no evidence suggests the average user views the "bargain" this way, the DPC maintained that "it is reasonable to assume that the average user would read the text of the Terms of Use prior to acceptance."[102] Thus, "any reasonable user would understand and expect that this is part of the core bargain that is being struck with Meta," and processing for the delivery of behavioral advertising must fall under Article 6(1)(b).[103]

The EDPB disagreed.[104]

2. The Article 65 Decision

As Meta's LSA, the DPC was required to circulate its draft decision to other SAs so that they could object in accordance with Article 60.[105] Ten CSAs raised objections to certain elements of the DPC's draft decision—notably, the DPC's view that Meta could rely on performance of a contract as the legal basis for the processing of personal data to deliver behavioral advertising.[106] The DPC viewed the Terms of Use as a contract between Instagram and users which promises the provision of a personalized service (including behavioral advertising), so it viewed performance of a contract as a valid lawful basis for processing personal data to deliver personalized advertisements in this instance.[107] The EDPB, in contrast, favored a stricter reading of "necessary" under Article 6(1)(b) and did not view the delivery of personalized advertising as necessary to perform the core elements of the contract between Instagram and its users.[108]

The EDPB grounded its analysis in the GDPR's general objectives and "normative context."[109] First, the EDPB asserted

101. *Id.* ¶ 106. This placed significant weight on Meta's statements that it considered behavioral advertising a core element of its service and that users understand and expect as much. *Id.*

102. There are arguments that this assumption is neither reasonable nor would it be desirable. *See generally* Hartzog & Richards, *supra* note 25; Solove, *supra* note 25.

103. DPC Instagram Decision, *supra* note 2, ¶ 108.

104. *Id.* ¶ 118.

105. *Id.*

106. DPC Press Release, *supra* note 2.

107. *Id.*

108. *Id.*

109. Eur. Data Prot. Bd., Binding Decision 4/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram Service (Art. 65 GDPR), ¶ 103 (Dec. 5, 2022) [hereinafter EDPB Decision].

that the rights of privacy and data protection take primacy over a controller's economic interests:

> The GDPR . . . treats personal data as a fundamental right inherent to a data subject and his/her dignity, and not as a commodity data subjects can trade away through a contract. The CJEU provided additional interpretative guidance by asserting that the fundamental rights of data subjects to privacy and the protection of their personal data override, as a rule, a controller's economic interests.[110]

Thus, a controller must comply with the principles of lawful, fair, and transparent data processing even where practical implication runs counter to its commercial interests and business model.[111] In fact, "it is the business model which must adapt itself and comply with the requirements that the GDPR sets out in general and for each of the legal bases and not the reverse."[112] Second, the EDPB took a different approach in framing how regulators should assess what a reasonable user would expect from a service like Instagram, focusing more on the relationship between users and Instagram than on the Terms of Use. The EDPB noted that "[t]he principle of fairness includes . . . recognizing the reasonable expectations of the data subjects, considering possible adverse consequences processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller."[113] The EDPB's embrace of these substantive principles that explicitly consider the social context of the GDPR's protections and the power dynamics of information relationships contrast sharply with the DPC's assessment, which was grounded much more in the text of the Terms of Use.

Backed by these substantive principles and its own prior guidance, the EDPB concluded that Meta inappropriately relied on Article 6(1)(b) and therefore lacked a legal basis to process personal data for behavioral advertising.[114] This conclusion rested on what the EDPB believed a reasonable user would expect and what reasonable funding alternatives Meta could rely on to support Instagram.

Starting with user expectations, the EDPB noted that necessity under Article 6(1)(b) should be justified by reference to

110. *Id.* ¶ 104.
111. *Id.* ¶ 108.
112. *Id.* ¶ 122.
113. *Id.* ¶ 106.
114. *Id.* ¶ 137.

the parties' mutually understood contractual purpose, which depends on the perspectives of both the controller and a reasonable data subject when entering into a contract.[115] With that framing, the EDPB disagreed with the DPC's assessment that a reasonable user would expect personalized advertising.[116] Despite the DPC's reliance on the mention of personalized advertising in the Terms of Use, the EDPB noted that nothing in the terms obligated Meta to offer such advertising to users.[117] The EDPB also took issue with the conclusion that a reasonable user who read the Terms of Use would "expect that their personal data is being processed for behavioural advertising simply because Meta IE briefly refers to this processing in its Instagram Terms of Use" or because of public awareness of this practice.[118] Given that behavioral advertising is a very complex process, and that the references to behavioral advertising in the Terms of Use were and Data Policy were very brief, the EDPB concluded that it is unlikely that the average user would "fully grasp it, be aware of its consequences and impact on their rights to privacy and data protection, and reasonably expect it solely based on the Instagram Terms of Use."[119] That the average user would not consider behavioral advertising to be core to Instagram was also apparent from how Instagram was advertised and how it was used—as a social network, a means of viewing photographs and videos by people and organizations that an individual follows and of sharing content with followers.[120] This conclusion was bolstered by the inference that if Article 21 provides data subjects with an absolute right to object to processing of their data (including profiling) for direct marketing purposes, then processing for behavioral advertising cannot be necessary to perform a contract.[121]

The EDPB also declined to place weight on the fact that Meta decided to monetize its service through behavioral ads. Working from the proposition that business models must adapt

115. *Id.* ¶ 116. The EDPB found that "a reasonable user cannot expect that their personal data is being processed for behavioural advertising simply because Meta IE briefly refers to this processing in its Instagram Terms of Use . . . or because of the 'wider circumstances' or 'recognised public awareness of this form of processing' derived from its 'widespread prevalence of OBA processing' to which the IE SA refers." *Id.* ¶ 126.

116. *Id.* ¶ 121.

117. *Id.*

118. EDPB Decision, *supra* note 109, ¶ 126.

119. *Id.*

120. *Id.* ¶¶ 126–27.

121. EDPB Decision, *supra* note 109, ¶ 125.

to comply with the GDPR, the EDPB stressed that "[n]or does [Meta]'s business model of offering services, at no monetary cost for the user to generate income by behavioral advertisement to support its Instagram service make this processing necessary to perform the contract."[122] The EDPB's prior guidance stated that "[i]f there are realistic, less intrusive alternatives, the processing is not 'necessary.'"[123] In the EDPB's view, there are such alternatives to behavioral advertising,[124] such as contextual advertising that is delivered based on the content on the page rather than the user viewing the advertisement. The main purpose of the contract thus did not include behavioral advertising,[125] and Meta was incorrect to rely on Article 6(1)(b) for this processing.[126] The EDPB ordered the DPC to alter its findings on Issues 1 and 2 and adopt the findings in the Article 65 decision.

In the wake of these decisions, the DPC has criticized the EDPB for overreach and intends to challenge the EDPB's authority to order the DPC to conduct a broader investigation into Meta's processing operations.[127] The two bodies also clashed in the DPC's recent decision concerning WhatsApp, giving little hope that this conflict will abate soon.[128]

* * *

The EDPB had final say in this matter, but that this almost came out differently should give privacy scholars and advocates

122. *Id.* ¶ 122.

123. *Id.* ¶ 123.

124. *Id.* ¶ 124.

125. *Id.* ¶ 128.

126. *Id.* ¶¶ 136–37.

127. DPC Press Release, *supra* note 2 ("Separately, the EDPB has also purported to direct the DPC to conduct a fresh investigation that would span all of Facebook and Instagram's data processing operations and would examine special categories of personal data that may or may not be processed in the context of those operations . . . . The EDPB does not have a general supervision role akin to national courts in respect of national independent authorities and it is not open to the EDPB to instruct and direct an authority to engage in open-ended and speculative investigation. The direction is then problematic in jurisdictional terms, and does not appear consistent with the structure of the cooperation and consistency arrangements laid down by the GDPR. To the extent that the direction may involve an overreach on the part of the EDPB, the DPC considers it appropriate that it would bring an action for annulment before the Court of Justice of the EU in order to seek the setting aside of the EDPB's directions.")

128. *See* LaCasse, *supra* note 83.

pause. On the one hand, this is an example of Article 65 working as intended. On the other hand, the idea that an influential SA was ready to decide that processing personal data for delivery of behavioral advertisements can be legitimized by including it in the terms of service and by identifying a weak nexus between that practice and the service requested raises questions about the limits of procedural data protection, the future of the GDPR, and the kinds of privacy protections that US lawmakers should look to implement.

III. REFLECTIONS ON THE GROWING SCHISM BETWEEN THE DPC & EDPB

Data protection regimes like the GDPR focus on empowering individuals to exercise control over their data. That goal is laudable, but scholars have argued that procedural protections based on concepts of fairness and transparency can inadvertently normalize and facilitate data processing and surveillance "as something inevitable or even virtuous."[129] Even the GDPR, which incorporates a normative theory of legitimate data processing into its lawful basis requirement, has the capacity to "normalize an advertising-based culture that forces itself upon our time, attention, and cognitive faculties . . . ."[130] The data protection model can also suffer from chronic blind spots in that a myopic focus on protecting data rather than people can fail to prevent and remedy uses of data that are harmful.[131] This is because rigid application of procedural protections fails to recognize the importance of power dynamics within information relationships or the broader social context in which rules operate.[132] For that reason, scholars have suggested that data protection and privacy law should embrace a relational approach that is

129. *See* Neil Richards & Woodrow Hartzog, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 1006 (2022). The DPC's own assessment illustrates this risk well. For example, the DPC emphasized that "'necessity' does not require the most minimal processing possible," and the necessity test "includes processing beyond the most minimal to meet the objective where the processing renders a lawful objective 'more effective.'" DPC Instagram Decision, *supra* note 2, ¶ 93.

130. Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1724 (2020).

131. *Id.*

132. Richards & Hartzog, *supra* note 17, at 982.

sensitive to power disparities within information relationships.[133] The DPC's readiness to allow Meta to rely on performance of a contract as a lawful basis for the delivery of behavioral advertising on Facebook and Instagram is illustrative of some of these risks. But the EDPB decisions offer a contrasting vision of the GDPR which is shaped by substantive principles, brings new life to GDPR enforcement, and goes further in protecting individuals from excessive and unwanted data processing.

This distinction between procedural and substantive rules has meaningful consequences for data subjects. Take for example the argument that processing need not be "strictly essential" to a contract and can include optional elements of the contract as determined by the parties.[134] Without acknowledging the power disparities that exist in information relationships and by giving too much deference to the terms of the contract, this interpretation, if applied broadly, would eviscerate the GDPR's heightened consent requirements.[135] A controller who offers a ubiquitous, information-intensive service (e.g., a social media network with millions or billions of global users) can take tangentially related data practices that do not serve the interests of their consumers, insert them into the Terms of Use, and then rely on the broadly defined contract legal basis to legitimize that data processing (rather than obtaining consent) so long as there is at least a weak nexus between the data practice and the service offered. In that scenario, the contract lawful basis would begin to resemble the oft-criticized notice and choice standard in

133. Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 6 EUR. DATA PROT. L. REV. 492 (2020).

134. DPC Instagram Decision, *supra* note 2, ¶ 85.

135. Article 7(4), for instance, states that, "[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." GDPR art. 7(4). That protection exists to prevent controllers from leveraging their power over data subjects by adding unnecessary data processing to contracts between the two parties. Article 7(4) and Meta's interpretation of "necessary to perform the full agreement" can coexist, but only in a way which would have significant implications for the future of data protection. Were Meta's argument to gain traction and a broad definition of "necessary to perform the full agreement" was adopted, then controllers could bypass the heightened consent requirements altogether. Several CSAs raised this point, noting that the DPC's draft decision would allow companies to engage in behavioral advertising in a way which could bypass informed consent. *See* EDPB Decision, *supra* note 109, ¶ 58.

the United States. That interpretation of the contract lawful basis fails to account for the power dynamics that exist between a company like Meta and a typical user who has no power to bargain, can be ambushed by unilateral changes to terms at any moment,[136] and faces the unenviable choice of either acquiescing to the new terms or abandoning their account (which they have invested time in curating, may rely on for their livelihood, or use to exercise free expression and access information). Many people believe that kind of ultimatum should be permissible and that privacy and data protection concerns should not trump a business's right to determine its business model. There is nothing fundamentally wrong with that outcome, but there is also nothing inevitable about it. That is a policy choice about the proper allocation of privacy in society.

An alternative approach is illustrated by the EDPB's analysis, which embraces concepts of relational vulnerability and realistic user expectations to conclude that the mention of behavioral advertising in Instagram's Terms of Use is not enough to invoke the contract lawful basis in this instance. The EDPB emphasized the heightened risks that users face from asymmetry of information and inappropriate reliance on the contract legal basis when a dominant market player creates a "take it or leave it" situation with standard, pre-formulated contracts:

> [T]he EDPB considers that the dominant position of Meta IE also plays an important role in the assessment of Meta IE's reliance on Article 6(1)(b) GDPR for its Instagram service and its risks to data subjects, especially considering how deficiently Meta IE informs the Instagram users of the data it strictly needs to process to deliver the service. . . . [Users] may either contract away their right to freely determine the processing of their personal data and submit to its processing for the obscure, and intrusive purpose of behavioural advertising, which they can neither expect, nor fully understand based on the insufficient information Meta IE provides to them. Or, they may decline accepting the Instagram Terms of Use and thus be excluded from a service that enables them to communicate, share content with and receive content from millions of users and for which there are currently few realistic alternatives. This exclusion would thus also adversely affect their freedom of expression and information.[137]

136. *See* Hila Keren, *I Am Altering the Deal. Pray I Don't Alter It Any Further.*, JOTWELL (May 4, 2020), https://contracts.jotwell.com/i-am-altering-the-deal-pray-i-dont-alter-it-any-further [https://perma.cc/V3U9-M6D7] (reviewing Shmuel I. Becher & Uri Benoliel, *Sneak In Contracts: An Empirical Perspective*, 55 GA. L. REV. 657 (2021)) (discussing the problem of unilateral changes to consumer contracts and quoting the iconic ultimatum issued by Darth Vader to Lando Calrissian, "I am altering the deal. Pray I don't alter it any further.").

137. EDPB Decision, *supra* note 110, ¶ 131–34.

Policymakers looking to enact privacy rules must be cognizant of which outcome they prefer—giving businesses significant deference or requiring business models to adapt to stricter privacy rights. Ultimately, the GDPR consistency mechanisms operated in this dispute to prevent the DPC from creating what many would see as a loophole in the GDPR's consent requirements,[138] but privacy advocates should be concerned that an influential SA nearly determined otherwise.

The practical implications of these decisions for behavioral advertising on two the internet's biggest services are important. But what makes this conflict so significant are the different approaches taken by the DPC and EDPB and what those differences could mean for the future of the GDPR. The surface level of this dispute is a technical quibble over whether the provision of behavioral advertisements is truly necessary for the full performance of the contract between Instagram and its users. That depends on definitional questions about what is a "contract," what it means to "perform," and what is "necessary" for performance. But as the consent hypothetical above demonstrated, the issues run deeper than contract interpretation, and there are a number of important issues bubbling under the surface: whether behavioral advertising is ever consistent with the fundamental rights of privacy and data protection; how much weight should be placed on privacy and data protection when weighed against other rights; whether a service such as Instagram should, consistent with those fundamental rights, be able to offer its service as a take-it-or-leave-it proposition (i.e., "free" with behavioral advertising or not at all); and to what degree regulators should consider social context and power dynamics when deciding enforcement actions.

Reasonable minds will differ on these issues, but the various responses to these decisions in public discourse illustrate how procedural protections, if not guided by deeper substantive principles, can suppress or distract from the more pressing normative questions in cases of this magnitude. For example, in the wake of these decisions several arguments arose regarding the conclusion, often muddled into the same unproductive conversation. Some agree with the DPC's draft analysis that processing personal data to deliver behavioral ads is necessary to fulfill the contract between Meta and the individuals who use its services.

138. Pending the results of Meta's appeal, of course.

Generally, this viewpoint hinges on giving Meta deference to determine its business model (the behavioral ads or no service ultimatum). But that reasoning is not very different in substance than saying that Meta has a legitimate interest in processing such data because their business model depends on it.[139] Similarly, some have asked whether individuals could theoretically freely consent to such processing where the only alternatives are to either cease using the service or ultimately pay a subscription to do so. But this argument again loops back to the propriety of Meta's underlying business model. These arguments all appear to be subtle variations of one broader debate—either that we should let platforms like Instagram engage in behavioral advertising because that is how Meta has decided it will derive a profit, or that individuals should be free of behavioral advertising, either through an outright prohibition or a meaningful opt-in requirement. It is an argument as old as the internet,[140] but one which the DPC only made fleeting references to in its decision.[141]

Behavioral advertising raises important questions regarding the proper balance of privacy, autonomy, manipulation, the importance of "relevant" content, whether advertising is "content," minimizing cost barriers for online content, etc. Policymakers need to address these issues proactively, determining whether and how to make substantive interventions by openly and honestly weighing the interests of concerned parties, the

139. An approach Meta is now testing. *See supra* Schechner & Horwitz, *supra* note 6.

140. *See generally* Matthew Crain, PROFIT OVER PRIVACY: HOW SURVEILLANCE ADVERTISING CONQUERED THE INTERNET (2021) (describing how the interests of advertisers shaped policy surrounding the development of the early internet in ways that still affect us today).

141. DPC Instagram Decision, *supra* note 2, ¶ 105 ("The core issue under consideration is whether, having regard [sic] the exact terms of the contract, the inclusion of behavioural advertising as a contractual term makes data processing conditional on the delivery of a contract, where that processing is not itself necessary to actually deliver the contract. The counter-argument to this is that behavioural advertising is the core of both Meta Ireland's business model and the bargain struck between Meta Ireland and Instagram users and, accordingly, processing in this regard is necessary to fulfil the contract between Meta Ireland and the Named Data Subject."); *Id.* ¶ 107 ("It remains my view that the text of the first and sixth clauses [of the Terms of Use] are clear that the core of the service offered by Meta Ireland is premised on the delivery of personalised advertising. This is notwithstanding the EDPB's view that processing cannot be rendered lawful by Article 6(1)(b) GDPR '*simply because processing is necessary for the controller's wider business model.*'").

balance of benefits and risks, and the need to encourage responsible innovation. Passing procedural privacy protections without backing those safeguards with substantive principles like relational vulnerability not only avoids dealing with difficult questions, such as the propriety of "take it or leave it" business models and the proper role of behavioral advertising online, it risks inadvertently legitimizing those practices.

The different assessments made by the DPC and EDPB reveal competing views of how to interpret and enforce the GDPR which should serve as a warning for US policymakers looking to implement privacy rules. The DPC's draft analysis touched on these issues, but only in fleeting references to deeper issues lurking beneath the surface, focusing instead on surface-level, circular discussions of "contract," "performance," and "necessity." This is at best an indirect approach to tackling these issues. Without resolving the underlying normative questions regarding the propriety of Meta's business model with respect to the fundamental rights or privacy and data protection, a procedurally-focused analysis like that of the DPC is not going to satisfactorily resolve this kind of dispute. The net effect of that approach will be a gradual erosion of privacy rights over time because failing to recognize relational vulnerability prioritizes the interests of information-intensive dominant platforms like Facebook and Instagram.

In contrast, both the EDPB and NOYB clearly recognize and openly discuss the important substantive issues in these decisions. For example, NOYB asked the DPC to "draw a line in order to separate the processing necessary to provide the services of a social network . . . from the processing in the sole interest of Facebook [Meta]."[142] That argument is reminiscent of growing calls for the U.S. to enact a duty of data loyalty, which would require companies entrusted with our personal data to act in our best interests with respect to the collection, processing, and transfer of personal data.[143] NOYB also alleged that consent could not be freely given in this context because there was a "clear imbalance of power" between Meta and data subjects re-

142. DPC Instagram Decision, *supra* note 2, ¶ 84.

143. *See, e.g.*, Richards, Hartzog & Francis, *supra* note 25 (arguing that the FTC should ground its future data privacy rules in concepts of trust, loyalty, and relational vulnerability); Richards & Hartzog, *supra* note 17; Richards & Hartzog, *supra* note 129.

sulting from Instagram's dominant market position and the network effect of social media.[144] Similarly, the EDPB's opinion is rife with references to normative context, information asymmetry, individual rights overriding a controller's economic interests, potential adverse consequences to data subjects, and the need for companies to adapt their business models to the GDPR rather than the other way around.[145] The EDPB's willingness to embrace relational vulnerability as a guiding principle and to make these substantive issues explicit in its analysis demonstrates how data protection can be bolstered by robust, substantive principles.

* * *

Arguing about which lawful basis applies to and legitimizes this kind of data processing, without discussing the underlying substantive issues, risks devolving into privacy theater. Procedural data protections like those offered in the GDPR have done much to reign in rampant data processing offenses in recent years, but regulators cannot lose sight of the issues that are meaningful to the individuals who rely on their protection. FTC Chair Lina Khan highlighted this problem in her speech at the 2022 IAPP Global Privacy Summit when she called for substantive data privacy rules rather than mere procedural protections.[146] There have been calls in recent years for the United States to enact privacy laws mimicking the GDPR's lawful bases approach. That course of action may be wise, but the contrasting analyses of the DPC and EDPB in these decisions highlight the importance of substantive principles in privacy law. Concepts of

144. DPC Instagram Decision, *supra* note 2, ¶ 16.

145. *See supra* Part II.B.2. The discussion of information asymmetry appeared in the context of the transparency violations. *See* EDPB Decision, *supra* note 109, ¶ 131, 235.

146. Lina Khan, *Fed. Trade Comm'n, Remarks of Chair Lina M. Khan as Prepared for Delivery IAPP Global Privacy Summit 2022 Washington D.C.*, FTC (Apr. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf [https://perma.cc/AT5F-5323] (citing Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1693 (2020)) ("Going forward, I believe we should approach data privacy and security protections by considering substantive limits rather than just procedural protections, which tend to create process requirements while sidestepping more fundamental questions about whether certain types of data collection and processing should be permitted in the first place.").

fairness and transparency are not enough on their own; they must incorporate further concepts such as relational vulnerability. Procedural safeguards have to be backed by substantive principles or they risk being captured by the information-intensive entities they were meant to curtail. The divergent views of the DPC and EDPB in this regard illustrate alternative paths which should inform the decisions of privacy advocates and policymakers who are seeking to implement privacy and data protection regulations.

CONCLUSION

Meta intends to appeal these decisions,[147] and the DPC will have to defend decisions which it views as incorrect.[148] In the meantime, Meta is trying its luck with the legitimate interest lawful basis.[149] The tension between the DPC and EDPB likewise shows no signs of abating. As of February 2023, the DPC has brought two legal challenges against the EDPB's authority over it,[150] and the EU Commission has begun work on legislation that would amend the Article 65 dispute resolution process to better encourage cooperation among SAs.[151] Whether the balance of power between the DPC and EDPB is modified by these judicial and legislative efforts remains to be seen, and that power struggle will likely be a significant story throughout 2023.

147. *How Meta Uses Legal Bases*, *supra* note 12.

148. *See* DPC Press Release, *supra* note 2, criticizing the decision reached by the EDPB.

149. Schechner & Horwitz, *supra* note 6. Whether Meta will have any luck with this approach remains to be seen. *See supra* note 22 and accompanying text.

150. At the time of writing, only the case numbers are available for these cases: T-84/23 and T-70/23. For a thread about the substance of the disputes, see Robert Bateman (@RobertJBateman), TWITTER (Feb. 22, 2023, 7:16 AM), https://twitter.com/RobertJBateman/status/1628383102501257216?t=aY4d77vdz46UfPpYxjGOpQ&s=03.

151. Clothilde Goujard, *Brussels Sets Out to Fix the GDPR*, POLITICO PRO (Feb. 20, 2023), https://www-politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/brussels-plans-new-privacy-enforcement-law-by-summer/amp [https://perma.cc/XF9J-NXZ8]; *see also* Robert Bateman (@RobertJBateman), TWITTER (Feb. 20, 2023, 9:52 AM), https://twitter.com/RobertJBateman/status/1627697732067491841 (noting that the EU Commission announced its new proposed regulation concerning DPA cooperation on the same day that the EDPB released "a set of case studies on cross-border cases to illustrate how well DPAs cooperate").

These decisions—both in terms of their substance and the institutional conflict they intertwine with—represent a crossroads for the future of the GDPR and the data protection model. If the decisions stand, then this may be the beginning of the end for behavioral advertising.[152] If they are reversed, however, and the DPC's view is reinstated, then privacy advocates everywhere should ask themselves, "Well, how did we get here?" The GDPR will not remain "the toughest privacy and security law in the world"[153] if regulators fail to incorporate substantive principles such as relational vulnerability and reaffirm that privacy and data protection rights are prior to a company's economic interest. Instead, there is a risk that the GDPR will be reduced to a hollow form of proceduralism which fails to meaningfully examine substantive uses of data or power imbalances within information relationships. As the appeal process plays out, privacy scholars and advocates should pay close attention to the underlying substantive issues and consider whether procedural data protection is truly serving its intended purposes. American policymakers should take this dispute as a cautionary tale about the importance of grounding data privacy rules in substantive principles.

152. *See, e.g.*, Morgan Meaker, *The Slow Death of Surveillance Capitalism Has Begun*, WIRED (Jan. 5, 2023), https://www.wired.com/story/meta-surveillance-capitalism [https://perma.cc/23Q9-JEW8].

153. Wolford, *supra* note 14.