


ARTICLE

Special Issue: Strategic Litigation in EU Law

Opportunities and Difficulties for Strategic Litigation to Advance Digital Rights in the Internet Audience Economy

Swee Leng Harris 

The Policy Institute, King's College London, London, England
Email: sl@sweelengharris.com

(Received 28 November 2024; accepted 28 November 2024)

Abstract

Internet tech giants are regulated by multiple overlapping yet distinct pieces of EU legislation that establish a range of substantive digital rights for internet users, and varying legal opportunity structures for strategic litigation within their enforcement architecture. My Article focuses on the digital rights and enforcement architecture of the EU's new Digital Services Act and Digital Markets Act compared to the General Data Protection Regulation. Consideration of key strategic litigation concerning the existing Regulation informs my exploration of opportunities and barriers for strategic litigation under the new Acts. Analysis of these strategic litigation opportunities necessarily encompasses the EU's new regime for mass claims under the Representative Action Directive, and interaction between internet users' digital rights and consumer protection laws. I contend that the new Acts comparatively centralize public enforcement power in the European Commission, marginalizing civil society, and effectively precluding most strategic litigation by civil society with regard to public enforcement. Furthermore, the new Acts could increase regulatory fragmentation and the risk of legal incoherence by establishing additional regulatory authorities and competences alongside existing institutions and regimes. I argue that private enforcement strategic litigation against internet tech giants could empower civil society to influence the development of digital rights. Private enforcement strategic litigation could also aid legal coherence as an enforcement mechanism that allows multiple areas of law to be raised and addressed at the same time, rather than in silos. However there are considerable barriers to such litigation, including legal questions such as cross-border jurisdiction and standing, and the resources needed for effective strategic litigation. Overall, concerning legal analysis for strategic litigation, my article demonstrates that we must consider both public and private dimensions of enforcement architecture across multiple area of law, taking into account the different power dynamics of different enforcement mechanisms, to understand the opportunities for strategic litigation to advance digital rights in the internet attention economy.

Keywords: Strategic litigation; digital rights; General Data Protection Regulation (GDPR); Digital Services Act (DSA); Digital Markets Act (DMA)

A. Introduction

This Article considers strategic litigation within the rights and enforcement architecture of the General Data Protection Regulation [hereinafter GDPR], Digital Services Act [hereinafter DSA], and Digital Markets Act [hereinafter DMA],¹ arguing for the value of private enforcement

¹Commission Regulation 2016/679 of Apr. 27, 2016, Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Council Directive 2016 O.J. (L 119) (EU) [hereinafter

strategic litigation to further the rights of internet users while highlighting some of the barriers to bringing such cases. The GDPR, DSA, and DMA constitute distinct but overlapping legal structures for the human rights of internet users—one area of digital rights. The EU’s 2016 GDPR provides human rights regulation applicable to tech giants’ processing data about internet users, but there is a gap between the GDPR’s substance and its enforcement in practice.² Strategic litigation by civil society has stepped into this gap. This includes public enforcement strategic litigation against regulators to enforce the GDPR against internet giants, and private enforcement strategic litigation upholding individuals’ rights directly against companies.³ The new DSA and DMA regulate internet giants, but their public enforcement architecture further fractures regulation across multiple regulators that could make inconsistent decisions causing incoherence in EU law. These new laws also centralize public enforcement power in the European Commission, marginalizing and disempowering civil society, which will not have standing to directly challenge the Commission in strategic litigation.

Private enforcement strategic litigation in the interests of internet users could counteract legal incoherence from regulatory fragmentation, and counterbalance disempowerment of civil society in DSA and DMA public enforcement, but there are procedural barriers to such litigation. Strategic litigation based on a private right of action against a company can incorporate relevant principles across multiple areas of law that apply to the same set of facts, promoting legal coherence by enabling judicial decisions that integrate distinct but overlapping laws. Civil society will need to overcome significant difficulties to bring this kind of strategic litigation, such as uncertainty over cross-border jurisdiction and access to legal expertise. The new EU regime for mass claims through representative actions potentially expands legal opportunity structures for private enforcement litigation under GDPR, DSA, and DMA. However, mass claims entail additional procedural requirements for standing or admissibility, which may render some of these mechanisms unusable for strategic litigation.

Efforts to advance digital rights for internet users have relied on strategic litigation as a catalyst to enliven legal rights and opportunities. Internet tech giants’ infringements of users’ human rights are diffuse, opaque, and occur at scale across millions of people. Strategic litigation can promote human rights in this context by: Developing legal rights and protections through judicial decisions; mobilizing regulators to correctly interpret and enforce the law through judicial review of a regulator; pressuring big tech companies to change their practices using litigation directly against a company; or raising awareness and seeking remedies for many users in a mass claim. Legal opportunity structures for litigation are necessary for strategic human rights litigation—civil society cannot bring such litigation if the rules of standing, for example, do not recognize

GDPR]; Commission Regulation 2022/2065 of Oct. 19, 2022, Single Market For Digital Services and Amending Council Directive, 2022 O.J. (L 277) (EU) [hereinafter DSA]; Commission Regulation 2022/1925 of Sept. 14 2022, Contestable and Fair Markets in the Digital Sector and Amending Council Directives, 2022 O.J. (L 265) [hereinafter DMA].

²Giulia Gentile & Orla Lynskey, *Deficient by Design? The Transnational Enforcement of the GDPR*, 71 INT’L & COMPAR. L. Q. 799, 806-823 (2022); Filipe B. Bastos & Przemysław Pałka, *Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?*, 19 EUR. CONST. L. REV. 487, 493-495 and 499-503 (2023); Diogo M. Brandão, *The One-Stop-Shop and the European Data Protection Board’s Role in Combatting Data Supervision Forum Shopping*, 13 INT’L DATA PRIV. L. 313, 319-325 (2023); Filippo Lancieri, *Narrowing Data Protection’s Enforcement Gap*, 74 ME. L. REV. 15, 57 (2022); Herwig C. H. Hofmann & Lisette Mustert, *Procedures Matter – What to Address in GDPR Reform and a New GDPR Procedural Regulation*, UNIV. OF LUXEMBOURG L. RSCH. PAPER NO. 2023-02 (May 31, 2023), <https://pure.uva.nl/ws/files/62817623/20539517211025061.pdf>; *Conference Report: EDPS CONFERENCE REPORT 2022 - THE FUTURE OF DATA PROTECTION: EFFECTIVE ENFORCEMENT IN THE DIGITAL WORLD*, 60–64, https://www.edps.europa.eu/system/files/2022-11/22-11-10-edps-conference-report-2022_en.pdf (last visited Jun.12, 2024), THOMAS STREINZ, *The Evolution of European Data Law*, in THE EVOLUTION OF EU LAW 902, 914 (Paul Craig and Gráinne de Búrca eds., 3rd ed. 2021).

³Ander Maglica, *Public End Through Private Means: A Comparative Study on Public Interest Litigation in Europe*, 16 ERASMUS L. REV. 71, 72-76 (2023). See also Gig Workers Score Historic Digital Rights Victory Against Uber & Ola, WORKER INFO EXCHANGE (Mar 15, 2021), <https://www.workerinfoexchange.org/post/gig-workers-score-historic-digital-rights-victory-against-uber-ola-2>.

individuals or NGOs. Yet, the mere existence in law of digital rights and legal opportunity structures for litigation is not sufficient to empower people against internet tech giants without the catalytic effect of strategic litigation.

I discuss different kinds of strategic litigation, which enable a range of approaches to advance digital rights with impact beyond the specific circumstances and actors in a case. Strategic litigation can arise in relation to public enforcement of the law where there is a legal challenge of a regulator's decisions or actions aimed at establishing a particular interpretation of the law or changing the behavior of regulators. Strategic litigation also arises in private enforcement where non-state actors litigate directly against an actor that has infringed their rights.⁴ Private enforcement is not limited to pursuing commercial interests—it encompasses strategic litigation brought against companies in the public interest. The Court of Justice of the EU [hereinafter CJEU] has recognized private enforcement litigation as an integral part of enforcing EU law and that damages claims help deter conduct that infringes EU law protections.⁵ Mass claims against companies, which are one type of private enforcement, will tend to be strategic litigation given that they concern the rights of many individuals, although some may argue that those mass claims driven primarily from a profit motive without a broader strategy to change the behavior of companies fall short of being strategic.

My Article adds to existing literature on digital rights by providing analysis of strategic litigation opportunities across both private and public enforcement architecture for the GDPR, DSA, and DMA, analyzing these legal opportunity structures in the round and not siloed from each other. Academic literature has tended to focus on public enforcement of the GDPR by regulators, and the role of regulators in other areas of law such as consumer law.⁶ The value of private enforcement strategic litigation to digital rights has been under-explored, and only a few commentators have focused on private enforcement under the DSA or DMA.⁷ Analysis of the EU's new representative action regime has largely come from the consumer law space,⁸ and the interplay of this new regime with digital rights laws needs further study. Only a small number of civil society actors, mainly None of Your Business [hereinafter NOYB] and BEUC—the European consumer organization—have worked on the interplay of the new representative action regime with digital rights laws such as the GDPR, DSA and DMA.⁹ My Article makes a contribution to the literature by analyzing the enforcement architecture of the GDPR, DSA, and DMA as a system,

⁴Jens-Uwe Franck, *Private Enforcement Versus Public Enforcement*, in *LAW OF REMEDIES: A EUROPEAN PERSPECTIVE* 107, 108 (Franz Hofmann & Franziska Kurz eds., 2019).

⁵See, e.g., Case C-724/17, *Vantaan kaupunki v. Skanska Industrial Solutions Oy & Others*, ECLI:EU:C:2019:204 (Mar. 14, 2019), <https://curia.europa.eu/juris/document/document.jsf?jsessionid=E64FB5CBE3F7EBE4A09BA046AC0E82D1?text=&docid=210531&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6710096>.

⁶See Gentile & Lynskey, *supra* note 2, at 799; Bastos & Paika, *supra* note 2, at 487; Brandão, *supra* note 2, at 313; Lancieri, *supra* note 2, at 57; Hofmann & Mustert, *supra* note 2; EDPS CONFERENCE REPORT 2022 - THE FUTURE OF DATA PROTECTION: EFFECTIVE ENFORCEMENT IN THE DIGITAL WORLD, 60–64, https://www.edps.europa.eu/system/files/2022-11/22-11-10-edps-conference-report-2022_en.pdf, (last visited Jun.12, 2024); STREINZ, *supra* note 2, at 914.

⁷Miguel D. Sánchez, *The Devil is in the Procedure: Private Enforcement in the DMA and the DSA*, 9 *UNIV. BOLOGNA L. REV.* 7, 24-35 (2024); Rupperecht Podszun, *Private Enforcement and the Digital Markets Act*, in *MAX PLANCK INST. INNOVATION & COMPETITION RSCH. PAPER NO. 21-25, TO BREAK UP OR REGULATE BIG TECH? AVENUES TO CONSTRAIN PRIVATE POWER IN THE DSA/DMA PACKAGE* 92, 95–96 (Heiko Richter et al. eds., 2021); Peter Picht, *Private Enforcement for the DSA/DGA/DMA Package*, in *MAX PLANCK INSTITUTE FOR INNOVATION & COMPETITION RSCH. PAPER NO. 21-25, TO BREAK UP OR REGULATE BIG TECH? AVENUES TO CONSTRAIN PRIVATE POWER IN THE DSA/DMA PACKAGE* 98, 98-99 (Heiko Richter et al. eds., 2021).

⁸Alexandre Biard, *The Age of Consumer Law Enforcement in the European Union: High Hopes or Wishful Thinking?*, 14 *EUR. J. RISK REGUL.* 1, 3–5 (2023); Louis T. Visscher & Michael G. Faure, *A Law and Economics Perspective on the EU Directive on Representative Actions*, 44 *J. CONSUMER POL'Y* 455, 468–470 (2021); Petra Leupold, *Private International Law and Cross-Border Collective Redress*, BEUC (Aug. 2022) https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-085_Private_International_Law_and_Cross-Border_Collective_Redress.pdf; Duncan Fairgrieve & Rhonson Salim, *Collective Redress in Europe: Moving Forward or Treading Water?*, 71 *INT'L AND COMPAR. L. Q.* 465 (2022).

⁹See, e.g., BEUC, *The Digital Services Act Proposal: BEUC position paper*, 31-33 (Apr. 9, 2021) https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf; 5 *Years of the GDPR: National Authorities let*

incorporating the novel area of representative actions, and focusing on power dynamics for strategic litigation by civil society to reveal shortcomings in public enforcement legal opportunity structures that could be addressed via private enforcement strategic litigation.

The next section sets out digital rights issues in the audience economy of the internet, and different kinds of civil society actors that have different priorities for strategic litigation on these issues. Section C looks at the substantive content of the GDPR, DSA, and DMA, highlighting their human rights dimensions. The DMA is also relevant for businesses—e.g. business users of big tech platforms¹⁰—who may also seek to bring strategic litigation; however, I limit my consideration to the rights of individual internet users. Section D outlines opportunities for civil society in these laws' public regulatory enforcement frameworks, which are more accessible in the GDPR than DSA and DMA. Section E turns to the avenues for civil society to mount strategic litigation directly against big tech under the GDPR, DSA, and DMA, including through mass claims under the new Representative Action Directive [hereinafter RAD].¹¹ I outline RAD's implementation in Germany, Portugal, and Ireland, which illustrates the highly uneven approaches in different jurisdictions that may undermine effectiveness.

B. Digital Rights, the Internet Audience Economy, and Civil Society

This section provides background on digital rights in the context of the internet audience economy, and different kinds of actors in civil society in digital rights litigation. Understanding the internet audience economy and the different kinds of civil society actors bringing strategic digital rights litigation serves as context for discussion in later sections of the legal structures for internet regulation that civil society navigates.

I. Digital Rights and the Internet Audience Economy

This Article looks at strategic litigation concerning internet tech giants to uphold “digital rights,” which are human rights in the modern digital age. Digital rights are not an entirely new set of rights, rather, the term digital rights acknowledges that the use of digital technology can negatively affect existing human rights.¹² Digital rights are not limited to privacy, but include all human rights depending on the context. For example, non-discrimination can be infringed by targeting ads at users in different demographics such as targeting ads for doctors at men. Data protection under the GDPR reflects one part of the larger picture of human rights in the digital age. This Article looks at the horizontal human rights effects for users from big tech companies such as Meta, which owns Facebook and Instagram, in the current internet model of an audience economy. These companies also have human rights impact on other stakeholders such as the workers reviewing content in content moderation systems, but present analysis is limited to individual internet users.¹³

In the internet audience economy, profit is driven by advertising targeted at users based on profiles that are constructed from data about users, which are collected from a myriad of sources, then passed to vast networks of intermediaries that process the data for profiling and targeting. Amnesty International highlighted human rights risks posed by internet giants in this audience

down European Legislator, NOYB (May 23, 2023) <https://noyb.eu/en/5-years-gdpr-national-authorities-let-down-european-legislator>; Collective Redress, NOYB <https://noyb.eu/en/project/collective-redress>, (last visited Nov. 24, 2024).

¹⁰See, e.g., DMA art. 5(3).

¹¹Council Directive 2020/1828 of Nov. 8, 2020, Representative Actions for the Protection of the Collective Interests of Consumers and Repealing Directive, 2020 O.J. (L 409) 1 (EU) [hereinafter RAD].

¹²See generally, *Digital Rights are Charter Rights: Essay Series*, DIGITAL FREEDOM FUND <https://digitalfreedomfund.org/digital-rights-are-charter-rights-essay-series/> (last visited May 15, 2024).

¹³See, e.g., Foxglove, *What is a content moderator?: an FAQ* (Mar. 29, 2022), <https://www.foxglove.org.uk/2022/03/29/what-is-a-content-moderator/>.

economy in the 2019 Surveillance Giants report.¹⁴ The business model of internet giants can negatively affect many human rights, including privacy, freedom of expression and thought, and non-discrimination.¹⁵

However, data processing and companies involved in the audience economy form a complex web that is difficult to map and understand. Van der Vlist and Helmond have used partner directories to map the audience economy, which is “a complex global and interconnected marketplace of business intermediaries involved in the creation, commodification, analysis, and circulation of data audiences for purposes including but not limited to digital advertising and marketing.”¹⁶ Their research looked at the partnerships between social media platforms, 67 audience intermediaries “that create software tools, products, and services for shaping the creation, buying, modelling, measurement, and targeting of data audiences,”¹⁷ and other commercial actors in the audience economy. They found 11,490 partnerships and integrations in the audience economy—partnerships are both technical and commercial arrangements, creating a vast network in which data about internet users are processed for profit.

Most of us are unaware of how data about us is extracted and exploited for profit in this vast network of commercial actors that is hidden from users as we seek information and communicate online. The audience economy is opaque to us. In this complex and opaque context, individuals struggle to enforce their rights against internet giants,¹⁸ and civil society organizations play an important role as intermediaries to uphold digital rights and access to justice through strategic litigation.

II. Civil Society working on Digital Rights in the Audience Economy

Although I refer to “civil society” throughout this Article, there are a range of different actors in civil society working on digital rights and big tech with differing values, goals, and strategies—these different actors span the different ideal actors identified in the framing paper.¹⁹ Digital rights and privacy NGOs play a key role in relation to big tech companies, such as the UK-based Foxglove, and Austria-based NOYB. These NGOs both have a wealth of legal expertise and from that perspective might best be understood within “the corporation” category. Individuals have played an important role in digital rights strategic litigation in part because GDPR is structured around the rights of individuals, for example litigation by Max Schrems—who founded NOYB—related to Facebook, and claims by Johnny Ryan related to targeted advertising.²⁰ Such individuals tend to be embedded in networks of human rights and digital rights NGOs, and thus do not fit neatly within “the loner” category in the framing paper.

¹⁴Amnesty Int’l, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*, AI Index AFR 30/1404/2019 (Nov. 21, 2019).

¹⁵*Id.*

¹⁶Fernando N. van der Vlist & Anne Helmond, *How Partners Mediate Platform Power: Mapping Business and Data Partnerships in the Social Media Ecosystem*, 8 *BIG DATA & Soc’y* 1, 3 (2021).

¹⁷*Id.*

¹⁸See Lancieri, *supra* note 2, at 30–32.

¹⁹Pola Cebulak, Marta Morvilla, and Stefan Salomon, *Strategic Litigation in EU Law: Who does it Empower?*, 25(6) *GERMAN L. J.* 800, 816–817 (2024).

²⁰See e.g., Case C-604/22, *IAB Eur. v. Gegevensbeschermingsautoriteit*, ECLI:EU:C:2024:214 (Mar. 7, 2024), (<https://curia.europa.eu/juris/document/document.jsf?docid=283529&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=2722153>) (arising from regulatory complaints spearheaded by Johnny Ryan); Case C-311/18, *Data Protection Commissioner v. Facebook Ireland and Schrems*, ECLI:EU:C:2020:559 (July 16, 2020), (<https://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6712657>); Case C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650 (Oct. 6, 2015), (<https://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6712903>).

Consumer protection associations are another kind of civil society actor related to big tech, which are NGOs that advocate for consumer rights.²¹ Even though individuals often do not pay money to use digital services provided by big tech, individual users are nevertheless consumers in relation to the companies.²² Consumer protection associations have taken enforcement action against internet giants under GDPR as well as relying on consumer protection and competition laws.²³ These consumer protection associations vary in size, priorities, and level of EU expertise and appetite for litigation, and so some are closer to “the organization” ideal category, while others are better characterized as “the corporation” in the framing paper.

Whilst acknowledging this complexity among the civil society actors, I treat the goal of upholding human rights from infringement by internet giants as a broadly shared concern for my discussion of strategic litigation. At the same time, the varied nature of these actors means that some will more easily overcome structural barriers to strategic litigation posed by standing. “Civil society” in this Article encompasses both individuals and organizations acting in the public interest.

C. EU Law’s Regulation of Big Tech: GDPR, DSA, and DMA

Having introduced civil society actors advancing digital rights in the audience economy of the internet, I now turn to the key laws that form the legal structures these actors navigate to set out their overlapping content and show where their legal opportunity structures do and do not provide strategic litigation opportunities. This section discusses the rights and protections in the GDPR, DSA, and DMA as key digital rights instruments. However, this is not a comprehensive analysis of applicable laws because, for example, consumer protection and competition laws also apply to the conduct of big tech towards users, as later sections touch on. The GDPR, DSA, and DMA are all regulations that are directly applicable across member states, harmonizing EU digital rights law on internet giants.

I. GDPR

Adopted in 2016, the GDPR requires that personal data—data about individuals—be processed in line with principles and protections that reflect the right to data protection contained in Article 8(1) of the EU Charter of Fundamental Rights. Data protection is not only a matter of privacy. The data protection principles set out in GDPR Article 5 include requirements that personal data be processed lawfully, fairly, and transparently; that personal data be collected for specific legitimate purposes and not processed for other purposes, commonly referred to as “purpose limitation;” and that personal data be accurate.

Individuals, referred to as “data subjects,” have a set of rights under the GDPR, which should have the overall effect of enabling individuals to control data about them. These include rights to have inaccurate personal data rectified; “data portability” meaning that an individual can move their data; and to object to some kinds of data processing.²⁴ There are GDPR obligations for data “controllers” which is any person or entity that determines the purposes and means of processing personal data, and “processors” who process personal data on behalf of a controller. The GDPR is not limited to big tech, applying generally to data processing by any actor in most contexts.

²¹See, e.g., *Who We Are*, BEUC, <https://www.beuc.eu/about-beuc/who-we-are> (last visited May 16, 2024).

²²See, e.g., Frithjof Michaelsen, *Five Meta Myths – What the Tech Giant Gets Wrong About Pay-or-Consent*, BEUC (Mar. 29, 2024), <https://www.beuc.eu/blog/five-meta-myths-what-the-tech-giant-gets-wrong-about-pay-or-consent/>.

²³See, e.g., *The Meta Smokescreen*, BEUC, <https://www.beuc.eu/enforcement/meta-smokescreen> (last visited May 16, 2024); Case C-319/20, *Meta Platforms Ir. Ltd. v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2022:322 (Apr. 28, 2022), <https://curia.europa.eu/juris/documents.jsf?num=C-319/20>.

²⁴GDPR arts. 16, 20, and 21.

“Processing” is defined extremely broadly, including collection, structuring, storage, alteration, and erasure.²⁵

II. DSA

The DSA came into full effect on February 17, 2024, regulating internet intermediary services for “a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected.”²⁶ “Intermediaries” are digital services that shape our use of the internet, including social media platforms such as Facebook, search engines such as Google, and online marketplaces.

Unlike the GDPR, the DSA provides very few substantive protections for internet users, instead taking a procedural approach. The DSA introduces a package of transparency and procedural measures for online platforms, services that host content, to address illegal content by content moderation.²⁷ DSA procedural provisions require that platforms establish a mechanism to allow civil society to notify platforms of illegal content, and for platforms to take action in terms of content moderation—“notice and action” mechanism.²⁸ The DSA provides additional procedural obligations for very large online platforms (VLOPs) and very large online search engines (VLOSEs). VLOPs and VLOSEs are those with 45 million or more average monthly users.²⁹ The additional obligations primarily concern assessment and mitigation of “systemic risk,” which includes negative effects on human rights.³⁰

Alongside these procedural provisions, the DSA has a few substantive protections for users. The DSA prohibits dark patterns, profiling users for targeted ads based on special category data such as religion or sexual orientation, and targeting ads at minors based on profiling.³¹ There is also an obligation for VLOPs and VLOSEs to provide a version of their recommender systems without profiling.³² As Farinho has highlighted, dark patterns and profiling were already subject to a degree of regulation under the GDPR.³³ The DSA extends and increases data protection by prohibiting dark patterns and restricting particular profiling and targeting practices.³⁴ As discussed below, these substantive prohibitions and obligations are likely to have direct effects, allowing users to bring strategic litigation against tech platforms.

III. DMA

The DMA regulates major online platforms that act as “gatekeepers” to ensure contestable and fair digital markets to the benefit of business and end users. Gatekeepers are designated based on their

²⁵GDPR art. 4.

²⁶DSA art. 1(1).

²⁷DSA arts. 14, 16–23, and 27; DSA art. 3 (defining illegal content as “information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State.”).

²⁸DSA arts. 17, 20 (discussing various procedural requirements for content moderation decisions by platforms such as providing a statement of reasons when taking action and establishing an internal complaint mechanism).

²⁹DSA art. 33.

³⁰DSA art. 34 (requiring that VLOPs and VLOSEs conduct risk assessments of systemic risk and defining “systemic risk”); DSA art. 35 (requiring that VLOPs and VLOSEs must implement measures to mitigate systemic risks, including consideration of the design of recommender systems, advertising systems, and data practices); DSA art. 37, 39–40 (adding that VLOPs and VLOSEs must be subject to independent DSA compliance audits and meet additional transparency requirements).

³¹DSA arts. 25(1), 26(3), and 28(2).

³²DSA art. 38.

³³Domingos S. Farinho, *Personal Data Processing by Online Platforms and Search Engines: The Case of the EU Digital Services Act*, 9 PUB. GOVERNANCE, ADMIN. & FIN. L. REV. 37, 49–53 (2024).

³⁴*Id.*

size; control over an important gateway between consumers and business; and an entrenched position in the market.³⁵ The Commission designated six companies as gatekeepers in September 2023: Alphabet, including Google and YouTube; Amazon; Apple; ByteDance, which owns TikTok; Meta, including Facebook and Instagram; and Microsoft.³⁶

Gatekeepers' substantive DMA obligations—as set out in Articles 5–7—are quite detailed and technical and overlap with some existing protections such as purpose limitation, consent, and data portability under GDPR, as well as consumer law prohibitions concerning unfair practices.³⁷ Several DMA obligations benefit individual users by prohibiting gatekeepers from exploiting their market power in relation to anticompetitive or unfair agreements or practices, data protection, interoperability, and transparency.³⁸ For example, gatekeepers must obtain users' consent to track users for targeted advertising purposes outside of a gatekeeper's core platform service, or use personal data from a core platform service in another of the gatekeeper's services.³⁹ These provisions benefitting users are likely to have an implied right of action for users to litigate against gatekeepers based on direct effect, discussed below.

D. Civil Society's Role in Regulatory Enforcement

Before embarking on analysis of the GDPR, DSA, and DMA's enforcement mechanisms and potential for strategic litigation, the power dynamics of different kinds of mechanisms are worth noting. Access to justice is a well-established concept in international human rights.⁴⁰ The UN's Guiding Principles on Business and Human Rights set out three types of access to remedy mechanisms, which I use to categorize the remedy mechanisms under the GDPR, DSA, and DMA: State-based judicial mechanisms, state-based non-judicial grievance mechanisms, and non-state based grievance mechanisms.⁴¹ The public/private enforcement distinction cuts across the category of state-based judicial mechanisms, which is the mechanism for strategic litigation. Where the decision of a regulator is challenged in court the judicial mechanism relates to public enforcement, and where civil society litigates against a non-state actor the judicial mechanism provides private enforcement.

There are different power dynamics inherent in each type of mechanism. The role of civil society and business is structurally empowered in private enforcement through state-based judicial mechanisms and non-state-based grievance mechanisms.⁴² In the courtroom of a state-based judicial mechanism, civil society acting in the public interest of rights holders will be a party to litigation with the same kind of power over the conduct of proceedings as a defendant company. By contrast, state-based non-judicial grievance mechanisms of public regulatory enforcement have an asymmetric structure where business has greater power than people.⁴³ When civil society makes a complaint, the regulator has powers to decide whether and how to respond, and procedural fairness rules primarily concern the company that may be subject to the regulatory decision and not the complainant. These asymmetrical dynamics are illustrated starkly in

³⁵DMA art. 3.

³⁶European Commission Press Release IP/23/4328, Digital Markets Act: Commission Designates Six Gatekeepers (Sep. 6, 2023).

³⁷Not all of the obligations for gatekeepers in Articles 5-7 relate to users, many relate to and are for the benefit of business users, such as advertisers, and competitors.

³⁸DMA arts. 5(2),(5)-(9), 6(3)-(6), & 7.

³⁹DMA art. 5(2); Christophe Carugati, *Policy Brief: Compliance Principles for the Digital Markets Act*, BRUEGEL (Nov. 16, 2023), <https://www.bruegel.org/policy-brief/compliance-principles-digital-markets-act>.

⁴⁰See generally, G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

⁴¹Special Representative of the Secretary-General, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011).

⁴²Fabrizio Cafaggi, *Towards Collaborative Governance of European Remedial and Procedural Law?*, 19 THEORETICAL IN. L. 235, 239 (2018).

⁴³*Id.*

litigation over a regulator's decision or action, where a business will tend to have a right to appeal a regulator's decision about them, but the complainant may not have standing as discussed further below.⁴⁴

Awareness of these different kinds of enforcement mechanisms and their different power dynamics enables clearer analysis of the enforcement architecture of the GDPR, DSA, and DMA as a system, including the existence or absence of strategic litigation opportunities in these laws' legal opportunity structures.

I. Data Subjects and Data Protection Authorities Empowered by GDPR

The GDPR requires member states to provide independent public authorities to enforce the GDPR, commonly referred to as Data Protection Authorities [hereinafter DPAs]. Where there is cross-border processing of personal data, meaning data about someone in one member state is processed by a processor or controller that is based in another member state, the DPA for the member state where the processor or controller is based, or has its "main establishment," is the lead DPA.⁴⁵ This is commonly referred to as the "one-stop-shop mechanism" and is the reason that some DPAs, like Ireland's Data Protection Commissioner, have an outsized role in GDPR enforcement due to major companies having their European headquarters there.

GDPR provides robust public enforcement rights to civil society, providing a legal opportunity structure for strategic litigation to advance digital rights and influence regulators. People as "data subjects" have the right to make complaints regarding GDPR infringements to DPAs under Article 77. Article 78 provides a right to judicial remedy against DPAs for their decisions or failure to act, which enables strategic litigation by civil society. Under Article 80(1), people have a right to opt-in to being represented by a not-for-profit public interest entity. The representative can be empowered to exercise the rights of complaint or litigation, discussed below.⁴⁶ These public enforcement rights effectively recruit civil society as important actors in the GDPR regime, playing a bottom-up role of raising complaints, and enhancing enforcement.⁴⁷

The GDPR's public enforcement problems are well documented,⁴⁸ notably blockages resulting from the "one-stop-shop" mechanism and the Irish Data Protection Commission's inaction. For example, Schrems had to sue the Irish DPA to enforce the GDPR regarding cross-border data transfers, because that DPA failed to correctly deal with his complaint.⁴⁹ More broadly, many DPAs are seen as slow and ineffectual partly because of under-resourcing, and there is the further frustration that a complaint is largely out of the complainant's control once it is filed with a DPA, particularly in cross-border matters.⁵⁰ Differences in national procedural laws and DPAs' practices make cross-border matters difficult to navigate for civil society at present. The European

⁴⁴Monika Glavina, *Private-Interests Actors as Catalysts for Actions under Public Law: Towards a Research Agenda for Legal Mobilisation of Private-Interests Actors in the Preliminary Ruling Procedure*, 16 ERASMUS L. REV. 86, 97 (2023).

⁴⁵GDPR arts. 56 and 60 (setting out the competence of the lead supervisory authority and cooperation mechanism between the lead DPA and other DPAs concerned with a decision, for example if similar complaints have been made to multiple DPAs about the same practice by one company).

⁴⁶GDPR art. 80(2) (permitting member states to establish an opt-out mechanism for a not-for-profit public interest entity to enforce the GDPR through regulatory complaints or litigation); GDPR art. 80(1) (including representation in litigation on an opt-in basis for compensation, while Article 80(2) excludes representation in litigation on an opt-out basis for compensation). Unlike Article 80(1), implementation of Article 80(2) GDPR is optional for member states.

⁴⁷Woojeong Jang & Abraham L. Newman, *Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation*, 60 J. OF COMMON MKT. STUD. 283, 289-291 and 294 (2022).

⁴⁸See, e.g., Estelle Massé, *Four Years under the EU GDPR How to Fix its Enforcement*, ACCESS NOW (Jul. 2022), <https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-4-year-report-2022.pdf>; Johnny Ryan, *5 Years: GDPR's Crisis Point*, ICCL <https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf> (2023).

⁴⁹Noyb Win: € 1.2 Billion Fine Against Meta over EU-US Data Transfers, NOYB (May 22, 2023), <https://noyb.eu/en/edpb-decision-facebooks-eu-us-data-transfers-stop-transfers-fine-and-repatriation>.

⁵⁰Gentile & Lynskey, *supra* note 2, at 813-817.

Parliament and Council of Ministers are in a legislative process for new rules on GDPR enforcement in cross-border cases that would address many of these concerns, aiming to harmonize cross-border cooperation through common procedural rules, speed procedures by setting deadlines for DPAs, and improve access to information.⁵¹

II. Civil Society's (Marginal) DSA Enforcement Role

There was a lot of talk among civil society about needing the DSA to learn lessons from the problems with GDPR enforcement, focusing almost exclusively on public regulatory enforcement.⁵² National regulators, called “Digital Services Coordinators” [hereinafter DSCs], are responsible for enforcement at a national level.⁵³ The DSA reproduces the GDPR’s one-stop-shop by giving exclusive competence to the DSC of the member state where a company has its main establishment, which has been criticized,⁵⁴ although there is a two month limit for a DSC to respond to other DSCs.⁵⁵ The European Commission has exclusive enforcement powers for Chapter III Section 5 concerning systemic risks of the largest companies.⁵⁶ The time limit and European Commission’s competence respond to one-stop-shop problems in cross-border GDPR matters.

DSA public enforcement rights of internet users are more limited than the GDPR. Users have a right to lodge a complaint with a DSC under Article 53, including rights to be heard and receive information on the complaint’s status, but no explicit right for complaints to the Commission on systemic risk. Article 86 allows users to mandate an entity to exercise the users’ rights under the DSA.⁵⁷ Unlike the GDPR, the DSA does not include a right to judicial review of DSC decisions, although many member states have existing rights of judicial review for regulators’ decisions and aspects of the DSA could be judicially enforced based on the principle of direct effect.⁵⁸

⁵¹New Measures to Strengthen the Cross-Border Enforcement of the GDPR, European Parliament News, <https://www.europa.eu/press-room/20240212IPR17631/new-measures-to-strengthen-the-cross-border-enforcement-of-the-gdpr>; Data protection cross-border enforcement: statement by rapporteur Markéta Gregorová, European Parliament News, (Nov. 4, 2024) <https://www.europarl.europa.eu/news/en/press-room/20241104IPR25136/data-protection-cross-border-enforcement-statement-by-the-rapporteur>. See also Report 2016/679 of Feb. 20, 2024, Proposal for a Regulation of the European Parliament and of the Council Laying Down Additional Procedural Rules Relating to the Enforcement of Regulation (EU).

⁵²See e.g., Asha Allen & Ophélie Stockhem, *A Series on the EU Digital Services Act: Ensuring Effective Enforcement*, CENTER FOR DEMOCRACY & TECHNOLOGY (Aug. 18, 2022), <https://cdt.org/insights/a-series-on-the-eu-digital-services-act-ensuring-effective-enforcement/>; Eliška Pirková, *The EU Digital Services Act Won't Work Without Strong Enforcement*, ACCESSNOW (Jan. 13, 2023), <https://www.accessnow.org/eu-dsa-enforcement/>.

⁵³DSA art. 49. See also Ilaria Buri & Joris van Hoboken, *The DSA Supervision and Enforcement Architecture*, DSA OBSERVATORY (Jun. 24, 2022), <https://dsa-observatory.eu/2022/06/24/the-dsa-supervision-and-enforcement-architecture/>.

⁵⁴DSA art. 56. See e.g., Gerhard Wagner, Martin Eifert, Axel Metzger, & Heike Schweitzer, *Taming the Giants: The DMA/DSA Package*, 58 COMMON MKT. L. REV. ET AL. 987, 1021 (2021); Can Şimşek, *Digital Services Act: Will the EU Draw Lessons from the GDPR?*, SCIENCESPO (Oct. 2, 2021), <https://www.sciencespo.fr/public/chaire-numerique/en/2021/10/02/digital-services-act-will-the-eu-draw-lessons-from-the-gdpr/>.

⁵⁵DSA art. 58(5).

⁵⁶DSA art. 56.

⁵⁷DSA arts. 16, 22, 37 & 40 (providing that civil society can contribute to DSA implementation as “trusted flaggers” of illegal content whose notices to online platforms are to be given priority, and potentially as independent auditors of VLOPs and VLOSEs or “vetted researchers” with access to VLOP and VLOSE data).

⁵⁸See e.g., Case C-103/88, Fratelli Costanzo SpA v. Comune di Milano, ECLI:EU:C:1989:256, (Jun. 22, 1989), <https://curia.europa.eu/juris/showPdf.jsf?text=&docid=96045&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6716603>; Case C-222/84, Marguerite Johnston v. Chief Constable of the Royal Ulster Constabulary, ECLI:EU:C:1986:206, (May 15, 1986), <https://curia.europa.eu/juris/fiche.jsf?id=C%3B222%3B84%3BRP%3B1%3BP%3B1%3BC1984%2F0222%2FJ&language=en>; Case C-41-74 Yvonne van Duyn v. Home Office, ECLI:EU:C:1974:133, (Dec. 4, 1974), <https://curia.europa.eu/juris/liste.jsf?language=en&T,F&num=41/74>.

III. Civil Society at the Outer Edge of DMA Regulation

The DMA provides even more limited public enforcement avenues for civil society than the DSA or GDPR. The Commission has exclusive competence for public enforcement of the DMA, with obligations to cooperate with national authorities, particularly those enforcing competition rules.⁵⁹ Third parties, which includes civil society, may inform the Commission about infringements of the DMA under Article 27. However, the Commission has full discretion on whether to follow up, and the third party has no entitlement concerning any proceedings that arise from their informing in contrast with antitrust law that entitles complainants to be closely associated with proceedings.⁶⁰ Strategic litigation by civil society to directly challenge the Commission is not possible due to the rules of standing, as the following section discusses.

IV. Centralized Regulation Precludes Strategic Litigation by Civil Society

The highly constrained rules on standing for judicial review of EU actions, described in the framing Article,⁶¹ mean that civil society seeking to bring strategic litigation are unlikely to satisfy admissibility concerning DSA or DMA acts by the Commission.⁶² Judicial review by civil society of public regulators is an important mechanism for strategic litigation as the (in)famous *Schrems* cases have illustrated. The *Schrems* cases reached the CJEU as indirect actions referred under Article 267 Treaty on the Functioning of the European Union [hereinafter TFEU], but national courts do not have jurisdiction to review DSA and DMA acts by the Commission. DSA and DMA Commission acts will be addressed to companies, which will have standing under Article 263 TFEU to challenge such acts. But civil society would only have standing if they could demonstrate direct and individual concern. Such acts will not confer rights or impose obligations on civil society, so there will be no “direct concern,”⁶³ and civil society will not have standing to bring strategic litigation against the Commission.⁶⁴

Civil society plays the role of a supplicant in DSA and DMA enforcement against big tech, submitting evidence of infringements to the Commission, but unable to bring strategic litigation. For example, technology investigation civil society organization AI Forensics recently celebrated the Commission’s launching investigation proceedings into Meta following AI Forensics’ report on pro-Russian propaganda ads on Meta’s platforms.⁶⁵ Yet, if the Commission falls short of robust DSA enforcement, AI Forensics has no legal recourse. By contrast, there have already been many legal challenges by big tech companies to the Commission’s early regulatory actions under the DSA.⁶⁶ Legal interpretation of these new digital rights instruments looks set to become a site of contestation between commercial interests and the Commission, but civil society will be voiceless

⁵⁹DMA arts. 37–38.

⁶⁰Giorgio Monti, *Issues Paper: Procedures and Institutions in the DMA*, CTR. REGUL. EUR. (Dec. 2022) https://cerre.eu/wp-content/uploads/2022/12/DMA_Institutions_and_Procedures.pdf.

⁶¹Cebulak, Morvilla, and Salomon, *supra* note 19, at 189–191.

⁶²Case T-600/15, *Pesticide Action Network Europe v. Commission*, ¶¶ 25–7 (Sep. 28, 2016), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015TO0600>. See also Marta Morvillo & Maria Weimer, *Who Shapes the CJEU Regulatory Jurisprudence? On the Epistemic Power of Economic Actors and Ways to Counter it*, 1 EUR. L. OPEN 510, 518–21 (2022). See also Suzanne Vergnolle, *Enforcement of the DSA and the DMA – What Did We Learn from the GDPR?*, in MAX PLANCK INST. INNOVATION AND COMPETITION RSCH. PAPER NO. 21-25 TO BREAK UP OR REGULATE BIG TECH? AVENUES TO CONSTRAIN PRIVATE POWER IN THE DSA/DMA PACKAGE 103 (Heiko Richter et al. eds., 2021) (raising rule of law and constitutional concerns about the EU Commission acting as regulator).

⁶³Case T-600/15, *Pesticide Action Network Eur. v. Comm’n*, ECLI:EU:T:2016:601, ¶ 62 (Sep. 28, 2016), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015TO0600>.

⁶⁴See Case C-25/62, *Plaumann & Co. v. Comm’n of the Eur. Econ. Cmty.*, ECLI:EU:C:1963:17 (July 15, 1963), <https://curia.europa.eu/juris/liste.jsf?language=en&T,F&num=25-62>. See also Gentile & Lynskey, *supra* note 2, at 817.

⁶⁵No Embargo in Sight: *Meta Lets Pro-Russian Propaganda Ads Flood the EU*, AI FORENSICS (May 17, 2024) <https://aiforensics.org/work/meta-political-ads>.

⁶⁶See e.g., Jon Porter, *Meta and TikTok Challenge Fees Paid to Fund EU’s New DSA*, THE VERGE (Feb. 8, 2024), <https://www.theverge.com/2024/2/8/24065809/meta-european-union-digital-services-act-monitoring-compliance-charge-challenge>; Clothilde

in court, particularly because of the restricted approach to third party interventions which tend not to be allowed before the CJEU.⁶⁷

The structural power dynamics of public enforcement through state-based non-judicial mechanisms, noted above, asymmetrically disempower people from strategic litigation while giving business a central role, particularly in the DSA and DMA compared to the GDPR. These Acts aim to regulate internet giants and uphold the rights of users, but the lack of litigation rights for users in relation to the Commission mean that the GDPR may remain the main site for strategic litigation by civil society concerning regulatory enforcement of digital rights. Meanwhile, internet giants will shape regulatory interpretation of the DSA and DMA through litigation.

V. Fractured and Fragmented Regulatory Enforcement of Digital Rights

The increasingly complex regulatory landscape places a burden on civil society to navigate the multiplicity of regulators that have competence to uphold digital rights in the internet audience economy.⁶⁸ This multiplicity of regulators at national and EU levels results from multiple areas of relevant legislation with parallel enforcement regimes relevant to big tech, such as equality laws which are not an area discussed in detail in this Article, but which could overlap with GDPR and DSA protections.⁶⁹ EU equality legislation requires member states to establish equalities bodies.⁷⁰ So, for example, if racist content was amplified by recommender systems based on personal data about users in France, then civil society would need to decide whether to file complaints to the DPC *Le Régulateur de la Communication Audiovisuelle et Numérique*, DPA *Commission Nationale de l'Informatique et des Libertés*, or equalities body *Défenseur des Droits*. Regulators themselves bring strategic litigation, including against big tech companies as illustrated below in *Meta v. Bundeskartellamt*, although I have not considered this in detail because my focus is on civil society actors in strategic litigation. However, this role of regulators in litigation is worth bearing in mind since the allocation of finite resources among multiple different regulators risks leaving regulators under-resourced to litigate against big tech.

DSCs and the Commission as DSA and DMA regulator will be added to the already fragmented landscape of regulators enforcing digital rights against big tech that could lead to inconsistent decisions and incoherence of the law.⁷¹ For example, the CJEU *Meta v. Bundeskartellamt* decision in 2023 considered regulatory overlap between competition law and the GDPR.⁷² The German

Goujard, *Amazon Loses EU Court Bid to Delay Digital Rules on Online Ads*, POLITICO (Mar. 27, 2024), <https://www.politico.eu/article/amazon-loses-eu-court-bid-to-delay-digital-rules-on-online-ads/>.

⁶⁷See e.g., Jasper Krommendijk & Kris van der Pas, *To Intervene or Not to Intervene: Intervention Before the Court of Justice of the European Union in Environmental and Migration Law*, 26 INT'L J. OF HUM. RTS. 1394, 1397-1399 and 1401-1402 (2022).

⁶⁸See e.g., *Statement on the Digital Services Package and Data Strategy*, EUROPEAN DATA PROTECTION BOARD (Jul. 2022), https://www.edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf. Cf., *Creating a French Framework to Make Social Media Platforms More Accountable: Acting in France With A European Vision*, RÉPUBLIQUE FRANÇAISE (May 2019), https://www.dimt.it/wp-content/uploads/2019/07/minifi.hosting.augure.com_Augure_Minifi_r_ContentuEnLigne_DownloadidAE5B7ED5-2385-4749-9CE8-E4E1B36873E4filenameMission-Régulation-de-s-réseaux-sociaux-ENG.pdf; *The future of digital technologies governance: Summary of the plenary session organised by AFNIC and Renaissance Numérique on 5 December 2022*, RENAISSANCE NUMÉRIQUE (Jul. 2022), <https://www.renaissancenumerique.org/en/publications/the-future-of-digital-technologies-governance/>.

⁶⁹Bengi Zeybek & Joris van Hoboken, *The Enforcement Aspects of the DSA, and its Relation to Existing Regulatory Oversight in the EU*, DSA OBSERVATORY (Feb. 4, 2022) <https://dsa-observatory.eu/2022/02/04/the-enforcement-aspects-of-the-dsa-and-its-relation-to-existing-regulatory-oversight-in-the-eu>.

⁷⁰See, e.g., Council Directive 2000/43/EC of June 29, 2000, Implementing The Principle of Equal Treatment Between Persons Irrespective of Racial or Ethnic Origin, 2000 O.J. (L 180); Council Directive 2004/113/EC of Dec. 13, 2004 Implementing the Principle of Equal Treatment Between Men And Women in the Access To and Supply of Goods and Services, 2004 O.J. (L 373).

⁷¹Zeybek & Hoboken, *supra* note 69.

⁷²Case C-252/21, *Meta Platforms and Others*, ECLI:EU:C:2023:537 (Jul. 4, 2023), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9446770>.

competition regulator found that Meta abused its dominant market position by collecting personal data on and off Facebook and linking those data to users' profiles to target advertising. The CJEU concluded that a competition authority has competence to determine whether the GDPR has been infringed where such determination is necessary to establish whether there has been an abuse of dominant market position contrary to competition law.⁷³ However, it remains to be seen what might happen if regulators take divergent views of the law, for example the Irish Data Protection Commission could find Meta's practices did not breach the GDPR, while competition regulators in other member states found abuse of dominant market position arising from GDPR breaches. The CJEU anticipated this risk and emphasized the importance of the duty of sincere cooperation between supervisory authorities, requiring cooperation to ensure consistent application of the law.⁷⁴

Private enforcement through strategic litigation, discussed in the following section, can promote legal coherence through judicial decisions that integrate the application of different areas of law to the same facts.

E. Civil Society's Opportunities to Use Private Enforcement for the Public Interest

Access to justice requires that users themselves have access to remedy, even if public regulators were to perfectly apply users' digital rights against big tech companies. Article 47 of the EU Charter of Fundamental Rights provides for access to justice and the right to an effective remedy, including that "[e]veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal".⁷⁵ In some cases regulatory action will have a similar effect as private enforcement, for example where declaratory or injunctive relief are sought, but not where users seek redress from a company. For example, where a regulator imposes a fine on a company that fine will go to the state, whereas if people sue the company for the same breach then the claimants will receive any damages awarded.

Private enforcement can also benefit the public interest from political and economics perspectives by mitigating the risk of a lack of political will for public enforcement of the law and reducing the financial burden on regulators.⁷⁶ Amplification of (dis)information on the internet based on processing of personal data to profile users is a deeply political subject, particularly during elections. Enforceable human rights can provide a counterweight to majoritarian views⁷⁷ or political influences that could arise that oppose robust public regulation of big tech's impact on human rights. Private enforcement strategic litigation also produces public goods of court decisions and precedents advancing legal interpretation.⁷⁸

I. Turning Towards Private GDPR Enforcement—Problems of Standing

The GDPR expressly provides robust private enforcement rights in parallel with the public enforcement rights enabling strategic litigation, and private enforcement strategic litigation has been an important part of advancing GDPR digital rights.⁷⁹ For example, although not related to internet users as such, litigation against Uber has used the GDPR to advance workers' rights, setting new precedents on transparency of data processing and automated decision making by

⁷³*Id.*, at ¶¶ 48, 51, and 62.

⁷⁴*Id.*, at ¶¶ 52-61, and 63.

⁷⁵*Access to Justice in Europe*, E.U. AGENCY FOR FUNDAMENTAL RTS., https://fra.europa.eu/sites/default/files/fra_uploads/1506-FRA-Factsheet_AccesstoJusticeEN.pdf.

⁷⁶Podszun, *supra* note 7, at 95-96; Picht, *supra* note 7, at 98-99.

⁷⁷Ander Maglica, *supra* note 3, at 71.

⁷⁸Adrian Cordina, *Is It All That Fishy? A Critical Review of the Concerns Surrounding Third Party Litigation Funding in Europe*, 14 ERASMUS L. REV. 270, 274 (2021).

⁷⁹See e.g., Tijmen Wisman, *The SyRI Victory: Holding Profiling Practices to Account*, DIGIT. FREEDOM FUND (Apr. 23, 2020), <https://digitalfreedomfund.org/the-syri-victory-holding-government-profiling-to-account/>.

companies.⁸⁰ People have the right to bring litigation directly against a data controller or processor for GDPR infringements and receive compensation.⁸¹ Civil society organizations are increasingly focused on private enforcement of the GDPR through strategic litigation against big tech, responding in part to the problems of public enforcement discussed above.⁸² However, prior to RAD, discussed below, civil society organizations had limited private enforcement avenues due to lack of standing.⁸³

Some consumer protection organizations have found a work around using standing under consumer protection law to bring strategic litigation. In 2022, the CJEU found that consumer protection associations had standing to bring claims for unfair commercial practices and consumer protection law infringements that related to GDPR infringements in *Meta Platforms Ireland Limited v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*⁸⁴ The German Federal Association of Consumer Organizations [hereinafter vzbv] argues that the information disclosed by the games in the App Centre fails to obtain valid consent for data processing. Vzbv relied on their standing under the Law against unfair competition and the Law on Injunctions, which both implement EU Directives, not standing under GDPR.⁸⁵ This work around may enable more public interest private enforcement action by consumer protection organizations, framing GDPR breaches as infringements of consumer protection, itself a fundamental right recognized in the Charter under Article 38. However, there may be a problem in access to justice terms if digital rights infringements can only be remedied when they coincide with consumer protection law.

II. Enforcing Digital Rights as a Whole

Private enforcement strategic litigation enables civil society to argue multiple areas of law in a single case, as the vzbv case against Facebook illustrates, which can promote coherent interpretation of the law. The DMA and DSA do not expressly provide for private enforcement by

⁸⁰Historic Digital Rights Win for WIE and the ADCU over Uber and Ola at Amsterdam Court of Appeal, WORKER INFO EXCH. (Apr. 4, 2023), <https://www.workerinfoexchange.org/post/historic-digital-rights-win-for-wie-and-the-adcu-over-uber-and-ola-at-amsterdam-court-of-appeal>.

⁸¹GDPR arts. 79 and 82.

⁸²Massé, *supra* note 48; Jennifer Bryant, *CJEU Ruling on GDPR Litigation Builds ‘Jurisprudence on Data Protection,’* IAPP (May 24, 2022), <https://iapp.org/news/a/cjeu-ruling-on-gdpr-litigation-by-consumer-groups-builds-jurisprudence-on-data-protection/>.

⁸³ONE YEAR UNDER THE EU GDPR: AN IMPLEMENTATION PROGRESS REPORT, ACCESS NOW (MAY 2019), <https://www.accesnow.org/wp-content/uploads/2019/06/One-Year-Under-GDPR.pdf> (explaining that most member states have not implemented GDPR Art 80(2) that would provide an opt-out mechanism for organizations to more easily represent individuals); Alexia Pato, *The National Adaptation of Article 80 GDPR: Towards the Effective Private Enforcement of Collective Data Protection Rights*, in NATIONAL ADAPTATIONS OF THE GDPR 98, 100-104 (Karen McCullagh, Olivia Tambou & Sam Bourton eds., Feb. 2019) (examining national adaptation of GDPR art. 80 in France, Belgium, Spain, Germany, Austria, and the UK).

⁸⁴Case C-319/20, *Meta Platforms Ir. Ltd. v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2022:322 (Apr. 28, 2022), <https://curia.europa.eu/juris/document/document.jsf?docid=258462&doclang=en>.

⁸⁵Gesetz gegen den unlauteren Wettbewerb [Law Against Unfair Competition], Mar. 7, 2004, BGBl I at 254, art. 8, last amended by Gesetz [G], May 6, 2024, BGBl I at 149, art. 6 (Ger.), https://www.gesetze-im-internet.de/uwg_2004/ (implementing Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market and Amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, 2005 O.J. (L 149) 22) See also Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen [UKlaG] [Law on Injunctions], Nov. 26, 2001 BGBl I at 4346, last amended by Gesetz [G], May 6, 2024, BGBl I at 149, art. 18 (Ger.), <https://www.gesetze-im-internet.de/uklag/BJNR317300001.html> (implementing Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on Injunctions for the Protection of Consumers’ Interests, 2009 O.J. (L 110) 30). The provisions for standing are paragraph 8(3) of the Law against unfair competition and point 1 of the first sentence of Paragraph 3(1) of the Law on Injunctions.

users with the same clarity as the GDPR,⁸⁶ but many of their substantive provisions could be used as the basis for strategic litigation against internet giants. Breaches of the DSA or DMA also provide a basis for a representative action through procedural mechanisms under RAD,⁸⁷ discussed below. Civil society could bring private enforcement strategic litigation based on relevant legal protections from the DSA or DMA as well as the GDPR, competition or consumer law, relying on these laws as applicable to the facts of a case. Such an approach would foster legal coherence in judicial decisions that address multiple overlapping areas of law but requires a high level of expertise across multiple areas of law, which needs significant financial resource.

An EU law provision can be enforced in national courts through private enforcement litigation if the provision meets the criteria for direct effect and an implied right of action, which is relevant for the DMA and DSA. The criteria for direct effect have been established by CJEU case law: A provision must be clear and sufficiently precise; unconditional, and not subject to further implementation; and confer a right or provide an obligation that protects the interests of a category of people to which the claimant belongs.⁸⁸ Where a provision of EU law meets these criteria, the claimant has a right of action for litigation in national courts, based on the overarching goal of ensuring the effectiveness of EU law.⁸⁹

Some provisions in the DMA and DSA will meet the criteria for direct effect, but which ones will remain uncertain unless and until there is strategic litigation that mobilizes judicial decisions. Commentators broadly agree that Articles 5-7 of the DMA have direct effect and imply a right of action, which users can use to enforce obligations that benefit them.⁹⁰ There is disagreement on the scope for private enforcement of DSA provisions, but the substantive prohibitions and protections concerning profiling and dark patterns, identified above, probably have direct effect.⁹¹ DSA Article 54 expressly provides a right for users to seek compensation for damages resulting from a DSA breach, although the DSA is silent on rights to other judicial remedies.⁹²

Jurisdiction will be an additional potential hurdle for strategic litigation by civil society against internet giants, even in cases where a right of action is expressly provided or recognized by the

⁸⁶Bengi Zeybek, Joris van Hoboken & Ilaria Buri, *Redressing Infringements of Individuals' Rights Under the Digital Services Act*, DSA OBSERVATORY (May 4, 2022), <https://dsa-observatory.eu/2022/05/04/redressing-infringements-of-individuals-rights-under-the-digital-services-act/>.

⁸⁷DSA art. 90 (amending the RAD to add the DSA to the laws upon which a mass claim can be made for a judicial remedy where there is an infringement of EU law); DMA art. 42 (stating that RAD “shall apply to the representative actions brought against infringements by gatekeepers of provisions of this Regulation that harm or may harm the collective interests of consumers”).

⁸⁸Case 26/62 Van Gend en Loos v. Nederlandse Administratie der Belastingen, ECLI:EU:C:1963:1 (Feb. 5, 1963), <https://curia.europa.eu/juris/fiche.jsf?id=C%3B26%3B62%3BRP%3B1%3BP%3B1%3BC1962%2F0026%2FJ&language=en>.

⁸⁹See e.g., Case C-724/17, Vantaan kaupunki v. Skanska Industrial Solutions Oy and Others, ECLI:EU:C:2019:204, (Mar. 14, 2019), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=211706&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7142666>.

⁹⁰Assimakis Komninos, *Private Enforcement of the DMA Rules Before the National Courts* (Apr. 5, 2024), <https://ssrn.com/abstract=4791499>. See also Podszun, *supra* note 7, at 95-96; Sánchez, *supra* note 7, at 7.

⁹¹Compare, Sánchez, *supra* note 7, at 7 (stating the due diligence provisions on illegal content, such as the requirement for a notice and action mechanism, may give rise to rights related to the outcome of such mechanism as well as a right to the procedure as such based on a more expansive interpretation of the DSA), with Martin Husovec, *Will the DSA Work? On Money and Effort*, VERFBLOG (Nov. 9, 2022) <https://verfassungsblog.de/dsa-money-effort/>, and Marta C. Gamito, *Do Too Many Cooks Spoil the Broth? How EU Law Underenforcement Allows TikTok's Violations of Minors' Rights*, 46 J. CONSUMER POL'Y 281, 298 (2023). See also, Farinho, *supra* note 33, at 37 (giving a characterization of the notice and action mechanism obligations as procedural); Jeanne Mouton, *Unbalanced Power Relationship in Digital Markets Between Platforms and Their Complementors: Can Consumers Come to the Rescue?*, 7 MKT. & COMPETITION L. REV. 71, 86 (2023).

⁹²DSA art. 20 (mandating that online platforms provide a non-state-based grievance mechanism, and provides for out-of-court dispute settlement, but these mechanisms do not meet the access to justice principle in Article 47 of the Charter and platforms must provide an internal complaints mechanism for content moderation decisions, which encompasses decisions to take down content, and suspending or terminating accounts or content monetization); DSA art. 21 (providing users may take unresolved disputes to out-of-court dispute settlement). Unlike a state-based judicial mechanism, out-of-court dispute settlement will not produce public goods from judgments that advance legal interpretation.

courts. The question of jurisdiction in cross-border cases is complicated, as discussed further below, and depends on the nature of the claim, for example consumer law or tort, and the facts of the case. Article 79(2) of the GDPR expressly provides that data subjects can litigate against companies in the claimant's home jurisdiction, but there is no such provision in the DMA or DSA.⁹³

Claims for damages act as a deterrent against breaching the law, which is in the public interest, but GDPR litigation suggests that courts may be reluctant to award damages for breaches of digital rights. In the context of competition law, the CJEU has pointed to private claims for damages as “an integral part of the system for enforcement” of law, ensuring full effectiveness of legal prohibitions, and discouraging practices that breach EU law.⁹⁴ Financial compensation is technically possible for loss or damage for a user due to a breach of obligations in the DSA, under Article 54, or DMA, based on direct effect. The GDPR recognizes a right to compensation for non-material damages, which neither the DSA nor DMA provide for, yet claimants have struggled to obtain damages where their GDPR rights have been infringed even with this express right for non-material damages.⁹⁵ Similarly, difficulty in obtaining damages in competition law makes DMA enforcement for compensation based on existing principles uncertain at best.⁹⁶ Thus, even though private claims for damages are an important part of EU law enforcement, there is considerable uncertainty whether claims seeking financial remedies will be successful against internet giants and may be even more difficult under the DSA and DMA.

Private enforcement strategic litigation could advance digital rights against internet giants and facilitate legal coherence across the many applicable areas of law that provide rights and protections for internet users. However, the legal opportunity structures for strategic litigation include considerable barriers, such as uncertainty over private rights of action based on direct effect, the resources and legal expertise needed to incorporate arguments from multiple areas of law, and questions of jurisdiction and remedies. In addition, litigation in different national courts could fracture EU law, which points to the importance of preliminary references to the CJEU and EU Commission contributions in such litigation.⁹⁷

III. A Collective New Hope: RAD

The 2020 Directive on Representative Actions for the Protection of the Collective Interests of Consumers, or RAD, aims to strengthen EU consumer protection law enforcement by requiring

⁹³Pietro Ortolani, *If You Build it, They Will Come: The DSA “Procedure Before Substance” Approach*, VERFBLOG (Nov. 7, 2022), <https://verfassungsblog.de/dsa-build-it/>.

⁹⁴See e.g., Case C-724/17, *Vantaan kaupunki v. Skanska Industrial Solutions Oy and Others*, ECLI:EU:C:2019:204, ¶¶ 43-45 (Mar. 14, 2019), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=211706&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7144093>.

⁹⁵Two decisions by the CJEU in 2023 on non-material damages interpret the right to redress under the GDPR, but uncertainty remains. In *Österreichische Post* the Court emphasized that three conditions must be met for compensation: Damage has been suffered, there has been an infringement of the GDPR, and there is a causal link between the infringement and damage. Case C-300/21 *UI v. Österreichische Post AG*, ECLI:EU:C:2023:370, ¶¶ 32, 36 (May 4, 2023), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=5955759>. The Court then clarified its views in *VB v. Natsionalna agentsia za prihodite*, concluding that: “[T]he fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of [the GDPR] is capable, in itself, of constituting ‘non-material damage’”. Case C-340/21 *VB v. Natsionalna agentsia za prihodite* ECLI:EU:C:2023:986, ¶ 82 (Dec. 14, 2023), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0340>. The Court underscored recital 146, which states that the concept of damage should be widely interpreted, and recital 85's broad illustrative list of types of damage including loss of control over personal data, limitation of rights, discrimination, financial loss, or other economic or social disadvantage.

⁹⁶Case C-26/62 *Van Gend en Loos v Nederlandse Administratie der Belastingen*, ECLI:EU:C:1963:1 (Feb. 5, 1963), <https://curia.europa.eu/juris/showPdf.jsf?text=&docid=87094&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7144773>; Podszun, *supra* note 7, at 95-96

⁹⁷DSA art. 82; DMA art. 39; Komninos, *supra* note 83.

that member states have civil procedure mechanisms for representative actions.⁹⁸ A representative action is a kind of mass claim, which is where one case addresses similar legal claims of multiple individuals, for example, the individuals all bought the same faulty model of car. In a representative action, an organization represents the interests of individuals, litigating on their behalf. Such organizations act as intermediaries and, potentially, gatekeepers for access to justice—RAD calls these organizations “qualified entities” [hereinafter QEs].⁹⁹

RAD applies to digital rights legislation and could enhance strategic litigation opportunities, but only for harm to consumers’ interests. RAD requires member states to have a representative action mechanism for both injunctive and redress measures.¹⁰⁰ Redress measures include compensation, price reduction, or reimbursement of the purchase price.¹⁰¹ RAD applies to GDPR, DSA, and DMA, which means that if they are infringed then a representative action can be brought. Yet, as with the use of consumer protection laws to provide standing discussed above, access to justice under RAD may be limited to overlap with consumer rights and not effectively protect all human rights in the scope of the GDPR, DSA, and DMA, particularly if digital rights organizations are unable to become QEs, discussed below.¹⁰²

Although RAD is new, the pre-existing mass claims mechanism in the Netherlands illustrates the potential benefits of such mechanisms for digital rights claims against internet giants, as well as the associated procedural barriers. As explained above, the scale and diffuse harms by internet giants to users’ digital rights are complex, opaque, and occur at scale, which means that mass claims could provide a particularly important access to justice mechanism because the claims of many users can be combined in a single case. RAD’s recitals highlight that consumers navigate a digitalized marketplace and receive digital services, increasing the need for enforcement of data protection law.¹⁰³ The Netherlands introduced a new regime for representative actions in 2020, known by its Dutch acronym WAMCA, and has since then become a hub jurisdiction for representative actions against big tech companies, including litigation against Google; X, or Twitter; Facebook; Apple; and TikTok.¹⁰⁴ This relatively high number of claims against internet giants in the Netherlands demonstrates that many actors in litigation—lawyers, litigation funders, and claimant organizations—see representative actions as well suited for claims against these companies, but there are notable procedural barriers in representative claims.

The potential procedural complexity of a new representative action regime is also illustrated by examples in the Netherlands. Significant time and resource has been spent establishing admissibility in cases, with difficulties related to whether the claimant organization is

⁹⁸Non-transposition of EU Legislation: Commission Takes Action to Ensure Complete and Timely Transposition of EU Directives, (Jan. 27, 2023), https://ec.europa.eu/commission/presscorner/detail/EN/inf_23_262 (stating 24 member states missed the deadline to transpose RAD into national law by 25 December 2022); *Current Collective Action Landscape Map*, BIRD & BIRD, <https://www.twobirds.com/en/trending-topics/consumer-class-actions/current-collective-action-landscape-map> (stating most member states had implemented RAD or had draft laws underway by the end of 2023); see also *The Representative Actions Directive across Central Europe*, DELLOITTE (Oct. 2024), available for download at <https://www.deloitte.com/lt/en/service/s/legal/analysis/the-representative-actions-directive-across-central-europe.html> (last visited Nov. 24, 2024)

⁹⁹Visscher & Faure, *supra* note 8, at 468–70.

¹⁰⁰RAD art. 1(2).

¹⁰¹RAD art. 3.

¹⁰²Maglica, *supra* note 3, at 81–82.

¹⁰³See, e.g., RAD Recitals (1), (5) and (13).

¹⁰⁴Evelyn Tjon-En-Fa, *The Continuing Rise of Consumer Litigation in the EU: A Deep Dive Into Current Trends - Trend 1: Consumer Class Actions*, BIRD & BIRD (Dec. 6, 2023), <https://www.twobirds.com/en/disputes-plus/shared/insights/2023/global/the-continuing-rise-of-consumer-litigation-in-the-eu-trend-1-consumer-class-actions>; *Almost 5 years of class actions under the WAMCA: What is New?*, LOYENS & LOEFF (Sep. 11, 2024), <https://www.loyensloeff.com/insights/news-events/news/almost-5-years-of-class-actions-under-the-wamca-what-is-new/>; Zachary Pogust, *Dutch Class Action Regime: Closing in on Two Years of WAMCA*, POGUST GOODHEAD (Dec. 14, 2021), <https://pogustgoodhead.com/opinions/dutch-class-action-regime-closing-in-on-two-years-of-wamca/>.

representative and whether the interests in the claim are sufficiently similar.¹⁰⁵ For example, The Privacy Collective filed a representative action against Oracle and Salesforce concerning their data practices profiling internet users on August 14, 2020, which was found inadmissible by the District Court of Amsterdam on December 29, 2021 on the basis that The Privacy Collective was not sufficiently representative. However, the claim was found admissible by the Amsterdam Court of Appeal on June 18, 2024.¹⁰⁶ There has not yet been an outcome on the merits of the case. In time the requirements for admissibility may be clarified by judicial decisions, streamlining the process for representative actions, but until then litigation under a new representative action mechanism takes considerable time and resources.

RAD takes a pluralistic approach and does not stipulate procedural requirements: Member states can decide whether to establish an opt-in or opt-out mechanism, the process for individuals opting in or out including deadlines, and thresholds for admissibility of claims.¹⁰⁷ Opt-out mechanisms mean that people benefit from the litigation if it is successful unless they opt-out of participating, whereas an opt-in mechanism requires that people actively opt-in to benefit.¹⁰⁸

1. Standing and Cross-border Jurisdiction under RAD

QEs play a central role under RAD given that individuals can only bring claims through a QE, so which organizations can be a QE and whether they prioritize human rights will shape digital rights strategic litigation. RAD allows member states to decide the criteria for QEs to be qualified to bring domestic representative actions but sets the qualification criteria for QEs to bring cross-border representative actions.¹⁰⁹ A representative entity needs to have standing as a QE for a case to be admissible. The criteria for QEs to bring cross-border representative actions include twelve months of activity, a statutory purpose that “demonstrates that it has a legitimate interest in protecting consumer interests,” “a non-profit-making character,” and independence. Consumer protection associations are likely to meet these criteria and are specifically referred to in Recital 24, but digital rights organizations may struggle because of the requirement to focus on consumer interests, and therefore be unable to bring strategic litigation under RAD.

There are no jurisdiction provisions in RAD and there is considerable uncertainty over jurisdiction for cross-border actions, which is relevant to strategic litigation against internet giants. One approach would be that of the 2004 decision in *Henkel*, where an Austrian consumer protection association was able to bring a representative injunctive action in Austria against a business based in Germany.¹¹⁰ The CJEU found that action to prevent a trader from using unfair terms in contracts was a matter relating to tort, delict, or quasi-delict and therefore jurisdiction lay where the harm would occur, which was where the affected consumers live. However, in 2018 in *Schrems II*, the CJEU found that where consumer claims had been assigned by others, the plaintiff could not rely on the jurisdiction afforded to that plaintiff as an individual consumer to bring

¹⁰⁵Mirjam van Dam & Tim Kluwen, *Admissibility*, in UNLOCKING THE WAMCA: A PRACTICAL GUIDE TO THE NEW COLLECTIVE ACTION REGIME IN THE NETHERLANDS 47, 50-54 (Dennis Horeman & Machteld de Monchy eds. 3rd ed. May 24, 2024), <https://www.debrauw.com/articles/third-edition-of-unlocking-the-wamca>; *Almost 5 Years of Class Actions under the WAMCA: What Is New?*, LOYENS & LOEFF (Sep. 11, 2024), <https://www.loyensloeff.com/insights/news-events/news/almost-5-years-of-class-actions-under-the-wamca-what-is-new/>.

¹⁰⁶*Oracle en Salesforce voor rechter wegens 'onrechtmatige verwerking van persoonsgegevens'*, PRIV. COLLECTIVE (Aug. 14, 2020), <https://theprivacycollective.nl/nieuws/oracle-en-salesforce-voor-rechter-wegens-onrechtmatige-verwerking-van-persoonsgegevens/>; Gerechtshof (Hof) Amsterdam 18 June 2024 JOR 2024, 245 m.nt. DA van der Kooij (The Privacy Collective Foundation/Oracle Nederland BV, et al.) (Neth.).

¹⁰⁷RAD Recitals (12) and (43).

¹⁰⁸*Collective Redress (Class Action)*, CONCURRENCES (dictionary), <https://www.concurrences.com/en/dictionary/collective-redress-class-action> (last visited May 17, 2024).

¹⁰⁹RAD art. 4.

¹¹⁰Case C-456/01, *Henkel v. OHIM*, ECLI:EU:C:2004:258, (Apr. 29, 2004), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=49150&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7151196>.

proceedings in the Member state where the plaintiff lives under Regulation No 44/2001.¹¹¹ That Regulation has been recast by Brussels I bis,¹¹² but the relevant provisions continue to raise the question of whether cross-border actions under RAD would be treated like *Henkel* and able to be brought in a QE's home jurisdiction, or as assigned consumer claims that must be brought in the jurisdiction where the defendant business is based.¹¹³ There is similar uncertainty as to how the GDPR's jurisdiction provisions in Article 79 would be interpreted. Even if courts ultimately find that *Henkel* should be adopted for most claims under RAD, defendant companies will probably argue the questions of cross-border jurisdiction and QEs' standing as delay tactics regardless of merit.¹¹⁴

IV. Uneven Implementation of RAD

The next sections consider RAD mechanisms established in three jurisdictions that illustrate differences in legal systems and approaches—Germany, Portugal, and Ireland.

1. Germany

Germany has implemented RAD via the Law on the Implementation of the Directive on Associations' Complaints, *Verbandsklagenrichtlinienumsetzungsgesetz* [hereinafter VRUG], passed on September 29, 2023. Part of VRUG, the Consumer Rights Enforcement Act (*Verbraucherrechtgedurchsetzungsgesetz*), provides for mass claims for damages, and Germany did not previously have a consumer rights mass claim mechanism for damages. For a claim to be admissible, a QE must "plausibly present" or "reasonably demonstrate" (*nachvollziehbar darlegen*) that at least 50 consumers may be affected.¹¹⁵ Consumers must opt-in by registering before the deadline of three weeks after the end of the oral hearing at first instance.¹¹⁶ Thus, although it is an opt-in mechanism, individual claimants need not be identified prior to commencing proceedings.

2. Portugal

Portugal already had an opt-out mass claims mechanism under Article 52(3) of the Constitution that provides for "Popular Action" (*ações populares*) for citizens to uphold diffuse interests in areas that include public health, consumer rights, and environmental matters.¹¹⁷ Portugal has added Decree-Law 114-A/2023, passed on December 5, 2023, implementing RAD. Portugal already regulated popular actions under Law no. 83/95 of 31 August 1995, which continues to govern cases outside the scope of Decree-Law 114-A/2023. Consistent with the existing approach to popular actions, Decree-Law 114-A/2023 provides for an opt-out procedure under which a QE

¹¹¹Case C-498/16, Maximilian Schrems v. Facebook Ir. Ltd., ECLI:EU:C:2018:37, (Jan. 25, 2018), <https://curia.europa.eu/>.

¹¹²Regulation 1215/2012 of Dec. 12 2012, Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (recast), 2012 O.J. (L 351) (EU).

¹¹³Compare Petra Leupold, *Private International Law and Cross-Border Collective Redress*, BEUC (Aug. 2022), https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-085_Private_International_Law_and_Cross-Border_Collective_Redress.pdf, with Fairgrieve & Salim, *supra* note 8, at 465.

¹¹⁴Fairgrieve & Salim, *supra* note 8, at 473–75.

¹¹⁵*New Class Action – Act on Representative Actions Now in Force*, NOERR (Oct. 13, 2023), <https://www.noerr.com/en/insights/new-class-action-act-on-representative-actions-now-in-force>; *Redress Action in Germany – the New Kid on the Block?*, FRESHFIELDS (Sep. 29, 2023), <https://riskandcompliance.freshfields.com/post/102iowe/redress-action-in-germany-the-new-kid-on-the-block>; see also *FAQs: The New German Representative Class Action*, LINKLATERS (Sep. 29, 2023), https://lpscdn.linklaters.com/knowledge/-/media/digital-marketing-image-library/files/06_ckp/230929-vrug-alert-en.ashx?rev=2459405c-878d-4391-828c-baec0f73d70b&extension=pdf.

¹¹⁶NOERR, *supra* note 115.

¹¹⁷Sandra Jesus & Micaela R. Roque, *The Arrival of Class Actions in Portugal*, CAIADO GUERREIRO (Jan. 2, 2024), <https://www.caiadoguerreiro.com/en/the-arrival-of-class-actions-in-portugal/#:~:text=114%2DA%2F2023%2C%20of,already%20existed%20in%20other%20jurisdictions>.

represents all individuals with claims who do not opt-out from the case before the deadline of the end of the evidence phase.

3. Ireland

On 11 July 2023, Ireland's president signed the Representative Actions for the Protection of the Collective Interests of Consumers Act 2023, implementing RAD.¹¹⁸ Like Germany, Ireland has established an opt-in process, but with an earlier registration deadline of when a court decides a case is admissible. Section 19(11) requires that QEs provide sufficient information about the class of consumers affected by an alleged infringement for the Court to determine admissibility.

4. Will RAD Open the Floodgates for Access to Remedy?

Under RAD there will be representative action mechanisms in all EU member states, providing a state-based judicial mechanism for strategic litigation to benefit many people. Such mechanisms are particularly appropriate for strategic litigation against internet giants because of their diffuse human rights impact, which happens at scale. The existence of representative action mechanisms can remove the access to justice barrier presented by the absence of mechanisms to bring mass claims as was the case in most member states prior to RAD. However, other access to justice barriers remain, particularly procedural requirements for representative actions and questions of jurisdiction in cross-border claims.

Furthermore, RAD has been unevenly implemented by member states,¹¹⁹ potentially reproducing some of the enforcement shortcomings of GDPR, and different procedures will vary in accessibility. For example, opt-out mechanisms are more appealing for commercial litigation funding, and easier to navigate for admissibility.¹²⁰ Some mass claim mechanisms were effectively unusable prior to RAD, and that may be the case for some RAD mechanisms.¹²¹ Different procedural rules and uncertainty over jurisdiction under RAD are likely to pose barriers to cross-border strategic litigation as has been the case for GDPR enforcement. In addition, RAD takes a consumer law framing to private enforcement through mass claims, which may undermine its efficacy for strategic litigation on digital rights where infringements do not produce an easily recognizable consumer harm.

F. Conclusion

The EU aimed to fill a legal lacuna in regulation of the internet audience economy with the DSA and DMA, supplementing existing laws such as GDPR and consumer protection, yet their enforcement architecture may undermine realization of their goal of strengthening internet users' digital rights. The new laws' public enforcement architecture risks legal incoherence because of the increasing number of regulators with overlapping public enforcement mandates that could produce inconsistent or contradictory decisions on internet giants. European Commission competence under the DMA and the DSA could counteract fragmentation, but leaves civil society disempowered and companies empowered to bring strategic litigation that will influence the public enforcement of these new laws.

¹¹⁸Caoimhe Clarkin, Jeremy Sher, Helen O'Connor & Des Cooke, *Consumer Representative Actions in Ireland*, DLA PIPER (Jul. 26, 2023), <https://www.dlapiper.com/en/insights/publications/2023/07/consumer-representative-actions-in-ireland>.

¹¹⁹Visscher & Faure, *supra* note 8, at 470–72; Antonia Hotter & Florian Scholz-Berger, *Organisation and Design of Collective Redress*, in ORGANISATION AND DESIGN OF COLLECTIVE REDRESS: WORKSHOP REPORT, MASS CLAIMS 40, 40–45 (2023).

¹²⁰Augusta Maciuleviciute & Alexandre Biard, *BEUC's Relentless Quest for Collective Redress that Works for Consumers*, BEUC (Nov, 4, 2022), <https://www.beuc.eu/blog/beucs-relentless-quest-for-collective-redress-that-works-for-consumers/>.

¹²¹Biard, *supra* note 8, at 4–5.

Private enforcement strategic litigation could enable legal coherence through judicial decisions that incorporate different areas of law, while empowering civil society to influence development of digital rights. Civil society can incorporate rights and protections from multiple areas of law in private enforcement strategic litigation, advancing digital rights while promoting legal coherence across different areas of law. Strategic litigation against internet giants based on multiple areas of law could be stronger and have more impact—some legal points may succeed even though others fail, and subsequent enforcement of multiple legal regimes following a precedent set by strategic litigation would increase the case's impact. Yet, such cases require greater legal expertise to cover different areas of law, and any private strategic litigation against internet giants involves procedural difficulties such as cross-border jurisdiction or standing.

The possibility of private enforcement strategic litigation against internet giants in different member states itself could result in fragmentation between jurisdictions, and uneven implementation of RAD may hamper cross-border claims. Preliminary references to the CJEU and intervention by the European Commission could avoid fragmentation between member states on digital rights. The CJEU has adjudicated on the relationship between different mechanisms for remedy,¹²² and the fundamental EU law principles of effectiveness and equivalence might lead to some consistency among enforcement mechanisms,¹²³ but only if cases reach the CJEU. Civil society will need considerable resources to gather evidence on internet giants, access wide ranging legal expertise, and navigate procedural complexity for strategic litigation before national courts and the CJEU to advance digital rights in the internet audience economy.

Acknowledgements. This Article benefitted significantly from the workshop organized by Pola Cebulak, Marta Morvillo, and Stefan Salomon, and their comments on earlier drafts, as well as the discussant for my draft Francesca Palmiotto. I also wish to thank colleagues who have provided thoughts and comments on this article and the ideas therein, including Emmanuelle Debouverie, Max Mackay, Jonny McQuitty, Ursula Pachel, Thomas Streinz, Aditi Tripathi, and Peter Wells. My analysis is informed by 10 years of working in non-profits and digital rights, most recently as Director of Litigation and Strategy at global philanthropic organization Luminare. This Article draws on my experience in the field and many conversations with partners and collaborators across NGOs, academic experts, activists, grant-makers, regulators, lawyers, and commercial litigation funders.

Competing Interests. The author declares none.

Funding Statement. There is no specific funding associated with this article.

¹²²Case C-381/14, *Jorge Sales Sinués v. Caixabank SA*, ECLI:EU:C:2016:252, (Apr. 14 2016), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0381>; Case C-73/16, *Pušár v. Finančné riaditeľstvo Slovenskej republiky*, ECLI:EU:C:2017:725, (Sep. 27, 2017), <https://curia.europa.eu/juris/document/document.jsf?text=&docid=195046&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9475199>; Cafaggi, *supra* note 42, at 24–43, 252–54.

¹²³Gentile & Lynskey, *supra* note 2, at 824–25, 827–28.