who was acting in the best interests of the general body of shareholders (at [754], [757]). This is a device with which all shareholder activists will be familiar. Therefore, in practical terms, if a constituent director takes the view that a company's board is managing the business in a way that is not consistent with the shareholder activist's agenda, and has not secured permission to "brief" the shareholder activist sponsor, then she may express dissent at a relevant board meeting, ventilate her views at the general meeting and then resign, in that order (at [419]–[422]). Given that shareholder activist campaigns are predicted to increase in the UK, *Stobart* signals a range of future possibilities: increased litigation due to a clash of legal cultures, a change in shareholder activists' behaviours or, now that the legal expectations placed upon a constituent director are more settled, a proliferation in boardroom activism.

Anna L. Christie and J.S. Liptrap

Addresses for Correspondence: Trinity College, Cambridge, CB2 1TQ, UK; Downing College, Cambridge, CB2 1DQ, UK. Emails: alc200@cam.ac.uk; jsl65@cam.ac.uk

SEARCH ENGINES, GLOBAL INTERNET PUBLICATION AND EUROPEAN DATA PROTECTION: A NEW *VIA MEDIA*?

THE ruling in *Google Spain* (Case C-131/12 (EU:C:2014:317)), which was handed down over five years ago, was undoubtedly a landmark decision on the interface between European data protection and online publication. However, even as regards determination of the duties of Internet search engines to de-index personal data on request, this Grand Chamber judgment only provided the beginnings of the necessary analysis. More recently, in Case C-507/17, *Google v Commission nationale de l'informatique et des libertés* (EU:C:2019:772), another Grand Chamber decision addressed one core issue which immediately arose, namely, specifying within which geographical services a global operator such as Google was mandated to accede to an otherwise valid claim by an individual to de-indexing or, in other words, to the removal of specified personal data from at least name-based searches. This reference arose from Google's appeal against the decision of the French Data Protection Authority (DPA) to fine this company for its failure to ensure such de-indexing on a global basis in all cases, an appeal which was ultimately heard by the French Conseil d'État. Although this DPA intervention was grounded in the former Data Protection Directive (DPD) 95/46/EC (OJ 1995 L 281/31), the Court of Justice ultimately gave even more attention to the current General Data Protection Regulation (GDPR) 2016/679 (OJ 2016 L 119/1). It held that this legislation required Google to adopt measures which had "the effect of preventing or, at the very least seriously discouraging internet users in

the Member States from gaining access to the links in question" (at [70]) through conducting searches which otherwise fell within the scope of the de-indexing right. Beyond this, Member State supervisory and judicial authorities were also empowered to undertake a case-by-case balancing between data protection and freedom of expression "in light of national standards of protection of fundamental rights" and order global de-indexing "where appropriate" (at [72]). Finally, the EU legislature had competence to provide for global de-indexing across the Union if it so chose (at [58]). The judgment has been widely touted as securing a "major victory" (*Washington Post*, 24 September 2019) for Google. Given that the Court of Justice clearly rejected the French DPA's contention that EU law mandated across-the-board global de-indexing, that is somewhat understandable. However, the judgment ultimately seeks to chart a *via media*, thereby giving plenty of scope to further vindicate data protection in ways which Google and others may find troubling. Much will depend, first, on how DPAs and courts interpret the requirement for the adoption of measures which prevent or seriously discourage circumvention of geo-blocking measures and, second, on whether and how these same actors develop criteria and mechanisms for mandating truly extra-territorial de-indexing in individual cases.

The difficulty of reconciling the global nature of information flows with locally situated content rules has been one that has confronted the development of online technology over many decades. Whilst rejecting outright cyberlibertarianism, Google has historically adopted a narrow approach to the application of local content rules other than as directly applicable in California, notwithstanding that it clearly exercises information dominance within many other jurisdictions worldwide. In sum, Google has acceded to specific local obligations only in relation to national versions of its services (e.g. google.fr or google.co.uk). Otherwise, it has carried on supplying such content within the relevant jurisdiction, notably through its google.com service, and even continued to target advertising at users of such content in the usual way. This mode of accommodation was initially applied to de-indexing under *Google Spain* in 2014 but soon attracted the opposition of EU DPAs including as assembled in the pan-European Article 29 Working Party. In particular, the Working Party's *Guidelines on the Implementation of Google Spain* (WP 225) issued in late 2014 held that "limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the judgment" and "[i]n practice, this means that in any case de-listing should also be effective on all relevant domains, including .com" (p. 9). Some DPAs, including not only the UK but even the Spanish, interpreted this to require only that Google ensure through geo-locating Internet Protocol addresses that no "direct" access was possible from within the EU

to any non-redacted service; Google ultimately acceded to this modification of its general approach. However, many others including the French and Italian DPAs drew inspiration in particular from *Google Spain*'s emphasis on ensuring the "effective and complete protection" (at [58]) of data subject rights and held that Google must ensure that de-indexing was effective across all its global services. In March 2016 the French DPA fined Google €100K for failing to ensure this and it was the latter's challenge to this that prompted the French Conseil d'État to issue this reference to the Court of Justice in August 2017.

Advocate General Szpunar issued an Opinion in the case in January 2019 (EU:C:2019:15). Whilst finding that the DPD required a global engine to "take all steps available to him to ensure effective and complete de-referencing" across the EU, the Advocate General rejected as unbalanced the contention that the DPD should require Google to undertake truly global action "in a situation such as that of the present case" (at [62]). Nevertheless, rather cryptically, he also stated that he did "not exclude the possibility that there may be situations in which the interest of the European Union requires the application of the provisions of Directive 95/46 beyond the territory of the European Union" (at [62]). The final judgment in the case, which was issued in September 2019, was broadly consistent with this Opinion (unlike the marked divergence between the Court and Advocate General in the initial *Google Spain* case). Nevertheless, the Court's requirement that the measures taken by Google prevent or at least seriously discourage circumvention of rights within the EU was more precise than the Advocate General's wording. In addition, albeit through reference to national rather than pan-EU protective standards, the Court also provided a concrete reference point for considering when the balance between data protection and freedom of expression may favour extra-territorial action. In further deference to national standards, the Court also refused to rule out the possibility that the justification or otherwise for de-indexing may vary within the Union (at [67]) although it also stressed that (aside from situations of urgency) it would be incumbent on DPAs to establish a consistent pan-EU position under the GDPR (at [68]).

Given its track record to date, it is inevitable that Google will seek to construe the interventionist aspects of this judgment narrowly. In the first place, it is likely to argue that absent a specific national law authorising a DPA to issue extra-EU injunctions, the supervisory authority is powerless to order extra-territorial action. Second, it will almost certainly claim that their current use of so-called 'IP geo-blocking' (which blocks by reference to the user's Internet Protocol address) is sufficiently robust in shielding noncompliant services from the EU itself. Both claims are somewhat dubious. First, given the ready public availability of Virtual Private Networks (VPN), a system based entirely on the location of an IP address would appear inadequate. At the very least, Google should cross-check this with

GPS or other location data which it is collecting and – as companies such as Netflix do already in order to protect their intellectual property rights – adopt measures to block use of commercial VPN services which provide a proxy IP address in order to circumvent geographical control. Second, an examination of the precise case references cited by the judgment make it clear that the Court conceives *any* national implementing measure to be sufficient to trigger national standards. Moreover, notwithstanding the GDPR's please define extensive harmonisation, EU DPAs remain established and empowered under national law and, in another recent case (C-18/18, *Glawischnig-Plesczek*, EU:C:2019:821), the Court has also clarified that nothing within EU or international law *ipso facto* prohibits extra-territorial orders. Therefore, assuming supportive national standards are present, any EU DPA should be able to deploy its standard implementing powers with extra-territorial effect but (assuming geo-location blocking can be made robust) should only do so in exceptional cases, after very careful balancing and subject to challenge in court.

If Google was an entirely EU company then it is clear that data protection would (at least as far as technically possible) have required it to achieve a fully global result in all cases. That this was not necessary here arose from Google having its seat in a third state (at [51]). That goes to show that ultimately this case was primarily about public international law. In that regard, the Court's confirmation that the powerful impact of global communicative networks can trigger extra-territorial jurisdiction under the effects doctrine is of great significance (at [57]). However, the Court also saw this doctrine as one factor amongst many, notably international comity and the impact on fundamental rights, which needed to be balanced. The specific data-protection context requires recognition of both the strong emphasis placed on protecting personality rights within the Union and an analysis of the extent of transnational agreement or otherwise on the particular substantive claim being made in any concrete case. Absent new pan-EU legislation intervention, the Court insisted that such balancing should be carried out by reference to national, rather than EU, standards. In either case, it is manifest that the legal environment within which Internet services operate remains messy. EU DPAs can contribute to greater clarity by insisting on truly robust geo-blocking as a default, promoting greater international consensus on tackling core personality rights violations and enunciating the criteria under which they will entertain extra-territorial remedies against global operators like Google.

David Erdos

Address for Correspondence: Trinity Hall, Cambridge, CB2 1TJ, UK. Email: doe20@cam.ac.uk