Editorial

At the crossroads of data protection and competition law: time to take stock

Orla Lynskey

In March 2014, a report published by the European Data Protection Supervisor (EDPS) kick-started a prescient discussion on the interplay of data protection, competition law, and consumer protection in the digital economy. The EDPS report highlighted topics sitting at the crossroads between these three branches of law and encouraged closer dialogue between experts and regulators across these legal boundaries. Four years on, there have been several significant substantive developments, and we find ourselves at a different crossroads, probing how these changes can be administered.

It is, therefore, a timely exercise to stop and take stock of these developments. This is the rationale for this symposium edition of *International Data Privacy Law* (*IDPL*). Renowned experts on this topic were invited to contribute articles and comments on the substantive alignment of data protection and competition law. The majority of contributions focus on European developments in this area, perhaps unsurprisingly given that this is where this debate has had most traction; yet, the themes discussed are of universal relevance. Indeed, contributions in this and future *IDPL* editions from South Africa, India, and Japan indicate that these debates are necessarily global in nature. Key themes covered in the symposium include legal convergence around the central principle of fairness; how market power in data-intensive services can impact upon the level of data protection offered to individuals; and how behavioural economic research on data privacy, of central importance in the data protection literature, can inform competition law enforcement.

Moreover, as several contributions note, the question is not simply how competition law can render data protection more effective, but also how data protection law can enhance and inform the application of competition law. Yet, as these contributions also note, competition law is not a panacea, and strong data protection law is the first, necessary step to effective digital rights.

Before continuing your reading, it is useful to recall the initial impetus for this discussion. Despite movements such as the Europe-v-Facebook campaign, and limited exceptions such as the 'Google Spain' judgment, the European Union (EU)'s 1995 Data Protection Directive struggled to guarantee the effectiveness of individual's data protection rights vis-à-vis the technology giants they encounter in their day-to-day use of the Internet. Data protection advocates, therefore, turned their attention to the more systemic impediments to individual rights and calls mounted for open social networks and the adoption of a more holistic approach to law and policy in the digital society.

Given that a handful of technology companies are responsible for the architecture of these services, and, thus, exercise de facto control over the quantity of personal data processed and the quality of its processing, a focus on their data processing practices was a good place to start this inquiry. Moreover, as competition law is the only instrument in the legal armour that constrains the exercise of power by private companies, its intersection with data protection laws became an inevitable focal point. In particular, competition authorities have the competence to oversee mergers and acquisitions and to ensure that monopolies do not abuse their market position in a way that excludes equally efficient competitors or exploits consumers. Competition authorities are also endowed with effective enforcement powers, including fines and the enforcement of behavioural remedies. For their part, competition lawyers expressed concern that competition law would be co-opted to achieve non-competition aims, a plausible fear given the open-textured nature of competition rules and its enviable enforcement apparatus.

This initial debate has now, four years later, taken shape with a number of notable developments. From a substantive perspective, the EU Commission has recognized that the level of data protection and privacy offered by a product or service is a potential element of its quality and, therefore, a parameter on which companies can compete or stifle competition. Moreover, the

German Bundeskartellamt's Facebook investigation suggests that data protection law can be used as a normative benchmark to establish whether the conduct of a dominant firm is abusive. At a broader level, debate continues in the EU over whether competition law should be concerned with fairness and, in the USA, over whether America has a 'market power problem' that antitrust should tackle.

Despite these substantive developments, the necessity of incorporating data protection concerns into substantive EU competition law might now be queried following the entry into force of the GDPR. The GDPR offers increased substantive protection (for instance, the potential limitations on 'take-it-or-leave-it' consent in Article 7(4) GDPR) and enhanced enforcement mechanisms (inspired themselves, in part, by competition law). Early indications suggest that these mechanisms can and will be availed of by civil society organizations to ensure full compliance with the data protection rules by technology giants. It is certainly the case that the existence of baseline data protection legislation is a prerequisite for the protection of individual rights online and that, as one of our contributions rightly suggests, the incorporation of data protection into competition law would not obviate the need for such legislation. Yet, equally it may be premature to think that the GDPR (or any data privacy legislation) negates the need for cooperation among data protection, consumer protection, and competition authorities. Where the constituent components of these other areas of law are fulfilled, then their application to a given scenario remains appropriate. This means, for instance, that a dominant firm's terms and conditions might simultaneously violate all three areas of law. Indeed, at present, all three forms of authorities are investigating this possibility. Moreover, whether data protection laws can impose prior restraints on a data-driven merger is an open query, leading to the ongoing discussion of whether the impact of such transactions on data protection and privacy should be considered before the transaction is approved by competition authorities. The GDPR does not preclude or resolve these issues.

At this crossroads, the next move is therefore a practical one: to determine how these rules can be applied when there is substantive overlap between these areas of law. The European Commission's recent warning to Facebook that it will face sanctions from national consumer protection authorities unless it changes its 'misleading' terms of service may raise some eyebrows from national data protection authorities, for instance. Turf wars are inevitable unless a clear division of labour between these authorities is planned. Once again here, the establishment by the EDPS of a 'Digital Clearing House', a voluntary network of enforcement bodies seeking to ensure greater cooperation and coherence between regulators, was a forward-thinking move. Moreover, such a move is likely to be replicated at national level in the EU and in other jurisdictions.

An initial question to be determined is how these cases should be allocated between respective authorities or how cooperation might function in practice. This would be necessary, for example, to ensure that companies do not get conflicting guidance regarding the lawfulness of particular practices from different authorities (for instance, if terms and conditions are simultaneously misleading and lacking transparency). Other open questions include how this process can unfold while respecting rights of the companies concerned (in particular, the principle of *ne bis in idem* and the principle of legality) and how such cooperation can be rendered compatible with the independence of national supervisory authorities. At this crossroad, progress may be stifled and data protection authorities may proceed with caution unless the rules for the road ahead are clear. The development of such clear guidance is therefore the next challenge for interested parties.

doi:10.1093/idpl/ipy023