

# Navigating the right to data portability in the EU GDPR

**Wenlong Li**, winner of PL&B's student essay competition 2019, discusses the right to data portability in the GDPR and its close relation to consumer protection and competition law.

The EU General Data Protection Regulation (GDPR) was introduced at a time when three areas of EU law – data protection, consumer protection and competition – are converging with each other.<sup>1</sup> Each area of law has also introduced new schemes that facilitate data flows. This begs the question as to whether the GDPR recognises and pursues consumer welfare, an overarching value that are also the objectives of both competition and consumer protection law. It is also worth exploring whether the GDPR's right to data portability (RtDP) should be either integrated with or differentiated from other rights.<sup>2</sup> This essay provides an account of EU law's convergence, and looks at how interpretation and implementation of the RtDP may be affected as a result.

## A TRIO OF EU LAW: COMMONALITIES, DIFFERENCES AND CONVERGENCE

The EU rules on data protection, consumer protection and competition are highly interrelated. As the European Data Protection Supervisor (EDPS) puts it, they share the common goals of promoting growth, innovation and the welfare of individual consumers.<sup>3</sup>

At granular levels, however, these rules markedly differ from each other. The most explicit difference lies in the disparate legal bases in the Treaty of the Functioning of the European Union (TFEU). Competition law lies in the centre of EU law and there are numerous Articles facilitating competition.<sup>4</sup> Further, Art 12 and Art 169 jointly require “a high level of consumer protection”.<sup>5</sup> After the Lisbon Treaty,<sup>6</sup> the EU no longer has to rely upon the market integration rationale to protect personal data. Art 16 TFEU now serves as the basis for legislating on data protection.<sup>7</sup> The EU Charter of Fundamental Rights offers additional normative support. Whereas Art 8 introduces

a new fundamental right to data protection,<sup>8</sup> Art 38 requires that Member States shall “ensure a high level of consumer protection”.<sup>9</sup>

Apart from the legal bases, the three areas of law also diverge on their regulatory targets. As Averitt and Lande argue, whereas antitrust law “[ensures] the marketplace remains competitive so that a meaningful range of options is made available”, consumer protection law makes it easier for consumers to “choose effectively”.<sup>10</sup> Similarly, Albers-Llorens contends that competition law addresses “external market failures which may reduce the number or quality of the options” whereas consumer law deals with market failures “internal to consumers, preventing them from making rational choices”.<sup>11</sup>

Data protection law does not squarely fit into this schema. This law may constitute a response to market failure<sup>12</sup>, but never recognises consumer welfare as a goal to be pursued. Conventionally, data protection law is concerned with the aspect of individual welfare relating to dignity.<sup>13</sup> In the GDPR-era, however, this dignity-based perception may be subject to revision. The RtDP now allows data subjects to reuse their personal data for benefits, and part of the GDPR should be hence associated with the economic wellbeing of individuals.

In sum, three areas of law appear to contribute to their shared goal(s) in distinct ways. These differences noted between them also affect the extent to which they can bleed into each other.

## THE CONVERGENCE OF EU LAW

In March 2014, the EDPS took the lead to explore the synergies between these rules. In several opinions, he expresses that a holistic approach to implementing EU rules is feasible.<sup>14</sup> The interplay between EU rules has also been noted in the academic literature. Albers-Llorens notes that consumer protection and competition

law are “theoretically and formally independent but linked by connections and mutual influences”.<sup>15</sup> Costa-Cabral and Lynskey argue that data protection and competition law are members of the EU law family and have “significant family ties”.<sup>16</sup> The complementary relationship between consumer protection and data protection law is expressed by Helberger and others, who propose an integrated vision on “data consumer law”.<sup>17</sup> The interfaces between each of the two areas will be examined in turn.

First, competition and consumer protection law are mutually complementary in the EU. As Albers-Llorens argues, they are “bonded together by an overarching theme of consumer welfare” but “essentially maintain their own objectives and sphere of application”.<sup>18</sup> It is contested, however, to what extent consumer welfare can be seen as a goal of EU competition law. Whereas the Court of Justice of the European Union (CJEU) has been reluctant to recognise it in its judgments<sup>19</sup>, the Commission explicitly acknowledges that competition law addresses the adverse impact on consumer welfare.<sup>20</sup>

Second, the EDPS has proposed a form of convergence between competition and data protection law. In his 2014 Opinion, the EDPS argues that privacy and data protection should be considered in the appraisal of companies' activities and their impact on competitiveness.<sup>21</sup> These considerations are “not as peripheral concerns but rather as central factors”.<sup>22</sup> In so doing, competition law may “promote privacy-enhancing services” on the one hand, and “greater consumer control over their own data” on the other.<sup>23</sup> *Bundeskartellamt*, the German Federal Cartel Office, is the first authority in the EU legal order to set a precedent in this respect. An investigation into Facebook's “limitlessly amassing of data” was initiated in 2016, the results of

which were released in January 2019.<sup>24</sup> Interestingly, the *Bundeskartellamt* found Facebook abusing its dominant position with reference to data protection rules. It concluded that “an obligatory tick in the box is not an adequate basis for intensive data processing.”<sup>25</sup> In addressing data protection issues, the *Bundeskartellamt* states that it is in close cooperation with the leading data protection authorities.<sup>26</sup>

Third, consumer protection law is also expanding in the digital age. Traditionally, consumer protection confines itself to transactions characteristically in exchange for money. In the digital economy, the fact that many services are marketed as “free” has raised serious concerns. In those cases, a price is paid not in the form of money, but by the disclosure of personal information. Against this backdrop, a modernisation of EU consumer protection law was initiated in 2015, and the proposed Digital Content Directive (DCD) aimed to extend consumer protection to new forms of transactions.<sup>27</sup> The Explanatory Memorandum states that it covers all types of “digital content”, including those “in exchange for data provided by consumers.”<sup>28</sup> The DCD has been recently finalised, and a number of its components are highly interconnected with the GDPR.<sup>29</sup> For instance, recital 39 of the Directive states that the GDPR right to erasure and the consumer’s right to withdraw consent should apply fully in connection with the contracts covered by this Directive.<sup>30</sup> Further, the right to terminate a contract concerning the supply of digital content or digital services entails a right to data portability upon the termination of the contract.<sup>31</sup> As will be detailed in the next section, this new right is devised to complement Art 20 GDPR, and should hence be used together in practice.

#### DATA PORTABILITY RIGHTS : AN EVOLVING LANDSCAPE

The nature of the RtDP has been highly contested. Many member states were concerned that the RtDP “touched upon issues more properly regulated in competition and consumer protection law” and that “coherence had to be maintained with those fields.”<sup>32</sup> Several competition law scholars were keen on examining the

RtDP from a competition law perspective. For instance, Engels argues that the RtDP should be restrictively interpreted and implemented “in a nuanced fashion in order to avoid [an] adverse effect on competition and innovation.”<sup>33</sup> Similarly, Grief and others suggest that the RtDP’s scope of application be confined to the market of social networks.<sup>34</sup> Vanberg and Ünver contend that the RtDP’s “adverse consequences particularly for SMEs’ can be alleviated by drawing lessons from EU competition law.”<sup>35</sup>

Data portability has also been framed as a consumer remedy to lock-in, the practice that businesses adopt strategies or technical measures to make consumers or users more dependent on the service concerned. For instance, the Article 29 Working Party (A29WP) implies in its Guidelines that the right, which supports choice, control, and empowerment, “provides consumer empowerment by preventing lock-in.”<sup>36</sup> In response to the A29WP’s public consultation, numerous participants agree that the RtDP is confined to a consumer-business relationship in the private sector because, as per Art 20(1) GDPR, it applies only to data processing legitimised on the grounds of consent or contract.<sup>37</sup>

In the A29WP’s public consultation, numerous responses pointed to the fact that the interpretation of the GDPR right to data portability had been affected by “political discussions on data portability expressed in the ongoing debate.”<sup>38</sup> At that time, the portability of digital content was being reviewed by EU legislative bodies, and the Commission was proposing the porting of non-personal data as a building block of the European data economy.<sup>39</sup> As data portability is believed to have a role in facilitating switching and alleviating lock-in, attempts have been made, in both authorities’ opinions and scholarly literature, to align the GDPR right to data portability with the logic of competition or consumer protection.

The last part of this essay compares the RtDP with similar schemes introduced recently. Against the prevailing view mentioned above, it is argued that the RtDP itself is unable to facilitate

competition or address lock-in due to the limited scope of the data concerned. However, new schemes are devised in a way that complements the GDPR, thereby encouraging the implementation of data portability schemes in a holistic manner.

To start with, the RtDP applies only to “personal data concerning the data subject, which he or she has provided to a controller.”<sup>40</sup> This scope can be further restricted by technical measures such as anonymisation, pseudonymisation and encryption. Anonymisation generally refers to the technique that removes personally identifiable information from certain datasets. Another attenuated technique for identity removal is pseudonymisation. According to Art 4(5), pseudonymisation is a technique that “makes data no longer attributable to a data subject without the use of additional information.”<sup>41</sup> Hence, whereas anonymisation in theory irreversibly prevents identification, pseudonymisation only makes data temporarily unattributable. Encryption is a technique not for de-identification but can be used to restrict the scope of personal data. As per Art 34(3)(a), it is defined as a protection measure that “render the personal data unintelligible to any person who is not authorised to access it.”<sup>42</sup> Encryption would render it difficult to “tie-back personal data to data subjects on demand” thereby affecting the implementation of subject rights.<sup>43</sup>

While anonymous data is completely outside the scope of the GDPR, it is contested whether the RtDP applies to pseudonymous data. The A29WP implies that it falls within the scope of Art 20, as pseudonymous data “can be clearly linked to a data subject.”<sup>44</sup> In practice, encryption techniques are also used to prevent others from decrypting the data. For instance, Apple uses end-to-end encryption to protect iMessage and FaceTime Conversations, and it claims that “there is no way for us to decrypt your data when it is in transit between devices.”<sup>45</sup> In its ‘Commitment to Consumer Privacy,’ Apple argues that it does not provide certain categories of data to either law enforcement or any other group because “no one but the sender and receiver can see or read them.”<sup>46</sup>

By conforming to identifiability,

the RtDP is not helpful to support data reuse and is thereby unable to promote competition or consumer welfare. In this context, data reusability appears to be a more pertinent quality than identifiability. To achieve the goals such as switching or supplying a functionally equivalent service, the data to be ported should be not just concerning data subjects, but useful for competitors. The latter case requires, for instance, sufficient amount of metadata to be provided to support data reuse in a new IT environment. The GDPR's focus on the identifiability of a natural person arguably discourages the inclusion of useful data and other information (e.g. metadata) in the scope of Art 20 GDPR. The RtDP itself is therefore incapable of facilitating switching or freeing consumers from lock-in. By allowing for the porting of just one copy of personal data, the right appears not to be a tool for switching but multi-homing (that is, using numerous services of complementary or equivalent functionality at the same time).

To remedy this, the A29WP has ostensibly attempted to overstretch Art 20(1) beyond its literal meaning.<sup>47</sup> Its Guidelines suggest that the data provided by the data subject includes:

- Data actively and knowingly

provided by the data subject; and

- Data provided by the data subject by virtue of the use of the service or the device (known as observed data).

By introducing a complementary scheme, the DCD has now provided a solution to the dilemma once encountered by the A29WP (now the European Data Protection Board). The portability of digital content is prescribed in the DCD that complements well the GDPR, thereby suggesting the combined use of EU rules for consumer welfare. When enforced holistically, the consumer may potentially port all data necessary for switching. With the new Directive in place, it is now unnecessary to overstretch the GDPR provisions to tackle lock-in. It is suggested that the new European Data Protection Board should refine the A29WP Guidelines in accordance with recent developments in the EU when possible.

## CONCLUSION

In a time when EU rules incrementally converge, it is necessary to navigate the RtDP by its unique associations with data protection. This essay examines this right at the intersection of EU law and reflects upon its essence and

externalities. To maintain the coherence of EU law, the RtDP should be clearly differentiated from the consumer right to digital content portability, as well as the porting of data facilitated in the Free Flow of Non-Personal Data (FFNPD) framework. While there are many similarities between these schemes, the RtDP has a much narrower scope of data concerned, which has a considerable impact on the right's capacity to facilitate competition or safeguard consumer welfare. It is argued that this right, with its unique objectives and pursuits, should neither be restricted by the logic of competition law nor be overstretched to protect consumers from lock-in. That said, the RtDP should not be viewed in isolation; both the DCD and FFNPD are supplementary to the GDPR, thereby enabling use cases of data portability beyond data protection.

## AUTHOR

Wenlong Li is a PhD Candidate/Tutor at the Faculty of Law, University of Edinburgh, Scotland.

## REFERENCES

- 1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.
- 2 GDPR, Art 20.
- 3 European Data Protection Supervisor, 'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (Preliminary Opinion, March 2014) 3.
- 4 TFEU, Arts 101-109.
- 5 TFEU Arts 12 and 169.
- 6 Roberta Panizza, 'The Treaty of Lisbon' (Fact Sheets on the European Union, October 2018) available at [www.europarl.europa.eu/factsheets/en/sheet/5/the-treaty-of-lisbon](http://www.europarl.europa.eu/factsheets/en/sheet/5/the-treaty-of-lisbon) accessed 26 June 2019.
- 7 TFEU, Art 16(1).
- 8 Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, Arts 7-8.
- 9 EU Charter of Fundamental Rights, Art 38.
- 10 Neil Averitt and Robert Lande, 'Consumer Sovereignty: A Unified Theory of Antitrust and Consumer Protection Law' (1997) 65(3) *Antitrust Law Journal* 713, 713-4.
- 11 Albertina Albors-Llorens, 'Competition and Consumer Law in the European Union: Evolution and Convergence' (2014) 33(1) *Yearbook of European Law* 163, 163-4.
- 12 Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection' (2016) 11(11) *Journal of Intellectual Property Law & Practice* 856.
- 13 Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 91-105.
- 14 European Data Protection Supervisor (n 3) 3. European Data Protection Supervisor, 'Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data' (Opinion 8/2016, 23 September 2016) 16.
- 15 Albors-Llorens (n 10) 164.
- 16 Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2017) 54 *Common Market Law Review* 11, 14.
- 17 Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54 *Common Market Law Review* 1427, 1427.
- 18 Albors-Llorens (n 11) 164.
- 19 Pinar Akman, '“Consumer welfare” and Article 82EC: Practice and Rhetoric' (2009) 32 *World Competition Law and Economics Review* 71.
- 20 European Commission, Communication from the Commission — Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings OJ C 45, 24.2.2009, Art 19.
- 21 EDPS (n 3) 26.
- 22 *ibid.*
- 23 *ibid.*
- 24 Bundeskartellamt, 'Bundeskartellamt

## REFERENCES

- prohibits Facebook from combining user data from different sources' (Bundeskartellamt News, 7 February 2019) available at [www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07\\_02\\_2019\\_Facebook.html](http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html) accessed 7 May 2019.
- 25 *ibid.*
- 26 *ibid.*
- 27 Proposal for A Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content, COM(2015) 634 final.
- 28 *ibid* 11.
- 29 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services, OJ L 136, 22.5.2019, p. 1–27.
- 30 Digital Content Directive, recital 39.
- 31 Digital Content Directive, Art 16(4).
- 32 Application for access to documents - Ref GestDem No 2018/6570, internal report (Ares(2019)693034, 11-12 July 2012), internal message (Ares(2019)693298, 13 March 2013), internal message (Ares(2019)693122, 9-11 April 2013).
- 33 Barbara Engels, 'Data Portability among Online Platforms' 5(2) Internet Policy Review 1, 10.
- 34 Graef and others, 'Putting the Right to Data Portability into A Competition Law Perspective' (2013) Law Journal of the Higher School of Economics 53, 60-1.
- 35 Aysem Diker Vanberg and Mehmet Bilal Ünver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?' (2017) 8(1) European Journal of Law and Technology 1, 1.
- 36 Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (WP242, Rev.01, 5 April 2017) 3-5.
- 37 Application for Access to Documents - Ref GestDem No 2018/1669. GDPR, Art 20(1), cf. Art 6.
- 38 Application for Access to Documents - Ref GestDem No 2018/1669, Syndicat National de la Communication Directe.
- 39 European Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 'Building A European Data Economy', 10.1.2017, COM(2017) 9 final, p.4-5.
- 40 GDPR, Art 20(1).
- 41 GDPR, Art 4(5).
- 42 GDPR, Art 34(3)(a).
- 43 Application for Access to Documents - Ref GestDem No 2018/1669, Digital Europe.
- 44 A29WP (n 36) 9.
- 45 Apple, 'This is How We Protect Your Privacy' available at [www.apple.com/uk/privacy/approach-to-privacy/](http://www.apple.com/uk/privacy/approach-to-privacy/) accessed 8 May 2019.
- 46 'Apple's Commitment to Customer Privacy' (16 June 2013) available at [www.apple.com/apples-commitment-to-customer-privacy](http://www.apple.com/apples-commitment-to-customer-privacy) accessed 2 August 2018.
- 47 A29WP (n 36) 9-10.

# Join the Privacy Laws & Business community

## Six issues published annually

### PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 125+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

### Included in your subscription:

#### 1. Online search functionality

Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

#### 2. Electronic Access

We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

#### 3. E-Mail Updates

E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

#### 4. Back Issues

Access all the *PL&B International Report* back issues since 1987.

#### 5. Special Reports

Access *PL&B* special reports on Data Privacy Laws in 125+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

#### 6. Events Documentation

Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

#### 7. Helpline Enquiry Service

Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

**To Subscribe: [www.privacylaws.com/subscribe](http://www.privacylaws.com/subscribe)**

“*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**”

## Subscription Fees

### Single User Access

*International Reports* £560 + VAT\*

*UK Reports* £450 + VAT\*

*UK & International Reports* £900 + VAT\*

\* VAT only applies to UK based subscribers

### Multi User Access

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

### Subscription Discounts

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

### International Postage (outside UK):

Individual International or UK Edition

Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions

Rest of Europe = £50, Outside Europe = £70

## Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

*Privacy Laws & Business* also publishes the United Kingdom Report.

[www.privacylaws.com/UK](http://www.privacylaws.com/UK)