From Intellectual Property (Data-Related) Disputes to Data Disputes: Towards the Creation of a Global Dispute Resolution Ecosystem for Data Disputes in the Digital Era.

Jacques de Werra

Available at: https://works.bepress.com/jacques-dewerra/21/
Resolving IP Disputes

A Selection of Contemporary Issues

edited by

Gerold Zeiler

Alexander Zojer

zeiler.partners

NWV

Vienna · Graz 2018
Jacques DE WERRA

From Intellectual Property (Data-Related) Disputes to Data Disputes: Towards the Creation of a Global Dispute Resolution Ecosystem for Data Disputes in the Digital Era

Table of Contents
I. Introduction .................................................................................. 87
II. Complexity of IP Disputes: Impact of Bilateral IP (contractual) Disputes on Third Parties ..................... 88
III. From IP Data-Driven Disputes to Data Disputes .......... 92
    A. Data Portability Disputes ................................................. 93
    B. Privacy Shield Disputes ................................................. 98
    C. Disputes about Online Intermediation Services .... 101
IV. Conclusion .................................................................................. 106

I. Introduction
The globality of many business activities and the growth of online transactions which frequently relate to the use of intellectual property (IP) assets have the consequence that IP disputes are very frequently transnational disputes. IP disputes also tend to become quite complex and to involve multiple parties. This is particularly the case for contract-related IP disputes. As reflected in this statement of a practising IP lawyer, “[t]here is a trend away from one off licensing of A to B, and towards multi-party know-how and IP arrangements in the context of bigger projects.”¹ The growing complexity of IP transactions logically

¹ IP lawyer, France, in: Results of the WIPO Arbitration and Mediation

87
translate into the corresponding complexity of the disputes that arise out of these transactions. This can particularly mean that one may have to take into account the position of third parties in such disputes, which will be discussed below in the light of selected case scenarios (see II below). These scenarios show that many of these disputes are about data (access and use) and can thus be considered as IP data-related disputes. Beyond these IP data-related disputes, this paper will also present selected facets of what can be called “data disputes”, that are disputes about (personal or non-personal) data and disputes with Internet platforms in view of the growing importance and of the connections that they have with traditional IP disputes (see III below). The paper will conclude by sharing a few comments and perspectives about IP disputes and data disputes and will expose the need to create a new global dispute resolution ecosystem for solving data disputes in the digital era (see IV below).

II. Complexity of IP Disputes: Impact of Bilateral IP (contractual) Disputes on Third Parties

Even if IP disputes originate from bilateral IP agreements (frequently international IP licensing agreements), it is not infrequent that third parties are directly or indirectly affected by such bilateral IP disputes and that courts and arbitral tribunals have to consider the position of third parties in deciding bilateral disputes.

This can occur in various circumstances. The first scenario relates to sublicensing which constitutes an example of the general contractual law question of chain of contracts. In the

---


2 The specific circumstances / cases that are (briefly) described here do not claim to be exhaustive. There are many additional circumstances in which the position and interests of third parties must be considered in bilateral IP disputes; this paper will not discuss at all the legal issues that arise in FRAND licensing, it being indicated here that FRAND licensing also raises challenging legal questions including about the effect of the FRAND commitments on third parties (which can potentially qualify as a contract with third party beneficiaries).
dispute between the (initial) licensor (and IP owner) and its licensee, the issue may for instance arise as to the obligation of the licensee to report to the licensor on the revenues generated by the licensee resulting from the commercialisation of the IP assets by its sublicensees. This may be complex in situations in which the sublicensing transaction is structured in a way that the licensee does not get royalties from the sublicensee but obtains instead another type of financial participation such as an equity participation in the sublicensee’s company. The issue thus arises (of course subject to the interpretation of the relevant agreement) to define the scope of the reporting obligations of the licensee.

A second scenario can arise when the exclusive licensee initiates infringement proceedings against a third party on the basis of its exclusive license. The question as to whether the exclusive licensee has such right is complex in an international setting.3 This case perfectly illustrates the point that, in the bilateral dispute between the exclusive licensee and the third party (allegedly infringing on the licensed IP rights), the position of the licensor (which is not necessarily a party in the proceedings)4 has to be considered. One issue is to define by interpretation of the license agreement the nature and scope of the rights granted to the exclusive licensee and to decide on the basis of the relevant governing law(s) whether the exclusive licensee has standing to sue for infringement.

A third scenario relates to potential conflicting contractual obligations assumed by a licensee as a result of diverging contractual obligations entered into with different licensors. A licensee, who would have obtained the right to manufacture products incorporating licensor’s IP assets (licensor A), may indeed be facing conflicting contractual obligations: an obligation to report on its royalty bearing activities to licensor A (e.g. number and type of products manufactured under the license) and an obligation of confidentiality on all of its activities to the licensor of another technology which is also integrated in its products (licensor B). The relevant licensing agreements should ideally have duly addressed this, which may however not be the case. This may

---


4 Depending on the local law.
become even more complex when the licensing agreements themselves (specifically the licensing agreement entered into with licensor B) is itself subject to confidentiality (i.e. the content of the licensing agreement cannot be disclosed by the licensee to any third party – thus including to licensor A).

A fourth scenario relates to the transfer of the licensed IP rights (e.g. patents) to a third party. A tricky question in this context is to assess whether and in the affirmative under what conditions the license can “follow the patents”. This is particularly complex in an international setting in which the parties are located in different countries and in which the IP portfolio that is transferred is composed of rights that are registered in multiple jurisdictions. These international elements can lead (under private international law) to the application of different laws and rules depending on the jurisdiction at issue. One element that can have an impact in this context is the registration of the license in the relevant patent registries. Even though local rules may diverge, it is frequent that the registration of the license in an IP registry will make the license opposable to third parties, including to the subsequent acquirer of the IP rights (patents). This question may arise for instance in the course of infringement proceedings initiated by the acquirer of the patent portfolio against the licensee: will the licensee be in a position to claim that it shall still benefit from the license in spite of / after the transfer of the patent portfolio. This can (here again) become even more complex when the license agreement is submitted to an extensive obligation of confidentiality.

A fifth scenario can arise in cases in which the disputed license agreement grants certain rights and benefits to third parties, specifically to licensee’s clients and distributors. This issue is of key relevance in many disputes where the IP owner may challenge the legality of the downstream use and the commercialization of the products by third parties. This can raise the question of the exhaustion of the licensed IP rights as well as the question of the potential impact of a contract with third party

---

5 The contract law governing the license agreement will generally not be considered to govern the issue whether the license agreement is opposable to third parties.


7 For a recent case, see Autodesk, Inc. v Joseph Alter, et al., Case No. 16-cv-04722-WHO, United States District Court, N.D. California (15 May 2018) 2018 WL 1335858.
A sixth scenario in which third parties can be affected by bilateral IP disputes relates to the case of the disclosure of confidential information (which would be prohibited under the disputed non-disclosure agreement) to such third party. In this scenario, the claimant (disclosing party) would claim that its contracting party (the receiving party) would have unduly disclosed confidential information to a third party which would in turn have allegedly benefitted from such disclosure and would have used such information in its own business activities (and integrated in its own product lines).

What can we learn from these (non-exhaustive) examples? The lessons learnt are (at least) twofold: first, even if IP disputes frequently arise in a bilateral context (specifically in the course of bilateral IP contract litigation or arbitration), such disputes also quite frequently impact third parties whose rights and interests can be affected. This consequently means that it is essential to view IP disputes and specifically IP licensing disputes in their entire ecosystem by adopting a global approach which shall not (too) narrowly focus on the bilateral relationships between licensor and licensee.

Second, many of these disputes constitute IP data-related disputes. What is indeed at the core of many of these disputes is access to data and/or use of data (e.g. access to royalty data or use & sharing of confidential data). From this perspective, these IP data-related disputes are relevant because they prefigure

---

8 By way of example, under California contract law, a "contract, made expressly for the benefit of a third party, may be enforced by him at any time before the parties thereto rescind it." Cal. Civ. Code § 1559. Based on case law, "[a] third party qualifies as a beneficiary under a contract if the parties intended to benefit the third party and the terms of the contract make that intent evident." Karo v San Diego Symphony Orchestra Ass'n, 762 F.2d 819, 821–22 (9th Cir. 1985); under New York contract law, an intended beneficiary may enforce a contract, but it bears the burden of proving its status as an intended third-party beneficiary, Port Chester Elec. Constr. Corp. v Atlas, 40 N.Y.2d 652, 389 N.Y.S.2d 327, 357 N.E.2d 983, 985–86 (1976). To prove it is an intended beneficiary, a party must show (1) the existence of a valid contract, (2) that the contract was intended for its benefit, and (3) that the benefit is sufficiently immediate, rather than incidental, to indicate the assumption by the contracting parties of a duty to compensate the intended beneficiary. Burns Jackson Miller Summit & Spitzer v Lindner, 59 N.Y.2d 314, 464 N.Y.S.2d 712, 451 N.E.2d 459, 469 (1983).
Jacques DE WERRA

the types of data disputes that are likely to arise as a result of various regulatory instruments and legal developments (specifically in Europe) that will be presented below (see III below). These types of IP disputes are also relevant to the extent that IP issues may also arise in data disputes. This can particularly happen for the right of access to personal data under the General Data Protection Regulation (GDPR)\(^9\) that may conflict with third party intellectual property rights (trade secrets and copyrights).\(^10\) IP data-related disputes and specifically disputes about the conditions of access and/or use of (confidential) data held by third parties could thus be an important source of guidance in non-IP related data disputes.

### III. From IP Data-Driven Disputes to Data Disputes

Moving beyond IP data-related disputes, we are in an era (also as a result of the GDPR) in which data has clearly become a key element of many online activities for both individuals and companies and about which disputes are most likely to arise. This has already caused an emergence of disputes and the creation of dedicated dispute resolution mechanisms that are distinct from IP disputes and from IP dispute resolution mechanisms, but are rather data disputes in the sense that such disputes essentially deal with access to and/or use of data. It is most likely that we will observe a growth of such data disputes about the GDPR as well as about regulatory instruments (as will be exposed below).

In this context, we are also witnessing the emergence of dedicated dispute resolution mechanisms (which include alternative dispute resolution) that are designed to apply to these data disputes. It is important to emphasize for the sake of clarity that

---


\(^10\) Recital 63 GDPR: “Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software”.

---
the focus shall be here on disputes about data, i.e. where data is the object of the dispute. This must be distinguished from the use of data-based technological tools and other IT technologies (including big data, artificial intelligence, machine learning, etc.) for managing dispute resolution processes (specifically arbitration), that shall not be discussed here. The focus shall thus be on disputes about data (access, use, portability), i.e. where data is the object of the dispute, and not on the use of data-related tools in dispute resolution (where data is a tool/resource in the dispute resolution process).

In that respect, it is important to stress that ADR and specifically arbitration appear particularly well suited for solving technology disputes, which also applies to data disputes, as will be developed below.

The non-exhaustive areas of data disputes and of data dispute resolution mechanisms on which we will focus here are:

A. Data Portability Disputes

The portability of data is a major issue in the on-line digital environment. On-line activities most frequently imply that clients (be they individuals or business clients) store their personal or non-personal data on data storage infrastructures made available by information service providers. Clients should in this respect have the opportunity to use another service provider and thus to transfer/migrate/port their data from their previous service provider to the new one without being hindered in this process.


12 See Vannieuwenhuysse (2018) 127 (with respect to smart contracts, as an emerging field for arbitration: “[…] the long-hailed advantages of arbitration make it a natural dispute resolution choice for conflicts arising out of the use of new technologies and artificial intelligence. […]. Because smart contracts are an emerging practice, disputes arising from their interpretation and enforcement will benefit from international arbitration’s high degree of detachment from national jurisdictions, its flexibility, and its streamlined enforcement”).
Different regulatory instruments facilitate the smooth migration and portability of data for the benefit of the clients by granting them certain rights to the portability of their data which depend on the type of data at issue and distinguish between non-personal data and personal data.

For non-personal data, a proposal for a regulation on a framework for the free flow of non-personal data in the European Union was published on September 13, 2017 (hereafter: “the European Non-Personal Data Regulation Proposal”). The European Non-Personal Data Regulation Proposal acknowledges that “data mobility in the Union is also inhibited by private restrictions: legal, contractual and technical issues hindering or preventing users of data storage or other processing services from porting their data from one service provider to another or back to their own IT systems, not least upon termination of their contract with a service provider.”

The European Non-Personal Data Regulation Proposal further recognizes that “[t]he ability to port data without hindrance is a key facilitator of user choice and effective competition on markets for data storage or other processing services”. It further indicates that “professional users should be able to make informed choices and easily compare the individual components of various data storage or other processing services offered in the internal market, including as to the contractual conditions of porting data upon the termination of a contract”.

On that basis, the European Non-Personal Data Regulation Proposal provides (in Article 6 entitled Porting of data) that “[t]he Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level, in order to define guidelines on best practices in facilitating the switching of providers and to ensure that they provide professional users with sufficiently detailed, clear and transparent information before a contract for data storage and processing is concluded, as regards the following issues: (a) the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another provider or port data back to its own IT systems, including the processes and location of any data back-up, the available data formats and supports, the required IT configuration and minimum network bandwidth;”

---

14 Recital 5.
15 Recital 20.
16 Recital 21.
the time required prior to initiating the porting process and the
time during which the data will remain available for porting; and
the guarantees for accessing data in the case of the bankruptcy
of the provider; and (b) the operational requirements to switch
or port data in a structured, commonly used and machine-
readable format allowing sufficient time for the user to switch or
port the data”.

Pursuant to Article 6(2), “[t]he Commission shall encourage
providers to effectively implement the codes of conduct referred
to in paragraph 1 within one year after the start of application of
this Regulation” and it (paragraph 3) “shall review the develop-
ment and effective implementation of such codes of conduct and
the effective provision of information by providers no later than
two years after the start of application of this Regulation” with a
mandate given to the Commission to “review the situation”17 “if
such codes of conduct are not put in place and effectively
implemented within a reasonable period of time”.18

Interestingly, the European Non-Personal Data Regulation
Proposal does not impose or even propose any dispute resolution
mechanism in case the data cannot be migrated from one pro-
vider to another. This is surprising because it can be expected
that such disputes may arise relatively frequently between clients
and their providers of IT services. The proposal rather relies on
the market and on self-regulation mechanisms (i.e. codes of
conduct) to ensure that clients can effectively benefit from the
mobility of their data.

Turning to data portability of personal data, Article 20(1)
GDPR provides that “[t]he data subject shall have the right to
receive the personal data concerning him or her, which he or she
has provided to a controller, in a structured, commonly used and
machine-readable format and have the right to transmit those
data to another controller without hindrance from the controller
to which the personal data have been provided, where: […]”.
This provision confirms the existence of an enforceable right of
individuals (data subjects) whose personal data are processed
to obtain the portability of their data “without hindrance”.19

17  Recital 21.
18  Ibid.
19  For an analysis of the right to data portability, see Paul De Hert/
Vagelis Papakonstantinou/Gianclaudio Malgieri/Laurent Beslay/
Ignacio Sanchez, The right to data portability in the GDPR: Towards
user-centric interoperability of digital services, Computer Law &
Security Review, Volume 34, 2 (2018) 193-203; Barbara Van der
Article 20(2) GDPR further provides that “[i]n exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible”. Article 20(4) GDPR also provides that “[t]he right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others”.

These reference to third parties and specifically to the new controller show that bilateral disputes may also involve the interests and positions of third parties (which is a point that was similarly made above with respect to traditional IP disputes, see II above).

It is likely that a flurry of disputes will arise about the exercise of this right. Its enforceability will be governed by the relevant provisions of the GDPR. The data subject shall first make a request for data portability to the controller. Based on Article 12(3) GDPR, “[t]he controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request”. Article 12(4) GDPR further provides that “[i]f the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy”. Based on Article 77(1) GDPR, the right of the data subject to

---


20 The controller must inform the data subjects about the existence of their right to data portability (Article 13(2)(b) and Article 14(2)(c) GDPR) — along with information about the other rights of the data subjects.

21 This provision does not seem to cover the case in which the controller would react positively to the request to data portability but would not do so in a satisfactory way from the standpoint of the data subject. In such a case, it seems reasonable to admit that the data subject shall also have the right to initiate legal action against the controller.
lodge a complaint with a supervisory authority is "without prejudice to any other administrative or judicial remedy". With respect to judicial remedy, Article (1) GDPR provides that "without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation". It can be assumed that disputes about the right to data portability under Article 20 GDPR shall fall under this provision, even though it may be uncertain, based on the wording of Article 79(1) GDPR, that the right to data portability under Article 20 is infringed "as a result of the processing of his or her personal data in non-compliance with this Regulation".

In any event, it is interesting to point out that Article 79(1) GDPR expressly reserves "any non-judicial remedy", thereby showing the potential importance of this type of remedy for enforcing the rights of data subjects under the GDPR. In this respect, Article 40(1) GDPR encourages "the drawing up of codes of conduct intended to contribute to the proper application of this Regulation", by providing more specifically that (Article 40(2) GDPR) "associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or

22 Pursuant to Art. 79(2) GDPR, "proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers".

23 Unless it shall be considered that the actions that are accomplished or not accomplished (because the data subject may frequently complain about the inactivity of the controller who will not make the data available for portability) by the data controller with the view to prepare and facilitate the data portability to another controller amount to "processing" within the meaning of Article 2(2) GDPR. Article 2(2) GDPR defines processing as "operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".
amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: [...] (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79”.

It may be uncertain (similarly to what was noted above with respect to the wording of Article 79(1) GDPR) that Article 40(2)(k) GDPR (based on its wording) covers disputes about the right to data portability (unless the actions — or the inactivity — of the controller with respect to the portability of data to another controller amount to processing of data). In any case, it seems important to contemplate the use of alternative dispute resolution mechanisms that could help ensure the effective enforceability of the right to data portability and that could also reduce the caseload that may affect or even paralyze both administrative (i.e. supervisory authority) and judicial bodies if they were to be massively seized with numerous requests of data portability. As this is the case for many other data disputes in the online environment, traditional court proceedings are unlikely to constitute an adequate solution because of the high cost and length of such proceedings.

In a data-driven and data-based online environment in which data mobility should be promoted, disputes about data portability are likely to increase massively in the future. This calls for the development of effective dispute resolution mechanisms. This should be achieved in a coordinated manner in order to avoid the fragmentation of such mechanisms, even if the right to data portability may result from different regulatory sources. On this basis, it would be helpful to develop uniform alternative dispute resolution mechanisms in order to ensure the enforceability and effectiveness of the right to data portability for personal as well as for non-personal data. The need to develop transnational dispute resolution mechanisms further appears of key importance because of the transnational nature of many data portability disputes.

B. Privacy Shield Disputes

Another type of data disputes for which dedicated dispute resolution mechanisms have been created and implemented is the arbitration mechanism that was adopted under the Privacy Shield system.24 This special arbitration system is managed by

a most established ADR service provider, which is American Arbitration Association’s International Center for Dispute Resolution (ICDR).25

It should however be noted from the outset that the future of the Privacy Shield system (and thus of the Privacy Shield arbitration) is uncertain in view of the judicial challenge that it faces26 and also in light of the application of the GDPR, which has led to a resolution adopted by the European Parliament calling for the suspension of the EU-US Privacy Shield on the ground that the Privacy Shield would not comply with the (now enhanced) EU standard of protection of personal data resulting from the GDPR.27 For this reason, the Privacy Shield arbitration mechanism may not necessarily be promised to a bright future. It should further be noted that, in any event, the Privacy Shield arbitration system can be used only provided that various (potentially burdensome) pre-arbitration conditions have been met by the individuals before they can submit their dispute to arbitration (thereby risking to reduce significantly the importance of arbitration in practice).28

In spite of this, the Privacy Shield Arbitration remains inter-

25  See http://go.adr.org/privacyshieldannex.html and http://go.adr.org/privacyshield.html; this paper will not discuss this arbitration system in detail beyond a few selected high level comments and will not discuss either the so-called Independent Recourse Mechanism (IRM) that has also been created under the Privacy Shield system.

26  The case is now pending before the Irish Supreme court as a result of an appeal made by Facebook, see https://www.theregister.co.uk/2018/08/01/irish_supreme_court_makes_surprise_decision_to_hear_facebooks_appeal_in_schrems_ii/.

27  See the European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)) at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0315&language=EN&ring=B8-2018-0305; under this resolution, the European Parliament (among other points) “Takes the view that the current Privacy Shield arrangement does not provide the adequate level of protection required by Union data protection law and the EU Charter as interpreted by the CJEU; 35. Considers that, unless the US is fully compliant by 1 September 2018, the Commission has failed to act in accordance with Article 45(5) GDPR; calls therefore on the Commission to suspend the Privacy Shield until the US authorities comply with its terms”; for a comment, see N. Lomas, EU parliament calls for Privacy Shield to be pulled until US complies, TechCrunch (5 July 2018) available at: https://techcrunch.com/2018/07/05/eu-parliament-calls-for-privacy-shield-to-be-pulled-until-us-complies/.

28  See https://www.privacyshield.gov/article?id=C-Pre-Arbitration-Requirements.
esting to observe because it shows the benefits that arbitration and alternative dispute resolution mechanisms more generally can offer for solving international data disputes. It should also be noted that the arbitration system that is established under the Privacy Shield has a limited scope because it is limited to “non-monetary equitable remedy” and thus expressly excludes any damages, whereby damages could be claimed in other fora. This however does not mean that the system would not have any relevance knowing that other alternative dispute resolution mechanisms under which damages are also excluded have proven to be extremely useful for the stakeholders and to be most successful in practice. This is notably the case of the Uniform Domain Name Dispute Resolution Policy (UDRP) that was adopted for solving Internet domain name cybersquatting disputes and that has inspired various other similar alternative dispute resolution mechanisms for Internet domain name disputes. Even if the UDRP remains as an alternative dispute resolution mechanism that clearly does not replace court proceedings, it is worth noting that the UDRP has progressively become the go to dispute resolution mechanism for solving international domain name-related trademark disputes. On this basis, and even if

29 See https://www.privacyshield.gov/article?id=B-Available-Remedies: "Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the arbitration panel with respect to remedies. In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney's fees".

30 See https://www.privacyshield.gov/article?id=D-Binding-Nature-of-Decisions: "An individual's decision to invoke this binding arbitration option is entirely voluntary. Arbitral decisions will be binding on all parties to the arbitration. Once invoked, the individual forgoes the option to seek relief for the same claimed violation in another forum, except that if non-monetary equitable relief does not fully remedy the claimed violation, the individual's invocation of arbitration will not preclude a claim for damages that is otherwise available in the courts".

31 From this perspective, the UDRP constitutes a very interesting example showing the importance of alternative dispute resolution mechanisms for solving international intellectual property disputes.
no damages can be granted under the UDRP, the UDRP is and remains of key value for all stakeholders. This is confirmed by the record breaking number of cases brought before the WIPO Mediation and Arbitration Center (which is the most important platform offering UDRP and other Internet domain name dispute resolution services) for domain name disputes in 2017, almost twenty years after the adoption and implementation of the UDRP (in 1999).32

C. Disputes about Online Intermediation Services

Another source of future data disputes33 in the EU may result from the adoption of the Proposal for a EU regulation on promoting fairness and transparency for business users of online intermediation services (April 26, 2018) (hereafter the “EU online intermediation Regulation Proposal”).34

The EU online intermediation Regulation Proposal aims at protecting business users of online intermediation services35


33 The disputes that may emerge from this regulatory proposal go beyond data disputes (as conceived in this paper). However, this regulatory proposal still deserves to be discussed here given that it partly covers data disputes and further has features that are relevant for data disputes.


35 Online intermediation services are defined in Article 2(2) as services “which meet all of the following requirements: (a) they constitute information society services within the meaning of Article 1(1)(b) of Directive (EU) No 2015/1535 of the European Parliament and of the Council; (b) they allow business users to offer goods or...”
against various activities which include the unilateral changes of terms of services, the suspension or termination of the business users’ accounts and the conditions under which rankings are made by providers of online intermediation services and by providers of online search engines\(^36\) (with obligations of transparency, non-discrimination etc.). In addition to substantive provisions granting rights to the business users, the EU online intermediation Regulation Proposal further contains various provisions about the enforcement of the rights for the purpose of creating efficient remedies to business users of online intermediation services in view of the unsatisfactory situation that exists at present.\(^37\)

The dispute resolution mechanisms that are proposed in the EU online intermediation Regulation Proposal build together a multi-tier/multi-track system that is composed of an internal / easily accessible system for handling the complaints of business users (Article 9), of a mediation (Article 10(1) - (4)) and of court proceedings (Article 10(5) and Article 12).

\(^{36}\) Article 2(5) defines "online search engine" as "a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found".

\(^{37}\) Based on the EU Factsheet "Online Platforms: New Rules to Increase Transparency and Fairness" (25 May 2018) available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52447, the problems that have been identified by the Commission in terms of remedies that the EU online intermediation Regulation Proposal is designed to tackle are: "Lack of redress as 1/3 of all P2B problems remain unsolved and 1/3 are solved with difficulties Business users are faced with:
- Platforms’ inexistent or ineffective internal complaint handling mechanisms
- Inexistent specialised and effective external, out-of-court redress mechanisms
- Limited and costly access to EU Courts"
The internal complaint-handling system requires that the providers of online intermediation services shall have the obligations (among others) to process complaints swiftly and effectively (Article 9(2)). It also requires that the providers shall communicate to the complainant the outcome of the internal complaint-handling process (individual/ clear and unambiguous language) (Article 9(2)) and that they shall report on the functioning and effectiveness of their internal complaint-handling system (number of complaints, subject-matter, time period needed to process the complaints and decision) (Article 9(4)).

With respect to mediation, 38 providers of online intermediation services shall have the obligation to “identify in their terms and conditions one or more mediators with which they are willing to engage to attempt to reach an agreement with business users” (Article 10(1)). They shall also have the obligation to “engage in good faith in any attempt to reach an agreement through the mediation” (Article 10(3)). In terms of costs, a “reasonable proportion of the total costs of mediation” shall be borne by the providers, and in any case “at least half of the total cost” (Article 10(4)). The providers are further encouraged to “set up one or more organisations providing mediation services [...] for the specific purpose of facilitating the out-of-court settlement of disputes with business users arising in relation to the provision of those services, taking particular account of the cross-border nature of online intermediation services [...]” (Article 11). The need to develop specialized mediation services and to involve specialized mediators is justified because “[t]he involvement of mediators having specialist knowledge of online intermediation services and online search engines as well as of the specific industry sectors within which those services are provided should add to the confidence both parties have in the mediation process and should increase the likelihood of that process leading to a swift, just and satisfactory outcome”. 40 This is an important statement confirming the importance of having specialized providers of dispute resolution service that are experts in the relevant digital online markets and industries.

The EU online intermediation Regulation Proposal clarifies...
that the mediation “shall not affect the rights of the providers of the online intermediation services and of the business users concerned to initiate judicial proceedings at any time during or after the mediation process” (Article 10(5)).

The initiation of court proceedings by business users remains of course possible in case of disputes. Article 12 further provides that “[o]rganisations and associations that have a legitimate interest in representing business users or in representing corporate website users, as well as public bodies set up in Member States, shall have the right to take action before national courts in the Union, in accordance with the rules of the law of the Member State where the action is brought, to stop or prohibit any non-compliance by providers of online intermediation services or by providers of online search engines with the relevant requirements laid down in this Regulation”. This approach (which is common under consumer law but not in a B2B context) aims at ensuring the effective compliance by providers of online intermediation services and by providers of online search engines with their obligations under the EU online intermediation Regulation Proposal, given that individual court proceedings initiated by business users may not constitute a viable approach.

On this basis, the EU online intermediation Regulation Proposal regulates three different dispute resolution mechanisms for disputes between business users and providers of online intermediation services, which are the internal complaint-handling system, the mediation and court proceedings. It however does not mention at all other dispute resolution mechanisms that could also be of relevance, and most specifically arbitration. Arbitration could however be a very appropriate dispute resolution mechanism for solving cross-border commercial disputes, and

---

41 Which remains available, as expressly confirmed for by Article 12(3), which provides that “[t]he right referred to in paragraph 1 shall be without prejudice to the rights of business users and corporate website users to individually take action before competent national courts, in accordance with the rules of the law of the Member State where the action is brought, to address any non-compliance by providers of online intermediation services with the relevant requirements laid down in this Regulation”.

42 Recital 27: “Various factors, such as limited financial means, a fear of retaliation and exclusive choice of law and forum provisions in terms and conditions, can limit the effectiveness of existing judicial redress possibilities, particularly those which require business users or corporate website users to act individually and identifiably”.
would thus be a most adequate tool for disputes that may arise between business users and providers of online intermediation services.

Even if we can understand the absence of reference to arbitration from a policy perspective because of a (largely overestimated) defiance against arbitration that may be perceived as negatively affecting the right of access to justice, it is still important to clarify that the parties, and specifically the business users of online intermediation services can validly refer their disputes with the providers of such services to trusted neutral and independent expert arbitrators that could validly decide on such disputes in the course of arbitration proceedings. From this perspective, the advantages of having specialized mediators that are identified in the EU online intermediation Regulation Proposal would also fully and similarly apply to specialized arbitrators and arbitration institutions. The EU online intermediation Regulation Proposal could thus have exposed this and could further have exposed the interactions that can arise between the different dispute resolution mechanisms that it identifies. In this respect, it would be of value to clarify whether a mediation procedure could be initiated without first going through the internal complaint-handling system. It would seem appropriate to first go through the internal complaint-handling system and obtain a decision from the provider before the initiation of a mediation proceeding.

Similarly, the EU online intermediation Regulation Proposal could have exposed that mediation and arbitration can perfectly

43 This could have a particular weight in consumer disputes, and a lower relevance for corporate disputes.
44 Recital 26: “...the involvement of mediators having specialist knowledge of online intermediation services and online search engines as well as of the specific industry sectors within which those services are provided should add to the confidence both parties have in the mediation process and should increase the likelihood of that process leading to a swift, just and satisfactory outcome”.
45 This does not seem to be required by Article 10(1): “Providers of online intermediation services shall identify in their terms and conditions one or more mediators with which they are willing to engage to attempt to reach an agreement with business users on the settlement, out of court, of any disputes between the provider and the business user arising in relation to the provision of the online intermediation services concerned, including complaints that could not be resolved by means of the internal complaint-handling system referred to in Article 9” (emphasis added).
be combined (in med-arb proceedings) by which parties shall first submit their dispute to mediation, in the failure of which the dispute shall then be submitted to arbitration.46

IV. Conclusion

What can we learn from these various developments relating to both IP disputes (see II above) and data disputes (see III above)? First, what results from this analysis is that data disputes conceived in a broad sense as including IP data-related disputes are very frequent today and that they will certainly continue to grow in importance in the years to come as a result of various regulatory instruments and initiatives creating rights relating to personal and non-personal data (such as, by way of example, the right to data portability).

Second, these data disputes are legally complex in terms of substantive legal issues not only because they frequently require to take into account the position of third parties47 but also because they regularly have to balance competing rights and interests (some of which may be anchored in IP). IP data-related disputes dealing with the conditions of access and/or use of data (e.g. royalty data, confidential information) may in this context be relevant sources of guidance for certain types of data disputes, because data disputes may cover IP-protected data (i.e. trade secrets or copyright-protected content)48 and also because IP disputes and data disputes show similarities in the sense that they all cover intangible assets.

They can also be similar because of the relationship of dependence that may exist between the parties in dispute over

47 Such as in the case of sublicensing, or in the case of the limits to the right to data portability on the basis of third party rights and interests (Article 20(4) GDPR).
48 Another area of data disputes and of potential conflict between regulatory instruments can result from the interaction between consumer protection and copyright regulatory instruments; this has been discussed in Europe, see e.g. Jacques de Werra/ Evelyne Studer, Contracts on Digital Content in Europe: Balancing between Author-Protective Copyright Policies and Consumer Policies, Revue suisse de droit des affaires et du marché financier (2017) 35-47, available at https://archive-ouverte.unige.ch/unige:92503.
the control of the intangible assets. In the IP context, a relationship of dependence may arise with respect to a licensee who may be in a situation of dependence towards its licensor because of the risks that may affect its right to continue to use the licensed IP right in the future (specifically in case of bankruptcy of the licensor). Similarly, for data disputes, the risk of bankruptcy of the provider of data storage or other processing services also exists. The contemplated regulation provides with respect to the portability of non-personal data that the codes of conduct shall provide information before a contract for data storage and processing is concluded covering (among other elements) “the guarantees for accessing data in the case of the bankruptcy of the provider”.49

Third, — and this is the most important point of this paper also in light of the title and overall goal of the IPDC Vienna 2018 conference “on IP disputes and their effective resolution”, there is a need to conceptualize dispute resolution tools that shall be adapted to this challenging new environment of massive data disputes. It is indeed predictable that data disputes and more generally disputes with or connected to online platforms will grow significantly in the future.51 Time is thus ripe to develop dispute resolution mechanisms that shall be adapted to address the challenges of digital data disputes and specifically the challenges of what I have called “Massive Online Micro Justice (MOMJ)”.

This requires to adopt a concerted approach offering a coherent framework applicable to the different types of disputes and a

49 Art. 6(1)(a) of the European Non-Personal Data Regulation Proposal.
50 https://www.ipdc-vienna.com/ with a focus on the dispute resolution aspects of IP disputes.
51 A single judicial decision can generate a massive amount of disputes, as this was the case of the CJEU decision in the “right to be forgotten case” (judgment of the CJEU of May 13, 2014, Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González), which has generated several hundred thousand requests made to Google since then, see https://transparencyreport.google.com/eu-privacy?hl=en (Google has received 711'361 requests to delist as of 15 August 2018).
uniform dispute resolution mechanisms for the benefit of all stakeholders. From this perspective, it is regrettable that the various policy instruments that are developed in Europe for the time being do not seem to be sufficiently coordinated in order to provide a global data dispute resolution ecosystem that could apply to the different types of disputes. By way of illustration, it would be most desirable to adopt a uniform approach for the enforcement of the right to data portability which could cover both personal data and non-personal data even if the data are governed by different regulatory instruments. If an individual (data subject) faces challenges in the exercise of his right to data portability and if the data at issue (it will most likely be a frequent case) cover both personal and non-personal data, it would be valuable to have one single dispute resolution mechanism that shall empower the claimant (data subject) to enforce his right efficiently. It is likely in this respect that mediation and arbitration or other types of alternative dispute resolution mechanisms (similarly to the UDRP) would be very beneficial avenues for settling these disputes which will be mostly cross-border disputes. It may even be risky and counter-productive if the claimant had to use separate dispute resolution mechanisms that would be cost-ineffective and could even lead to potentially conflicting decisions.53

In terms of the level of specialization and of expertise of the dispute resolution providers, it would be adequate that such expertise of mediators / experts / neutrals shall also be transversal and shall thus cover issues relating to the portability of all kinds of data, irrespective of whether they are personal data or non-personal data.

In short, it is necessary to avoid the creation of a fragmented, piece-meal dispute resolution system under which each regulatory instrument would provide for its own separate set of dispute resolution rules and principles for data disputes, without consideration of parallel initiatives resulting from other regulatory instruments. Many policy documents rightly denounce the risks of fragmentation from various angles and thus ambition to find solutions that shall prevent the legal fragmentation by creating a

53 The right to data portability (for personal data) could be enforced in one proceedings and could not be enforced in another proceeding (for non-personal data) in spite of the hypothetically very close connection between the two categories of data (also because it can be difficult to assess in certain circumstances whether certain data may qualify as personal data under the GDPR).
framework of uniform rights and obligations at the EU level. However, they do not necessarily adopt the same approach when dealing with procedural issues and with the design of efficient dispute resolution mechanisms, even if these aspects do play an essential role in avoiding any fragmentation in practice. This means that a harmonization at the level of substantive law should be led hand in hand with measures of harmonization of procedural / dispute resolution legal principles. This harmonization should obviously and ideally not be limited to Europe but should rather be global knowing the worldwide reach of online activities and the global mobility of data.

What we thus (ideally) need is a new global data dispute resolution ecosystem that shall offer to all stakeholders a multi-tier dispute resolution mechanism for solving data disputes in a fair, equitable and (time and cost) efficient manner. This system should include a transparent internal review process. It should also include mediation and other alternative dispute resolution mechanisms (potentially arbitration — at least in B2B disputes —) that could be activated by the parties. It shall further keep traditional court proceedings before national courts available to the extent this shall be required in order to preserve the right to access to justice of the stakeholders, knowing that court proceedings will most likely be and remain quite burdensome, expensive and lengthy in many instances.

As a final note, it is important to stress that the dispute resolution and the intellectual property communities of practitioners and academics could most valuably contribute to this endeavour by sharing their precious expertise and extensive experience in order to conceive a new global dispute resolution ecosystem for solving data disputes in the digital era.

54 See e.g. EU online intermediation Regulation Proposal, 7 ("It should also address and prevent regulatory fragmentation across the EU").

55 It is therefore critical to pursue the development of policy proposals for this purpose, such as the Geneva Internet Dispute Resolution Policies 1.0 project led at the University of Geneva: www.geneva-internet-disputes.ch.