jipitec

3 | 2012

Volume 3 (2012)
Issue 1
ISSN 2190-3387

Journal of Intellectual Property, Information Technology, and Electronic Commerce Law

www.jipitec.eu

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 3 Issue 1, Mai 2012
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J.,
Karlsruhe Institute of Technology,
Vincenz-Prießnitz-Str. 3,
76131 Karlsruhe

Prof. Dr. Axel Metzger, LL. M.,
Institute for Legal Informatics,
Leibniz Universität Hannover,
Königsworther Platz 1,
30167 Hannover

Prof. Dr. Gerald Spindler,
Dipl.-Ökonom, Georg-August-Universität Göttingen,
Platz der Göttinger Sieben 6,
37073 Göttingen

Karlsruhe Institute of Technology, Leibniz Universität Hannover, and Georg-August-Universität Göttingen are corporations under public law, and represented by their respective presidents.

ISSN 2190-3387

Funded by
DFG Deutsche Forschungsgemeinschaft

Table Of Contents

Articles

Court Decisions

Book Review

Refining the legal approach towards the underage consumer: A process still in its infancy

by **Lodewijk Pessers,** Amsterdam, LLM, MA, Institute for Information Law (IViR)
University of Amsterdam

Keywords: Minors; E-Commerce; Underage Consumers; Contractual Capacities; Unfair Commercial Practices

Recommended citation: Lodewijk Pessers, Refining the legal approach towards the underage consumer: A process still in its infancy 3 (2012) JIPITEC 1, para 2

A. Introduction

1 If asked in what respects present-day consumers differ from those of a century ago, one can think of many possible answers, such as disposable income, brand loyalty, mobility, mentality and so on. One very significant aspect, though, will often not come to the mind: consumers have become much younger. The advent of e- and m-commerce has further sped up this development that was already in full swing. Nowadays children and adolescents constitute a sizable segment of the consumer population with their very own, sometimes contradictory, characteristics. On the one hand they are viewed as particularly vulnerable and protection-needy, while on the other they can be savvy and media literate as no other group. But not only may the nature of this heterogeneous consumer category be complex, the legal regime(s) under which they fall can be just as intricate. Especially the application of traditional, national rules in a digital and cross-border environment may prove confusing, to say the least. This situation thus gives rise to a broad spectrum of questions that is likely to continue to occupy the minds of academics (and hopefully those of politicians as well) in the years to come.

2 Recently, the author of this article contributed to an EU-commissioned study on 'digital content services for consumers' in which the subgroup of minors received research attention as well. The comparative analysis that was carried out in this context gives interesting insights into the current European situation with regard to the underage consumer. The perspective of this article, however, will be broader (both in space and in time) than this study alone: the child-consumer will also be put in a historical context, which may shed some light on long-run tendencies regarding the economic relevance and autonomy of this subgroup as well as the legislative responses to these developments. Against this backdrop it will be examined in which direction(s) lawmakers have moved so far and to what extent this concords with everyday practice.

3 Besides that, there is the continuous interplay with technological aspects. While new media, platforms and devices can complicate the functioning of existing rules and provisions, they can also be used to make enforcement more effective and reliable. As a brief outlook, the final part will touch upon a few challenges *and* opportunities that the on-going digitization may bring about.

B. A new consumer segment taking shape

4 Due to terminological and geographical indeterminacies, it is unfeasible to establish a precise moment in time when 'the underage consumer' came into being. It seems fair to assume, however, that the position of the child in the consumption process began to change somewhere in the early 20th century, especially in the United States.[1] In the 1910s, apparel retailers started to sell clothing for children in separate departments.[2] Previously, articles were arranged according to type, rather than to the age of the intended user. Of course, commerce specifically aimed at children was not completely new at the time – in Western Europe, toy shops already existed in the 18th century.[3] The change merely lay in the fact that children's departments were created within warehouses selling mainstream products. Purchasing decisions, however, were still made by parents. Minors, far from being an autonomous group of consumers, could at best influence the parental choice. This factor, the indirect decisional power of children, became increasingly important in the decades ahead.[4]

5 At the same time, a more fundamental transition evolved in which traditional educational values, such as thrift and frugality, were replaced with new ones, such as wise spending.[5] In the United States, for example, School Savings Bank programs were gradually overtaken by consumer education. Along with this shift of emphasis from saving to spending, pocket money was ever more used as an instrument to familiarize children with controlling their own finances.[6] This can be considered an important step in the emancipation of the underage consumer: the commercial relevance of this group was no longer exclusively based on their ability to influence purchasing decisions; with their own money at their disposal, children also became directly involved in the consumption process.

6 In the years after World War II, the autonomy of the underage consumer increased even further. This is partially due to the consolidation of changes already set in during the early 20th century, but other developments played a role, too. Among the latter, one can discern the enhanced position of minors in the job market. During the economic boom in the post-war period, wages went up significantly, particularly when compared with the meagre years of the depression in the 1930s.[7] In the late 1950s, a teenage worker in Britain earned 50% more in real terms compared to pre-war levels.[8] These incomes often came on top of the pocket money they already received.

7 Changes in consumption patterns were also associated with demographic factors. First of all, the number of children per family steadily declined over the last fifty years.[9] Combined with higher incomes brought about by the increase of dual-working families, more money could be spent per child. Similar numerical changes, with similar consequences, took place in the relationships of grandparents vis-à-vis grandchildren.

8 The sociological, psychological and cultural explanations for the rise of the child-consumer that have been put forward are even more numerous. Just to mention a few: as a reaction to the (relative) scarcities they had experienced in their own youth, the previous generation (over)compensated by coddling their children, the baby boomers;[10] working parents often redeemed guilt feelings towards their children with presents and gifts;[11] and through successful efforts by marketers to change the connotation of consumption – from traditionally feminine into a masculine, entrepreneurial and juvenile activity as well – a broader and younger segment of the population was tapped.[12]

C. Economic and media literacy

9 With minors gaining financial autonomy and visibility in the course of the past century, advertisers also began to take increasing interest in this group of consumers. New technologies – the first of which was the television pervading the Western world in the post-war decades – gave rise to direct and insistent marketing strategies.[13] With the gradual diversification of programming, commercials could reach the intended viewer in a more precise manner.[14] This form of communication between business and the child-consumer further strengthened a direct relationship between them, thus contributing to the ongoing 'emancipation' of the latter.

10 With the advent of Internet, this process even seemed to accelerate. According to a Belgian survey about minors and e-commerce,[15] conducted in the scope of the European Commission's Safer Internet Programme,[16] 34% of the minors interviewed have Internet access in their own room, and nearly all can use a shared computer for this purpose. When surfing on the Internet, most preadolescents (11 to 13 years old) and all adolescents (14 to 16 years old) visit commercial websites.[17] The frequency of Internet use steadily increases during childhood, reaching daily use around the age of 11. According to declarations of participants to the survey, awareness of privacy risks is quite low among all age groups and personal data – used to customize commercial communications – are often being shared without much of a hesitation.[18]

11 These findings suggest that children are often exposed, consciously and unconsciously, to commercial content and (targeted) advertising online. Even though the precise results may change per coun-

try, it seems fairly safe to conclude that the Internet has become an important (commercial) forum for minors, considering how early in life and how often it is used.

12 These emancipatory developments led to a reassessment of the relation between minors and commerce. In his book *The Kids Market*, Jim McNeal states that children constitute a three-layer market: a primary market for the money they spend on their own wants and needs, an influence market for as far as they direct their parents' purchases, and a future market of adult consumers on the basis of brand loyalty.[19] The author calculates that these layers, taken together, account for a multibillion market potential, unrivalled by any other demographic group.

13 An interesting question would be how these numbers exactly break down: What kind of products or services do minors buy? And what is the ratio between purchases made online and offline? Unfortunately, it seems that detailed statistics are still lacking.[20] However, in recent research on the situation, in the online environment some commercial activities and preferences are signalled more often, such as participation in auctions, visits to music and book stores like Amazon.com, the ordering of cinema or concert tickets and, ever more important, subscriptions to mobile phone services, in particular ringtones.[21] For some time, especially the latter has preoccupied national consumer authorities and the European Commission because a considerable number of providers active in this trade seem to operate in breach of Community law.[22]

14 It is important to notice, however, that revenues do not only come from direct transactions with minors. As mentioned earlier, in some business models the main objective is to gather personal data which are subsequently used for targeted advertising. To this end, websites offer games, quizzes or even virtual pets in exchange for children's personal data.[23] Considering the growing marketing expenditures for products aimed at children, a sum that in 2004 already totalled $15 billion in the United States alone, this business sector is likely to become even more important in the coming years.[24]

15 But once we have established that minors can be quite active netizens who also use the Internet for commercial purposes, it's still unclear if they are sufficiently skilled to operate in a safe manner. Here we touch upon the issues of economic and media literacy. Given the openness of these concepts and the diversity among minors, it is hard to treat these matters properly within the limited scope of this article. Yet a few findings may be worth mentioning.

16 We'll first have a brief look at children's and teenagers' financial expertise. Out of the numerous studies that have been conducted in this field, the picture emerges that there are considerable differences among youngsters, often reducible to obvious factors such as age, but also to social background and access to financial institutions.[25] Educational efforts to improve financial literacy have often been criticized for not keeping up with present-day practice or for remaining too theoretical in nature.[26] That's why alternatives have been proposed that focus rather on 'empowerment' of the minor than on 'protection', as taken in its traditional sense.[27] This, however, should not be understood as a plea for 'learning the hard way' by letting children work it out themselves in the (online) commercial environment. Instead, one should think of opening accounts for pupils so that they get familiar with financial instruments and saving money, rather than denying them any practical experience. But when it comes to actual spending, more prudence is in order. Obviously, a (basic) understanding of financial matters does not necessarily imply the required discipline and self-control to resist all kinds of commercial temptations. Indeed, it is known that minors are particularly susceptible to marketing strategies and peer pressure.[28] Up to the age of 16, children are still undergoing cognitive and social developments during which the capacity to make well-informed, independent choices is not fully matured.[29] It is important to bear this in mind, even if modern attempts to enhance 'economic literacy' among youth might be successful.

17 Somewhat different is the situation with regard to media literacy. It is often held that the younger generations are much better versed in (the working of) new technologies than the older ones. Some authors even see a crucial distinction between those who are 'born digital' and those who are not.[30] And shouldn't it be admitted that minors can be savvy, picky, streetwise and unexpectedly well-informed as no other group?[31] On the other hand, it's important to realize that these characteristics are just part of a larger picture. Media literacy does not only consist in mere technical knowledge but also in the experience to put this to safe and effective use.[32] A recent EU-funded study called 'EU kids online' even warns that more skills are associated 'with more, not less, risk.'[33] In addition to that, the belief that 'digital natives know it all' tops their list of myths about children's online risks.[34] Of course this is not the only appraisal: there are others that put more emphasis on the 'smart kid' as well.[35] For the moment it may therefore be better to reiterate the earlier observation that 'minors' are anything but a homogeneous group. The cognitive differences between the various age segments are vast, and general qualifications often run the risk of being inadequate or incomplete representations of reality.[36]

18 As a consequence, a rather blurred picture of the underage consumer may arise. As one can expect, law precisely tailored to the needs of such a diverse group is hard to make. In the next paragraph we will

describe how legislations within Europe deal with this consumer on the rise.

D. Legal and contractual capacities

19 The concept of 'legal capacities' as a way of protecting vulnerable parties has a long tradition, going back at least to Roman law.[37] To avoid misunderstandings, it is important to note that not the general capacity to have rights and obligations is meant here, for this is typically conferred upon natural persons at the moment of birth. In the context of the underage consumer, it is rather the 'contractual capacity' (which also goes under the broader name of 'legal capacity') that is relevant. Within the framework of this concept, rules have been developed to determine the validity of certain contracts.

20 At this point, no uniformity exists within the European Union, as all Member States have their own national contract laws. Even though some harmonization may be expected if Europe can, sometime in the future, agree upon a common set of contract law rules,[38] contractual capacities are very unlikely to be part of it. In an early stage this matter has been disqualified for harmonization, since it would rather appertain to the law of persons than to contract law. With this argumentation, the Lando Commission[39] has declared the subject outside the scope of the Principles of European Contract Law, as its article 4:101 explicitly states.[40] The subsequent (Draft) Common Frame of Reference or a future European civil code will therefore not change the continent's legal diversity on this point.

21 So, with regard to legal capacities, what does the European legal patchwork actually look like? For convenience of comparison it may be helpful to start with two characteristics that most jurisdictions have in common. First of all, a minor is typically defined as a person under the age of eighteen. Yet, under some circumstances – e.g. in the case of an early marriage – it is possible to attain majority even at the age of sixteen.[41] The second commonly shared feature is that persons enjoy no or limited legal capacities, as long as this age of majority has not been reached. Practically speaking, this means that legally binding contracts cannot be concluded unless parental consent has been given or an exception applies.

22 But when it comes to the exceptions, applicable laws within Europe start to diverge. Of course, this should not be understood as if every jurisdiction is highly unique in its approach: certain recurring principles can be discerned. Nonetheless, the translation of these principles into law and their interpretation by judges is often dissimilar. And even if such national idiosyncrasies did not exist, countries still make different selections out of the pool of criteria. Therefore, an overview of the European situation is hard to give without resorting to certain generalizations.

23 One of the most common exceptions may illustrate the point. In many jurisdictions, contracts can still be validly concluded by a minor, as long as they qualify as 'everyday' or 'usual'. But behind this broad term lies a wide range of nationally defined criteria. In France, for example, a minor always needs legal representation, except for 'acts of daily life' which, in their turn, are defined by the rather abstract concept of 'usage.'[42] The basic assumption that underpins this term seems to be that no serious risk may be involved in the transaction. Only trivial purchases, such as candies or other small objects, will therefore fall within the scope of the exception. In the Netherlands a comparable principle applies, but there the law refers to acts with regard to which it is 'common practice' that they are performed independently by minors of a certain age.[43] In the United Kingdom the situation is again somewhat different, since the Sale of Goods Act 1979 defines the exempted category as 'necessaries', i.e. goods suitable to the condition in life of the minor [...] and to his actual requirements at the time of sale and delivery.[44] Since this test has to be applied subjectively, with consideration of the actual circumstances it is hardly possible to predict with certainty what will be deemed a necessary other than basic needs such as food and clothing. And to make the assessment even more complicated, it is also required that the underage contractor had not already been adequately provided with the item that was purchased.[45]

24 Many more jurisdictions could be cited that all apply their own versions of this exception for 'usual' transactions. So, although it's not infrequently a common principle that inspires legislators, the diverse, national elaborations thereof do still lead to a rather heterogeneous situation in Europe. It is very likely that a doubtful case – let's say the downloading of a mid-priced video game by a fourteen-year-old minor – would be decided upon differently throughout the continent.

25 In some countries these difficult assessments, which are an inevitable result of 'limited' capacities, can simply be left untouched when the minor's age is below a certain minimum. In such cases, a contract concluded without parental consent is void or voidable, no matter the normality of the transaction or the necessity of the good. This 'threshold' is set at various ages, running from 7 in Germany[46] up to even 15 in Norway.[47] Of course, it is questionable whether it reflects daily practice when minors still lack any legal capacity only three years before adulthood. As pointed out earlier, in the course of the last century children have become ever more active and independent consumers. In addition to that, before turning fifteen, children are already likely to be familiar with purchasing 'anonymously' via computer or

mobile phone, which partially deprives the rule of its practical effect.[48] Of course, this objection can be raised (and *will* be raised later on in this article), not only with regard to minimum age provisions but on a much broader front.

26 But besides these protective measures, one can also find emancipatory rules – and it is the very same Norway with the high minimum age of 15 years that provides some interesting examples in this respect. Most importantly, there is the so-called pocket money exception.[49] This means that a minor is allowed to spend according to his own judgment all money intentionally placed at his free disposal. The same is true for transactions paid for by a minor's own earnings.[50] Compared to the standard of 'normality', this provision grants the underage consumer with greater autonomy. The purchase itself is not scrutinized to establish whether the transaction was allowable, but just the source of the money. It must be repeated, though, that these first steps towards full legal capacity are taken quite late in adolescence. In addition to that, exceptions for pocket money and own earnings are accompanied by rather stiff safety catches in the form of high minimum ages. Also in other countries that have similar exceptions, such as Poland and Hungary, the minimum ages are again rather high with 13 and 14 respectively.[51]

27 As this cursory look at the European situation reveals, the treatment of minors within contract law consists of a combination of elements both aimed at the protection and at the empowerment of the underage consumer. This dilemma was already faced in the 1970s when the Council of Europe adopted a resolution[52] that lowered the age of full legal capacity to 18 years. Its fourth recital reads: 'Believing that even though life today is more complex than formerly, the education gained during a prolonged and compulsory schooling and the abundance of information available enable young people to meet the exigencies of life at an earlier age than before.'[53]

28 The statement pithily summarized the forces that were in play: life was getting increasingly complex, and youngsters were growing more and more accustomed to it. Even though this observation may still hold some truth nearly forty years after its drafting, it also sounds somewhat dated. Today the argument of 'prolonged and compulsory schooling' sounds less compelling when it comes to the pitfalls modern consumers may encounter. In this respect, the digital and technological savvy of younger generations may sometimes trump the 'prolonged and compulsory schooling' of the older ones. Obviously, this doesn't turn things around completely: during childhood, cognitive and psychological capacities are still in the process of development and are not equal to those of an adult. However, the uneven distribution of digital skills over the generations does have its effects on traditional notions about vulnerability.

29 The same can be said about the information argument. Where the Council believed that 'the abundance of information' could only be beneficial to the young consumer, today this view has been substantially nuanced. Strategic uses of 'abundant information' by traders can also be a threat to transparency, hurting in particular less experienced (and often underage) parties.

30 Admittedly, the resolution should be understood in the context of its time, and a modern interpretation could easily fail to grasp its emancipatory essence. An anachronistic reading, however, may reveal how volatile the subject is. The appropriate level of protection should continuously be assessed against the backdrop of the society's complexity and the child's maturity (as referred to in the recital): while ever more hazards and lures are out there, minors also get increasingly skilled in understanding and avoiding them. The balance that is subsequently struck differs in space and in time. Although an overall tendency towards the enhancement of a minor's autonomy seems to prevail, a closer look shows that this course is far from 'linear'. More recent pieces of legislation, mainly in the field of unfair commercial practices (and media law), illustrate that the struggle between sufficient protection and further emancipation is still on-going.

E. Unfair commercial practices

31 Under contract law, protection of minors is mainly corrective in nature, since it can only offer remedies *after* an undesired contract has already been concluded. Of course, such provisions often have preventive effects as well: when parties expect that the validity of a certain transaction can easily be affected, it is less likely to be initiated. However, this will hardly count as a sufficient reassurance. Because many unwanted contracts will still be concluded (only a small percentage of which will make it to judicial examination), earlier intervention in the form of market regulation remains necessary.

32 The European legislator has taken up this task on several occasions. Most recently with the introduction of a Directive on Unfair Commercial Practices, in which some provisions for the protection of vulnerable consumers have been adopted.[54] Article 5(3) of the Directive, for example, sets forth that commercial practices aimed at a 'clearly identifiable group [...] shall be assessed from the perspective of an average member of that group'. The article makes particular mention of those who are vulnerable because of 'their mental or physical infirmity, age or credulity'. Even more specific is the reference to 'children' in no. 28 of the Directive's first Annex, which designates as 'misleading' any 'advertisement [that contains] a direct exhortation to children to buy adver-

tised products or persuade their parents or other adults to buy advertised products for them.'

33 So may we already speak of a robust reinforcement of the underage consumer's legal position? Not quite. First of all, both provisions sanction existing practice rather than enrich it with new or additional measures. The prohibition of commercial exhortations towards children was already included, albeit in a slightly different wording, in the 1989 Television without Frontiers Directive (which will be discussed shortly). And the flexible benchmark consumer, adaptable to the addressees of the commercial practice, is also certainly not a novel concept. As revealed by a survey conducted in the context of the study on 'digital content services for consumers', national legislations often already provide for this kind of adjustment when interpreting such open norms.[55] In Germany, for example, the Supreme Court considered an advertisement for an excessively priced ringtone subscription unfair by giving particular weight to the young age of the targeted public, whose inexperience was capitalized on.[56] It is quite conceivable that the Directive will not have a significant bearing on the approaches national courts already took. And if any effect is nonetheless to be expected, in some jurisdictions this may also be the lowering, not the heightening, of the level of protection. Indeed, the Unfair Commercial Practices Directive is a maximum harmonization instrument that could in some cases require a 'downward' adjustment of national legislations. Micklitz, for example, observes that under Swedish and Finnish laws, rules about advertisements aimed at children are more stringent than in the Directive, in particular no. 28 of its first Annex.[57] This means that the implementation of the new standard could leave the underage consumer even worse off, at least in those countries.

34 Of course, all this doesn't imply that no good should be expected from the Directive. Since it outlaws a considerable number of practices for being misleading or aggressive, it undoubtedly entails benefits to the consumer *at large*. Yet before placing the Directive in a tradition of increasing (or decreasing) protection for the specific subgroup of minors, it should be examined alongside more fundamental transformations in consumer law. As some authors have roughly sketched, in the past century legislators have gradually moved away from a *laissez faire* ideology in favour of values such as solidarity and equality.[58] Boldly put, we are all ever more regarded as vulnerable parties. Seen within this greater development, the protection granted to minors by adopting a 'new', adjustable benchmark consumer for the evaluation of commercial practices hardly stands out. In addition to that, the flexibility of the standard makes its practical functioning uncertain and probably nationally coloured.[59]

35 So if the European legislator has resumed his role of caretaker towards minors by issuing the Directive on Unfair Commercial Practices, it cannot be denied that he did so with some reticence.

36 The relative restraint of the approach becomes even more apparent when it is compared to earlier initiatives aimed at strengthening the protection of minors, such as the aforementioned Television without Frontiers Directive,[60] which later was replaced by the Audiovisual Media Services Directive.[61] The former may – somewhat euphemistically – be called 'ambitious' in this respect. While commercial television was on a rapid rise, Europe felt that prompt and effective measures had to be taken to regain some control over the content and advertisements reaching the public.[62] Commercials and unsuitable programs were subjected to detailed rules safeguarding the physical, mental and moral development of minors. By adding subsequent amendments, which resulted in the said Audiovisual Media Services Directive, the stringency of the provisions was made contingent on whether content was broadcast or, less intrusively, made available on-demand.

37 The rules in these Directives are rather elaborate and explicit: they proscribe aggressive advertising strategies aimed at children[63] (such as those exploiting their credulity or containing exhortations to buy a product; cf. number 28 of the Unfair Commercial Practices Directive first Annex), addressing minors in commercial communications for alcoholic beverages[64] and making available to them pornographic or violent content.[65] And not unimportantly: the provisions only formed a minimum threshold. Although these and many other articles have been preserved in the Audiovisual Media Services Directive, the spirit of the Directive has changed significantly in the course of the amendments. While the first version exhibited a relatively strong belief in the efficacy of legislation, its successors appeared to put more responsibility on (media) consumers themselves. In this new approach, the emphasis shifted to – here it is again – media literacy, which according to the Directive consists of the skills, knowledge and understanding that allow consumers to use media effectively and safely.[66] By upgrading consumers, including minors, 'from couch potato[es] to active market player[s]'[67] the European Commission made a visible attempt to eschew its traditional paternalistic reflexes. 'Empowerment' became the new shibboleth in Brussels, which could better be achieved by 'continuing education', 'internet training' and 'national campaigns' than by further expanding the legal arsenal.[68] The efficacy of such an approach obviously remains very uncertain. We saw before that there are clear limits to what any financial or media education program can accomplish. So, as with the Unfair Commercial Practices Directive, it again seems advisable to retain some caution about the re-

modelled Directive's face value until more is known about its practical consequences.

F. Legal challenges and opportunities in the digital era

38 When the underage consumer ascended nearly a century ago, the world looked considerably different. Consumption required face-to-face contact with traders, no television existed and much less the Internet. Even though laws have also changed in the wake of advancing technologies, their development has been rather modest. The age of full legal capacities has been lowered somewhat, and media laws have been put in place to protect against undesirable content. However, this legislative trend, which may at best be called cautiously emancipatory, seems to have proceeded at a slower pace than everyday practice.

39 Especially the advent of the Internet and mobile phones has significant implications for minors as consumers, both from a practical and a legal perspective. While the former has already been briefly discussed in the historical analysis, the latter might need some further clarification.

40 Since online transactions take place without contracting parties being physically present, minors cannot be differentiated from adults.[69] This means that traders are usually not aware of the legal (in) capacities of their customers. Where minors would have difficulty to conclude certain contracts in 'offline' stores, in the digital environment they can easily escape notice. This may seriously undermine the preventive effect that the doctrine of legal capacities used to have. Obviously, this can come to the detriment of traders, who may face voidances of contracts they could hardly prevent. (To mitigate these adverse effects somewhat, a few countries have stipulated that such protection may not be invoked in case of fraud or deceit.[70])

41 Another complication lies in the fact that e-commerce can easily cross borders, thus becoming subject to a host of different legal regimes with different criteria, exceptions and terminologies. While underage consumers gained autonomy and mobility –combined with decreased recognisability – their protection is still nationally organized and based on traditional concepts.

42 In addition to these uncertainties, the digitization may also give rise to legal conundrums. An important issue, for example, regards the voidance of contracts involving intangible products, such as a ringtone or a movie in a streaming format. National law often stipulates that undoing a transaction entails the restitution of the good. Obviously, this can hardly be applied to content delivered in a digital form. Hence rules relating to services – which are usually incapable of being rendered – may come into play. However, the typical solution – that in such circumstances, compensation is due if the content has been to the true benefit of the minor (which will often be the case) – makes voidance a sham remedy. But the opposite approach, in which risks and costs should be borne by traders, is also hard to justify.

43 So it does seem that existing laws are not always fit for the digital environment. While it is rather obvious that this will affect businesses operating online, especially when legislation is scattered or unclear, consequences may also be felt by the underage consumer. Indeed, undesired and possibly voidable contracts will often not be subject to judicial review.[71] Legal problems that traders may face from a theoretical point of view will therefore not always materialize in actual adverse judgments. When the increased facility of entering into all kinds of agreements has negative effects, they will not infrequently stay with the aggrieved minors and/or their parents. Secondly, legal costs that *are* being made by companies are likely to be partially passed on to their customers by way of higher prices. So the financial burden of inadequate legislation will probably be shouldered by businesses and consumers alike.

44 Of course, the on-going digitization should not only be viewed as a threat to the smooth functioning of laws dating from the previous century. If used intelligently, new technologies can also be used to *enhance* the transparency of online consumption. By developing sophisticated age verification tools, legal capacities can be assessed even more reliably than ever before.[72]

45 And perhaps that's not all. When such tools become part of smarter payment systems, other opportunities may arise as well.[73] Take, for example, the exceptions to the rule of legal incapacity in the case of pocket money or own earnings as enacted in some jurisdictions. If new payment systems allowed for the 'labelling' of money, such emancipatory provisions might gain practical significance. Instead of creating legal uncertainty, digitization could also be employed to reduce it.

G. Conclusion

46 In the course of the 20th century, minors have become an ever more important consumer segment. The era in which they could, at best, influence their parents' purchase decisions, popularly termed the 'nagging factor', is long past. Today, underage consumers have their own resources at their disposal in the form of allowances or their own earnings, and spending them is often just a mouse-click away. In

addition, consumption increasingly takes place in the digital environment, which makes it harder to recognize and prevent inappropriate transactions.

47 The legislative response to the enhanced autonomy of this subgroup may be called cautiously emancipatory: the age of majority has been lowered to eighteen years throughout Europe, and exceptions to the default rule of absent legal capacities have been introduced in most countries. However, lawmakers (at both a national and a European level) have also taken steps to protect this vulnerable group against the risks of new media and intrusive or deceptive advertisement strategies. Since this simultaneous 'paternalistic' tendency cannot only be perceived with regard to minors, but rather to the consumer at large, it is hard to isolate and characterize the legislative stance towards the former.

48 But probably more important than this issue of typification is the question whether the current approach is in line with everyday practice. At this point, doubts may be raised. First of all, the current system of legal capacities works on the assumption that the suitability of contracts is assessed by traders on a case-by-case basis, considering e.g. the age of the consumer and the nature of the purchase. In the context of e- and m-commerce, such appraisals will (and can) hardly ever be made. And neither are the remedies always fit for the digital age, as the voidance of digital content contracts may illustrate. Moreover, there is the problem of scattered legislation governing a cross-border phenomenon. The legal uncertainty resulting from this fragmentation is likely to burden online commerce with practical hindrances and financial costs.

49 So how should policy makers respond to all this? As argued before, an easy solution to these problems probably does not exist. Minors form a large, highly heterogeneous group of consumers, which complicates the draft of clear-cut rules that suit all. In the light of this difficulty, one may be sceptical about the chances of quick and effective legal reforms being put in place. In this respect, it suffices to recall the explicit rejection to deal with the subject of legal capacities in the (Draft) Common Frame of Reference. And even if an attempt to harmonization were made, the outcome of such a harsh task would inevitably be prone to criticisms. This doesn't alter the fact, however, that consumers and businesses would probably welcome such political courage: a single set of rules could help cross-border trade function much more smoothly, thus reducing transaction costs. If, for example, minors in Europe were allowed to conclude 'everyday contracts', this could significantly level the common commercial playing field without imposing a very unfamiliar criterion. But for a large number of small reasons, such a step is unlikely to be taken.

50 And if it's not from a practical perspective, then there might also be a more fundamental reason to question whether trust should predominantly be put in the legislators in the present case. Technological developments have played an important role in shaping the current underage consumer and in challenging existing laws as to their applicability and tenability. It may well be the case that (a part of) the solution must be sought in the very same field that necessitated reforms in the first place. The development of reliable age verification tools or smarter payment systems could reduce uncertainties and make digital commerce more transparent for traders and consumers alike. Even though caution is advised, especially when it comes to privacy implications, the protection and empowerment of the underage consumer may this time depend on forces other than legislators alone.

■

1 D. Cook, *The Commodification of Childhood: The Children's Clothing Industry and the Rise of the Child Consumer* (Durham: Duke University Press, 2004), 41-65.

2 *Ibid.* Cook mentions in particular a manufacturer of infants' garments called Earnshaw. The new marketing strategy was combined with the issuance of specialized catalogues, such as The Children's Wear Review.

3 P.N. Stearns, *Consumerism in world history: the global transformation of desire* (London and New York: Routledge, 2006), 20.

4 Cook, *The Commodification of Childhood*, 66-95.

5 L. Jacobson, *Raising Consumers: Children and the American Mass Market in the Early Twentieth Century* (New York: Columbia University Press, 2004) 56 et seq.

6 G. Cross, 'The Consumer Economy', in *The Encyclopedia of Children and Childhood in History and Society*, vol. 1, ed. Paula S. Fass (New York: Macmillan Reference, 2004), 242 et seq.

7 B. Gunter & A. Furnham, *Children as consumers: a psychological analysis of the young people's market* (London and New York: Routledge, 1998) 1.

8 J. Davis, *Youth and the condition of Britain: images of adolescent conflict* (London: Atlantic Highlands, 1990) 118.

9 J. McNeal, *The Kids Market: Myths and Realities* (Ithaca NJ: Paramount Market Publishing, 1999), 20.

10 E. Seiter, *Sold Separately: Children and Parents in Consumer Culture* (New Brunswick, NJ: Rutgers University Press, 1993), 15.

11 McNeal, *The Kids Market*, 22.

12 Jacobson, *Raising Consumers*, 13.

13 See also M.L. Chiarella, 'The Regulation of Child Consumption in European Law: Rights, Market and New Perspectives', *Revista para el Análisis del Derecho* 3 (2009): 5.

14 S.L. Calvert, 'Children as Consumers: Advertising and Marketing', *The Future of Children* 18/1 (2008): 207.

15 The survey was carried out in 2008 by OIVO-CRIOC, the Information and Research Centre of the Belgian Consumer Organisations, and is online accessible at <www.oivo-crioc.org/files/nl/3943nl.pdf> http://www.oivo-crioc.org/files/nl/3943nl.pdf(Dutch) and <www.oivo-crioc.org/files/fr/3944fr.pdf> http://www.oivo-crioc.org/files/fr/3944fr.pdf(French).

16 For more information, see the website at <ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm>.http://ec.europa.eu/information_society/activities/sip/index_en.htm

17 Survey by OIVO-CRIOC, 15-16. Contrary to what one might expect, the interest in commercial websites does not grow linearly with age, but shows two 'peaks' instead: one at the age of 12/13 and one at 16.

18 This should not be understood, however, as though minors were not aware of any privacy risks in the online environment. See, for example, S. Youn, 'Teenagers' perceptions of online privacy and coping behaviors: a risk-benefit appraisal approach', *Journal of Broadcasting & Electronic Media* 49/1 (2005): 86-110.

19 McNeal, *The Kids Market*, 29.

20 *Ibid.*

21 See the OIVO-CRIOC survey, 15-16, R. Willet, 'Consumer Citizens Online: Structure, Agency, and Gender in Online Participation', in Youth, Identity, and Digital Media, ed. D. Buckingham (Cambridge, MA: The MIT Press, 2008) 53, K.C. Montgomery, 'Digital Kids: The New On-Line Children's Consumer Culture', in Handbook of Children and the Media, eds. D.G. Singer & J.L. Singer (London: Sage Publications, 2001) 635-650, D. Cook, 'Knowing the child consumer: historical and conceptual insights on qualitative children's consumer research', Young Consumers, 10/4 (2009): 269-282 and Calvert, Children as Consumers.

22 See a press release by the European Commission, IP/09/1725, Brussels 17 November 2009. For an overview of the results in national investigations by consumer authorities, see the accompanying MEMO/09/05.

23 See, for example, Ellen Seiter about the website www.neopets.com, E. Seiter, *The Internet playground: children's access, entertainment, and mis-education* (New York: Peter Lang Publishing, 2005), 83-100.

24 Calvert, *Children as Consumers*, 207.

25 M.H. McCormick, 'The Effectiveness of Youth Financial Education: A Review of the Literature', *Journal of Financial Counseling and Planning* 20/1 (2009): 70-83.

26 L.E. Willis, 'Financial Education: Lessons Not Learned & Lessons Learned', Legal Studies Paper No. 2011-22, Working Paper presented at Conference on Financial Education and Consumer Financial Protection (Boston 2011).

27 See, for example, E. Johnson and M.S. Sherraden, 'From Financial Literacy to Financial Capability among Youth', *Journal of Sociology and Social Welfare* 34/3 (2007): 119-146.

28 D.R. John, 'Consumer socialization of children: A retrospective look at twenty-five years of research', *Journal of Consumer Research* 26 (1999): 183–213.

29 *Ibid.*

30 See in particular J. Palrey & U. Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (New York: Basic Books, 2008).

31 See, for example, Seiter, *The Internet playground*, 106.

32 See also the definition of 'media literacy' in the Audio Visual Media Services Directive, Recital 47.

33 The short explanation for this statement is that 'more use leads to more skills, more skills lead to more opportunities, and opportunities are linked to risk. One reason that opportunities and risks are linked is because children must explore and encounter some risk to learn and gain resilience. Another is that exploring for information or fun leads to unexpected risks because the online environment is not designed with children's interests in mind (too many pop-ups, for instance).' See S. Livingstone et al., 'Final Report EU Kids Online', deliverable 8.3 for the EC Safer Internet Programme, 43, available online at <www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>.

34 'Children knowing more than their parents has been exaggerated – only 36 per cent of 9-16-year-olds say it is very true that "I know more about the internet than my parents" – 31 per cent say "a bit true", and two in three 9-10-year-olds say "not true". Talk of digital natives obscures children's need for support in developing digital skills.' Livingstone, Final Report EU Kids Online, 43.

35 According to Seiter, the truth about children's ability to discriminate isn't even in the middle: 'I believe the advertising industry's image of the savvy viewer is much closer to reality than ACT's [Action for Children's Television] image of the innocent child.' Seiter, *Sold Separately*, 106.

36 D.R. John describes how the development of the underage consumer can be subdivided in three stages, differing significantly among each other: the perceptual stage (3-7 years), the analytical stage (7-11 years) and the reflective stage (11-16 years); see D.R. John, 'Consumer socialization of children: A retrospective look at twenty-five years of research', *Journal of Consumer Research* 26 (1999): 186.

37 Under Roman law, the attribution of legal capacities – that is, the faculty to enter into legally binding agreements – was made contingent upon a number of features, such as age, sex, citizenship and mental health. Male minors, for example, could independently transact all business matters for themselves from the age of 14 onwards. However, until the age of 25 they enjoyed special protection against fraudulent or even disadvantageous transactions, which made them unattractive counterparties for adult traders. Only when the minor had appointed a curator (which was often the case, especially when the minor had possessions of any significance) could contracts confidently be concluded upon the approval of the latter. See A. Berger, *Encyclopedic dictionary of Roman law* (Philadelphia: The American Philosophical Society, 1991), 379 and W.L. Burdick, *The principles of Roman law and their relation to modern law* (Clark NJ: The Lawbook Exchange 2007), 269.

38 For an update by the Commission about the progress that has been made so far, see the 'Optional Instrument', European Commission, Proposal for a regulation of the European Parliament and of the Council on a Common European Sales Law, COM(2011)636final, Brussels, 11.10.2011.

39 Officially known as the Commission on European Contract Law.

40 This chapter does not deal with invalidity arising from illegality, immorality or the lack of capacity.'

41 M. Loos et al., *Digital Content Services for Consumers: Comparative analysis, law and economics analysis, assessment and development of recommendations for possible future rules on digital content contracts* (Amsterdam: University of Amsterdam, 2011), final report prepared for the European Commission, accessible online at <http://www.ivir.nl/publications/helberger/digital_content_contracts_for_consumers.pdf>, p. 138.

42 The so-called '*actes de la vie courante*,' see N. Baillon-Wirtz, *L'enfant, sujet de droits* (Paris: Lamy, 2010), 126 on article 408 of the French civil code.

43 See article 1:234 of the Dutch Civil Code.

44 Sale of Goods Act 1979 s 3(3).

45 P. Richards, *Law of contract* (Oxford: Oxford University Press, 2007), 86.

46 Article 104 of the German Civil Code.

47 Article 33 of the Norwegian Guardianship Act.

48 The Consumer's Ombudsman in Norway has indicated this lack of physical presence as one of the major challenges with regard to the enforcement of the Guardianship Act. See the 'Consumer's Ombudsman Guidelines on Commercial Practices towards Children and Youth' (Oslo 2009), 15 available at <www.forbrukerombudet.no/english>.

49 Loos et al, *Digital Content Services for Consumers*, p. 138-141.

50 *Ibid.*

51 *Ibid.*

52 Resolution (72)29 on the lowering of the age of full legal capacity, adopted by the Committee of Ministers on 19 September 1972 at the 213th meeting of the Ministers' Deputies.

53 *Ibid.*, 4th Recital.

54 Article 5(3) and No. 28 of Annex I of the Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market.

55 Loos et al, *Digital Content Services for Consumers*, p. 141-142.

56 Bundesgerichtshof, case I ZR 125/0, rendered April 6th, 2006.

57 G. Howells, H. Micklitz & Th. Wilhelmsson, *European Fair Trading Law, The Unfair Commercial Practices Directive* (Aldershot, Hampshire: Ashgate, 2006), 249, note 24 and 25.

58 See also M. Hesselink, 'Capacity and Capability in European Contract Law', *European Review of Private Law* 13/4 (2005), 497.

59 See again Micklitz, who rightly points out that the terms used in article 5(3) are often open to national interpretations, which may notably differ among each other. The 'children', for example, referred to in recital 18 are not defined (by age or otherwise) and neither are qualifications such as 'credulity' or 'commercial inexperience.' This means that 'Member States will retain a margin of appreciation in determining the need for protection of weaker parts of the population as the Community is far from agreeing and wanting to agree on such subtle, and at the same time fundamental, social policy questions.' See G. Howells, H. Micklitz & Th. Wilhelmsson, *European Fair Trading Law,* 113-115.

60 Directive 89/552/EEC of the Council of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities.

61 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive).

62 C. Pauwels, H. Kalimo & K. Donders, *Rethinking European Media and Communications Policy* (Brussels: Brussels University Press, 2010) 141.

63 Article 9(1)(g) of the Audiovisual Media Services Directive (2010/13/EU), which replaced article 16(a-d) of the Television without Frontiers Directive (89/552/EEC).

64 Article 9(1)(e) of the Audio Visual Media Services Directive replacing article 15(a) of the Television without Frontiers Directive.

65 Article 27 of the Audio Visual Media Services Directive replacing article 22 of the Television without Frontiers Directive.

66 Audio Visual Media Services Directive, 47th Recital.

67 N. Helberger, 'From eyeball to creator - toying with audience empowerment in the Audiovisual Media Service Directive', *Entertainment Law Review* 6 (2008) 137.

68 Audio Visual Media Services Directive, Recital 47. See also the Safer Internet Programme at <ec.europa.eu/information_society/activities/sip/index_en.htm>; a five-year extension of the programme (up to the year 2013) has been agreed upon by the European Parliament and the Council in Decision No 1351/2008/EC, entailing a € 55 million financial envelope; see art. 6(2).

69 In the words of D. Kidd and W. Daughtrey, '[e]lectronic contracts may never appear on a piece of paper, may involve instantaneous transactions, may involve minimal or no negotiation or interaction, and may involve no human interaction at all.' See D.L. Kidd & W.H. Daughtrey, Jr., 'Adapting Contract Law to Accommodate Electronic Contracts: Overview and Suggestions', *Rutgers Computer & Technology Law Journal* (26) 2000, 215.

70 Loos et al, *Digital Content Services for Consumers.*

71 Especially when the product is of limited value, as may often be the case when a purchase by a minor is concerned, many consumers would not bring a dispute to court because they deem it too costly or time consuming. See Chapter IV of the European Commission Special Eurobarometer 195, 'European Union Citizens And Access To Justice', October 2004, available at <ec.europa.eu/consumers/redress/reports_studies/eurobarometer_11-04_en.pdf >.

72 The use of age verification tools may also have undesired side-effects, mainly in the field of privacy. About the benefits and risks of age verification technologies: F. Gilbert, 'Age Verification as a Shield for Minors on the Internet: A Quixotic Search?', *Shidler Journal of Law, Commerce and Technology* 6 (2008), G. Hornung & A. Roßnagel, 'An ID card for the Internet – The new German ID card with "electronic proof of identity"', *Computer Law & Security Review* 26/2 (2010) 151-157, and from a broader perspective S. Livingstone, Children and the Internet (*Cambridge: Polity Press*, 2009), 91-120.

73 Although quite a few such payment systems are the subjects of patent (applications), widespread use of these inventions still seems far away. For example, see US Patent No. 7,502,761 and Patent applications No. 20090210240 and 20080265020.

Cloud Computing in the EU Policy Sphere

Interoperability, Vertical Integration and the Internal Market

by **Jasper P. Sluijs, Pierre Larouche, Wolf Sauter**, Tilburg Law and Economics Center (TILEC), Tilburg Law School

Abstract: Cloud computing is a new development that is based on the premise that data and applications are stored centrally and can be accessed through the Internet. This article sets up a broad analysis of how the emergence of clouds relates to European competition law, network regulation and electronic commerce regulation, which we relate to challenges for the further development of cloud services in Europe: interoperability and data portability between clouds; issues relating to vertical integration between clouds and Internet Service Providers; and potential problems for clouds to operate on the European Internal Market. We find that these issues are not adequately addressed across the legal frameworks that we analyse, and argue for further research into how to better facilitate innovative convergent services such as cloud computing through European policy – especially in light of the ambitious digital agenda that the European Commission has set out.

Keywords: Cloud Computing; Economic Policy Concerns; European Law; Competition Law

Recommended citation: Sluijs/Larouche/Sauter, Cloud Computing in the EU Policy Sphere: Interoperability, Vertical Integration and the Internal Market, 3 (2012) JIPITEC 12, para 12

A. Introduction

1 Cloud computing is currently viewed by many in the industry as the 'next big idea'thatwill see major information technology companies vying to compete.[1] It has also been described as providing computing resources as if it were a utility – accessible by anyone anywhere with an Internet connection, and always on tap.[2] Finally, it is regarded as an 'extreme form of vertical integration, just carried out by other companies than the telecommunications service providers, and at higher levels of the protocol stack'.[3] Arguably, therefore, cloud computing stands to shake up the technology, telecommunications and media sectors for the next few years.

2 This change and innovation give rise to the question whether and how cloud computing policy should be approached on a European level. Cloud computing is a global phenomenon with impact on the internal market in terms of innovation and regulatory harmonization. European law has settled for a regulatory approach to the digital sphere in which competition law, regulation of networks and electronic commerce regulation are treated as separate legal regimes.[4] The main regulatory issue to address, therefore, is how to approach a cloud computing provider in regulatory terms – through competition law, network regulation, electronic commerce or across those fields.

3 The European Commission has circulated an ambitious digital agenda as part of the 2020 Lisbon strategy, highlighting the importance of innovative and convergent online services – such as cloud computing providers – for the European internal market.[5] Can available European laws accommodate the broad adoption of cloud computing facilities, while addressing possible concerns that arise along the way? How does European policy deal with the challenges raised

by the further emergence of cloud computing? Is the EU regulatory regime ready to meet this trend? The literature on cloud computing in relation to European law shows a strong emphasis on data protection, privacy and security issues.[6] We wish to introduce a different approach, focusing on the relationship of cloud computing to domains of EU law that have hitherto had less attention. This research sets up a broad framework to assess a numberof European legal fields and their relationship to cloud computing. After a thorough analysis of the phenomenon of cloud computing on a technical and policy level, we will single out challenges that cloud computing services face as they develop to maturity as a market: data portability and interoperability constraints; the complexity involved in vertical integration between clouds and Internet Service Providers (ISPs); and potential problems for clouds to operate on the European Internal Market. We will then analyse how competition law, network regulation and electronic commerce regulation can address these potential challenges.

4 We will conclude that the challenges for cloud computing that we highlight cannot be addressed adequately by the existing European regulatory regime. We find that competition law addresses interoperability and data portability constraints for clouds only in an indirect way, through the abuse of dominance regime. At the same time, we find that the competition law framework for vertical integration is not very well tailored towards advanced online services such as clouds, mainly due to problems involved with market definition of the cloud sector. Moreover, competition law does little to streamline clouds' operation on the European internal market. European electronic communications (network) regulation only indirectly affects cloud computing services, as this regulatory framework mainly applies to the ISPs that carry cloud data. Here we see that network regulation is of little use to mitigate interoperability and data portability for clouds, and might not prevent the leveraging of market power by dominant ISPs into cloud computing markets. Finally, EU electronic commerce regulationis most applicable to cloud computing in terms of definitions, but it does little for clouds that is beneficial. The guidelines on jurisdictional issues of the Electronic Commerce Directive will most likely not streamline operating on the internal market for cloud service providers, and the Directive's provisions on secondary liability are increasingly coming under pressure by courts and governments.

5 In all these fields that we analyse, cloud computing seems to exceed the scope of the provided legal mechanisms. The disconnect in legal scope between clouds and the laws that concern clouds demonstrates that the fields of competition law, network regulation and electronic commerce regulation remain more distinct than would be desirable in the light of convergent practice. Cloud computing forms a new, hybrid technology that is affected by all of the above legal instruments, yet we find that clouds are over-regulated on matters of minor importance, while aspects that could seriously stifle the further emergence of cloud computing remain legally unaddressed.

6 As Iansiti has argued, we need to investigate how the principles behind cloud computing relate to existing policy rationales.[7] This article aims to function as a first attempt at providing a guide to cloud computing on a European policy level with a focus on competition law, network regulation and electronic commerce regulation. As such, we argue that these legal domains are not prepared to accommodate the further advent of cloud computing. Our article offers a critical roadmap to the status of clouds under these specific and interrelated fields of European law, and provides suggestions for a more elaborate research agenda on cloud computing in the EU policy sphere.

B. On cloud computing: Definitions, market, policy

7 Cloud computing is a new development combining different services in a manner that arguably revolutionizes computer and Internet usage. The central feature of cloud computing is that existing and novel computing applications are increasingly being performed in a 'cloud' online – i.e. not on users' own hardware.[8] The announcement by Google and IBM of their collaboration on cloud computing research in 2007 sparked broader public awareness of cloud computing.[9] The 'revolutionary' aspect of cloud computing, however, may sometimes be overstated, as many applications of cloud computing – think of webmail – have been around since the Internet became popular for consumers.[10] Indeed, some have remarked that the move to cloud computing demonstrates a cyclical progression in computing: from centralized mainframes, to personal computers, to personal computers tied together in clouds.[11]

I. Relevant characteristics of cloud computing

8 The underlying idea of cloud computing seems to be that functions that are now discharged either on the client or on the firm-internal local area network (LAN) server would be moved to the 'cloud'. The possibility of placing in the 'cloud' well-established local applications such as word processors or spreadsheets – and the documents produced therewith – has caught the public imagination and has brought cloud computing to the fore.

9 The nascent academic field that analyses cloud computing has developed many formal definitions of this phenomenon,[12] yet the recent set of precise definitions provided by the US National Institute of Standards and Technology (NIST) is rapidly becoming authoritative. We find the NIST definition of cloud computing a useful starting point. It mentions five defining characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.[13]

10 (1) On-demand self-service implies that consumers have unilateral access to different cloud services whenever required. These cloud capabilities are available through (2) broad and ubiquitous network access, a virtual web platform accessible through a variety of devices—PC's, laptops and smartphones, for instance.[14] Such ubiquity distinguishes cloud computing from previous stages of evolution in computing:[15] cloud services are accessible from any point, over any network, using any device.[16] Because of this ubiquity, cloud computing enables (3) resource pooling (also referred to as multi-tenancy[17]), which means that a cloud offers access and services to multiple at the same time, and computing resources are assigned flexibly based on demand.

11 Resource pooling allows for (4) rapid elasticity, or mass customization[18] of computing power both on the demand and supply side: From the supplier's perspective, choices and options for consumers can be built into the software platform. Customers pick and choose on their side of the platform, in a process that can be automated easily.[19] The provider can thereby reap economies of scope, which are the essence of mass customization.[20] Accordingly, from the customer's side, cloud computing services can appear customized: customers get the right amount of services, with the combination of features and options that matches theirneeds.[21] For suppliers versed in a server-client model, the shift to cloud computing marks a radical change in the business plan: instead of selling software licenses, suppliers must move to an access- or subscription-based business model, whereby customers will purchase services offered on the cloud computing platform on a discrete (pay-as-you-go/access) or continuous (subscription) basis. For (corporate) consumers of cloud computing power, clouds in fact represent a form of outsourcing of IT services that used to be run in-house. Therefore,moving to cloud computing involves significant organizational change, which will usually imply that larger customers will have specific requirements regarding privacy, data protection and security, confidentiality, reliability, etc.[22]

12 The demand for IT outsourcing that cloud computing affords can be explained by multiple interrelated factors. The proliferation of digital data has created a demand for large amounts of processing power and storage owned and operated by third parties instead of by the users themselves.[23] Moreover, the Internet economy has so far both stimulated and thrived upon bottom-up market entry by small-scale startups,[24] for which cloud computing services offer opportunities to enter markets and innovate, without having to invest in costly hardware and other resources.[25] Furthermore, outsourcing through cloud computing meets a demand for 'utility-like' access to computing resources, which are available 'ontap' for a subscription fee.[26] This can be seen as a commoditizing effect on the market for online computing power.[27]

13 The rapid elasticity of cloud computing, finally, is facilitated by the (5) measured service provision that clouds enable: resource allocation can be measured and disclosed, 'providing transparency for both the provider and consumer of the utilized service'.[28]

14 Combining these five characteristics, cloud computing can thus be described as 'a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources ... that can be rapidly provisioned and released with minimal management effort or service provider interaction'.[29] This definition, however, does not address the wide variety of applications and services that are available through a cloud today. We want to distinguish different implementations of cloud computing in order to explain the phenomenon of cloud computing more accurately. At this stage of development of the cloud computing market, however, it would be premature to analyse systematically how subcategories of cloud computing individually relate to European regulation. Further implementations are likely to be added as cloud computing takes off, as well as further examples of the categories below. Following the same NIST scheme, we propose a subdivision as follows:

1. Software as a Service (SaaS): This is the most visible application of cloud computing on the consumer market. It involves access to services without having to install additional software on a computer. Applications such asGoogle Maps, YouTube and Salesforce's CRM are run from a cloud and involve data-intensive operations that are executed in the cloud, returning the results to the user.

2. Platform as a Service (PaaS): These services offer remote access to development platforms for software without the need for buying and deploying the necessary software and hardware for this 'on the ground'. Platforms such as Microsoft Azure, Google App Engine, Servoy and Salesforce's force.com allow application builders to design, implement and run their products using the firms' own server power.

3. Infrastructure as a Service (IaaS): An IaaS offers remote computing and storage services. Consumers or corporate clients can store or backup data on servers with unlimited capacity. For instance, the *New York Times* makes available its archive from 1851 through 1989 via the Amazon S3 server.[30]

II. Potential economic policy concerns surrounding cloud computing

15 In the following section, we will carry out a preliminary examination of potential economic policy concerns surrounding cloud computing. This examination is conducted in the light of the characteristics outlined above, on the basis of a rudimentary model, whereby a number of cloud computing providers (two for the sake of simplicity) compete to sell their services to an enduser.[31] This enduser, however, is using those services in various locations and with various devices (computer, smartphone, tablet, etc.). In order for the enduser to consume cloud computing services, a link between the cloud and the enduser must be established. That link runs over an IP network, which can rest on a variety of underlying architectures (DSL, cable/DOCSIS, cellular mobile [GPRS/EDGE/3G and further developments]or wireless (wi-fi, WiMAX, etc.).

16 In the first part of this analysis, we will assume that the link to the enduser is provided by a single supplier – at cost plus reasonable return and in a uniform and non-discriminatory fashion across different network types – in order to focus on concerns thatcould arise horizontally at the cloud computing provider level. Second, we will introduce multiple (and partly competing) network providers in the model to ascertain which vertical concerns could arise through the interplay of cloud computing providers and network providers.

1. Concerns at the cloud computing provider level

17 Assuming for the sake of argument that the link between the cloud and the user is always available at a reasonable price under uniform and non-discriminatory conditions across the various networks, we can concentrate for this section on competition between the cloud computing providers as the main phenomenon to study. Here, two features described above – outsourcing and mass customization – are relevant. First of all, the outsourcing of data storage and computing power naturally involves the delegation to clouds of data processing formerly run in-house. As in all outsourcing agreements, this creates dependency of the outsourcing client on clouds. Second, this dependency is reinforced by the mass customization of the service, which implies some relationship-specific investment from the customer (to configure the services to its needs, in terms of features, consumption volumes, etc. and then to upload consumer-specific data on the cloud).

18 For cloud computing providers following a model of mass customization, there is limited interest in engaging in relationship-specific investments. Nevertheless, the relationship-specific investments from the customer side can suffice to create some product differentiation. In other words, there is a risk of the customer becoming locked in with the supplier. In that case, providers could conceivably create switching costs – for instance, by limiting the portability of customer data to and from competing servicesto enhance customer lock-in.

19 Indeed, the emerging literature on cloud computing has voiced concerns about consumers' demand to migrate data to and from different clouds (data portability),[32] and interoperability between clouds.[33] This is in essence a horizontal issue: potential interoperability and data portability constraints impede on the possibility for consumers to use complementary cloud services alongside each other and migrate their data from one cloud to another. At the same time, if potential customers find that the risk of lock-in is too high, they will refrain from purchasing cloud computing services altogether, or request assurances from cloud computing providers. So there is a trade-off, and cloud computing providers cannot enhance lock-in at will. Yet even if switching costs are kept in check, in order to induce uptake of the services, they might still be high enough to discourage the entry of new cloud computing providers. Consumer lock-in due to limited data portability and interoperability can thus be seen as a key challenge for the further development of cloud computing.[34]

2. Concerns at the ISP/ network operator level

20 Second, the characteristics of cloud computing, as set out above, imply that data will have to be carried between cloud service providers and consumers. In the above section, we assumed away any concerns regarding the link between the cloud and the consumers for the sake of argument. In practice, however, that link is very significant for our analysis. Herein lies a key difference from the computing models used until now, where the link between the central and non-central units was part of the computing architecture and under the control of the provider or the customer: either it was a mere conduit (mainframe-terminal) or a local area network (server-client). In a cloud computing model, the link is in the

hands of third parties. What is more, because of ubiquity, it is part and parcel of the cloud computing model that service provision for a single cloud computing customer can run over various types of links, operated by different third parties, depending on where the customer is located and which type of device (and network interface) it is using. In other words, customers expect to have the same service, with the same quality and 'feel', irrespective of whether they reach the cloud computing provider via an ADSL network in Brussels, a hotspot in London, or a 3G network in Paris.

21 Therefore, unless cloud service providers plan to rollout their own networks – which only Google is planning to do on a small scale[35] – this required transfer of data between the cloud and the customer requires cloud providers to interact with Internet Service Providers (ISPs) or network operators. A number of remarks must be made here.

22 As a preliminary matter, contractual relationships between the cloud provider, the customer and the ISP are complex. The cloud computing provider (CCP) and the customer are bound by an agreement for the provision of cloud computing services. This agreement assumes that a means will be found to transfer data between the cloud and the customer. This is when ISPs step in. Presumably, the customer at any given time and location has a contractual relationship with an ISP at his or her end (ISP_{cust}); otherwise the customer is unable to send and receive data. This can be a permanent relationship (subscription) or a temporary one (permission to use hotspot or Wi-Fi services, roaming). Given the desired ubiquity of cloud services, the identity of ISP_{cust} might vary from time to time and from one location to another. However, at any given time and location, the customer is usually reachable through one ISP_{cust} at a time.[36] As will be further elaborated upon below, ISP_{cust} thereby gains some market power (i.e. a situational monopoly, even if transitory), in a way reminiscent of the terminating operator in traditional telecommunications. In turn, the CCP must also have a relationship with an ISP (ISP_{CCP}) in order to branch out of the cloud and towards the customer. ISP_{CCP} can be the same as ISP_{cust}, or the CCP can indirectly rely on ISP_{CCP} having some form of arrangement (peering, routing) with ISP_{cust}. It will already be apparent that, given ubiquity, a CCP must entertain and maintain relationships – direct or indirect – with a large number of ISPs that might potentially qualify as ISP_{cust} at any given time and customer location.[37]

23 ISPs find themselves in a difficult strategic position at this juncture: their service – Internet access – has been on a path to commoditization over the last decade. Access-based tariffs have been replaced by monthly flat-rate subscriptions, and even though the quality of the services has increased steadily – at least if speed is a reference – subscription prices have decreased. Yet ISPs must undertake significant investments to upgrade access networks to the capacity and performance level needed to use the next-generation applications (usually involving video). In order to generate the revenue streams needed to finance such investments, ISPs are driven to try to break the trend towards commoditization by introducing differentiated offerings. Among other means of differentiation, ISPs can turn their networks from mere conduits to two-sided platforms,[38] where content, service and application providers meet users. In order to do so, they need to generate mutually reinforcing network effects on both sides of the platform – for instance, by adding features to their network that enable themtooffer better Quality of Service (QoS) parameters.[39] If and once ISPs embark on a differentiation strategy, two potential concerns could arise.

24 A first concern relates to *vertical integration and discrimination*. ISPs can decide to make cloud computing part of their differentiation strategy, i.e. to try to gain a competitive advantage through the offer of cloud computing services. This could be done either on their own motion (greenfield entry),[40] via vertical integration with a CCP, via some form of preferential agreement with a CCP or even unilaterally by giving a preferential QoS level to a given CCP provider.[41] In all these situations, by implication, the ISP would discriminate against competing CCP providers in favour of its own/affiliated/preferred CCP. Vertical issues have already been mentioned repeatedly in the literature as being of key importance in the further development of cloud computing.[42] Yet it seems that ISPs have strong incentives to interact with CCPs and not to engage in discriminatory practices. Since cloud computing services must be ubiquitous and CCPs are unlikely to rollout their own network to reach their users, as mentioned above, CCPs will want to ensure that their services are available through as many ISPs as possible. Moreover, two-sided-platform theory predicts that ISPs benefit from offering access to as many CCPs as possible,[43] since this makes their platform more attractive to users. Clouds and ISPs thus seem to have strong incentives to interact amicably.

25 A second concern arises more clearly in Europe and is related to the *internal market*. In principle, CCPs have little to gain from ISP efforts to escape commoditization by turning their services into two-sided platforms. From the perspective of the CCP, it is preferable if the ISP rather invests in upgrading its network so as to provide the best possible commodity service, i.e. Internet access at the highest possible speed, with the best possible quality of service. The situation in Europe is already complicated enough, when compared to the USA. Following consolidation in the USA, a CCP in fact must deal with only two large providers of fixed and mobile line communications,[44] two additional mobile com-

munications providers[45] and a few large cable-based ISPs. In the EU, each of the 27 Member States comprises a few mobile communications providers (one of which is usually the fixed-line incumbent) and perhaps a couple of competitive fixed communications providers, including cable-based ISPs. Despite some consolidation at the European level, business plans are still essentially made at the Member State level. Accordingly, a CCP would have to oversee upwards of 100 ISPs to ensure that its service is ubiquitous. If these ISPs all decide to embark into differentiation strategies, then a CCP could be left with a patchwork of different ISP platforms to contend with. Since these platforms would offer varying levels of Quality of Service, it could become impossible for CCPs to implement ubiquity (with a constant feel across ISPs), at least in Europe. At present, the TCP/IP protocol, with its end-to-end principle and best-efforts routing, is used across Europe, so this issue does not truly arise. The internal market is fostered by the same token. With the implementation of QoS differentiation, as part of an effort by ISPs to escape commoditization, the internal market could become fragmented so that CCPs would not be able to deploy ubiquitous services across the EU.

26 Contrary to interconnection, it is not possible to deal with QoS differentiation among European ISPs simply via contracting, i.e. entering into an agreement with one ISP and relying on this ISP to provide uniform QoS across the EU, just like major ISPs can offer universal connectivity to their customers. The problem is not so much transaction costs arising from a contractual maze (as with interconnection), but rather the fragmentation among QoS offerings across the EU. Aggregating all those various QoS offerings in the hands of one contractual partner for CCPs does not overcome that fragmentationas such.

27 In summary, three potential concerns come up when approaching clouds from a (European) economic policy perspective. First, we find *interoperability and portability* concernsbetween cloud computing providers. Second, we find that *vertical integration and discrimination* issues could arise between CCPs and ISPs if ISPs decide to integrate vertically into cloud computing. Third, we find that the *internal market* could be fragmented by a patchwork of different ISP platforms and their various network management policies so that CCPs could not provide ubiquitous services, i.e. services with the same 'feel' and quality across the many ISPs present in the EU.

28 In the rest of this paper, therefore, these three concerns will be addressed specifically when assessing how cloud computing relates to European law. We will embark on this endeavour by outlining what effect European competition law, network regulation and electronic commerce regulation have on the development of cloud computing.

C. Cloud computing under European law

29 As in the policy concerns set out above, the following outlines the possible approaches to cloud computingin European law and policy. As described above, cloud computing in essence is an IT service for which there is no explicit regulation on a pan-European level. Nonetheless, three European legal regimes are potentially relevant to the concerns set out above: EU competition law, EU electronic communications regulation and EU electronic commerce regulation.

I. The regulatory division of labour

30 Before examining each of these three regimes, the 'regulatory division of labour' among them must bebriefly explained. On the one hand, EU economic regulation is characterized by a rich and complex relationship between competition law and sector-specific regulation. On the other hand, the regulation of the converged telecommunications and media rests on a distinction between network regulation and content regulation. Both these interactions between legal fields have an effect on cloud computing services, as will be illustrated in this section.

31 The first legal articulation that has an effect on cloud computing is between sector-specific regulation and general competition law. As is now well established, EU law proceeds differently from US law: under EU law, competition law is always applicable across the whole economy, irrespective of any sector-specific regulation.[46] Accordingly, sector-specific regulation is always formulated against the backdrop of competition law, with some implications. At the systemic level, rightly or wrongly, sector-specific regulation is seen as a temporary phenomenon which complements competition law until such time as competition law alone can suffice to police the sector in question.[47] At the substantive level, sector-specific regulation relies on economic analysis and borrows concepts from competition law. At the institutional level, competition and regulatory authorities are meant to coordinate their actions. For instance, in electronic communications regulation, heavier obligations are only available against operators holding 'Significant Market Power' (SMP). The SMP concept in turn is based on the concept of dominance under general competition policy – in an attempt to dovetail the two regimes and avoid a proliferation of competition standards.[48]

32 Regulation of content, by contrast, does not overlap as much with competition law as electronic communications regulation. Accordingly, the policing of proper market functioning is by and large left to competition law, including state aid law – which

plays a large role in regulating public broadcasting. Sector-specific regulation of media and broadcasting has traditionally pursued other objectives, beyond proper market functioning, such as plurality and cultural diversity, with a strong role for national politics in the policymaking process.[49] The harmonizing attempts in the content sector have a more 'vertical' character than in telecommunications, and content regulation is concerned more with guaranteeing the internal market freedoms.[50] There is a wide range of content-related regulation, yet we wish to focus on the regime that is most related to cloud computing: the Electronic Commerce Directive.[51]

33 Thus, the European legal regimes that potentially have an effect on cloud computing are characterized by an interaction between sector-specific regulation and competition law, and a horizontal separation between content and network regulation. While especially the content-network divide in European law has been subject to criticism,[52] our aim for this article is not to critique any of these two divisions of labour as such; we will assume them for the sake of analysis. Rather, we want to investigate how the main outstanding issues in the development of cloud computing that we have outlined above – data portability and interoperability,vertical integration and internal market concerns – relate to these legal regimes.

II. Competition law

34 In contrast with EU electronic communications or e-commerce regulation, competition rules always apply to all firms active in the EU – therefore, all cloud operators active in the European Union are subject to it.[53] In this section we will investigate whether competition law is able to address the three issues of interoperability and data portability, vertical integration and internal market fragmentation.

1. Market definition

35 Prior to any discussion of the substantive provisions, it is essential to try to assess how relevant markets could be defined to ascertain how competition authorities would comprehend the competitive constraints on cloud computing providers. Market definition hinges on establishing product and geographic markets,[54] with some attention to temporal dimensions as well. This temporal aspect is quite relevant in relation to cloud computing. The Commission has recognized that in markets with a high degree of technological progress – such as cloud computing – market conditions can change significantly over time, which would argue in favour of a (short) time window for markets, allowing for narrower market definitions.[55] In the EU, market definition typically depends on demand-side substitutability, which is ascertained with the help of a qualitative analysis of product characteristics and intended use, sometimes complemented with quantitative analysis, using an SSNIP test for a hypothetical monopolist.

36 Product market definition issues would arise at the upstream (cloud computing provider) and downstream (ISP) level. At the upstream level, at its narrowest, the relevant market could be limited to individual types of cloud computing services (i.e. SaaS, PaaS, IaaS), because these services differ in characteristics and use. Such a definition would overlook supply-side substitutability, however. Cloud computing services rely on mass customization, meaning that providers try to exploit economies of scope by ensuring that large investments into facilities can be leveraged across many services at limited cost (software modifications). A broader market definition would include not just cloud computing, but also software solutions from which users are migrating to cloud computing (e.g. software installed locally in a server-client environment). Here the outsourcing characteristic of cloud computing is of importance: Is cloud computing a new market in and of itself, or are clouds simply part of the larger market for IT services?

37 At the downstream level, market definition exercises have already been conducted in the course of applying electronic communications regulation. Some conclusions can be drawn from that practice, bearing in mind that relevant market definition carries limited precedential value. As far as retail customers are concerned, the Commission has usually considered that broadband Internet access is separate from narrowband access, because substitutability runs in one direction only (from narrowband to broadband). Furthermore, mobile and fixed access are generally put on separate markets because of their different product characteristics.[56] On that basis, there is a good chance that ISPs would not all be put on the same market.

38 Beyond that, it is worth examining whether the specific approach to market definition for wholesale call termination (fixed and mobile) might have an impact here. Since the first Recommendation on relevant markets in 2003,[57] the Commission has considered that when it comes to the wholesale market for call termination, each network forms its own relevant market. In essence, when a call is made, the operator of the calling party (the originating operator) has no choice but to deal with the operator to which the called party is subscribing (the terminating operator) in order to complete the call as requested by its customer, the calling party. There is no alternative to the terminating operator, since the number of the called party is reachable only through the terminating operator. By aggregation, considering that all subscribers of a given operator are in the same position vis-à-vis that operator, the Com-

mission found that all the subscribers of a given operator – i.e. all subscribers reachable via the network of that operator – are on a separate relevant market for call termination.

39 This reasoning can be applied by analogy to cloud computing. For a cloud computing provider, at any given point in time, a customer can usually be reached via one ISP only – i.e. the ISP to which the device used at that point in time is attached, whether it is a DSL- or cable-based ISP, an ISP associated with a workplace LAN, a mobile provider or the ISP to which a Wi-Fi network is connected. What is more, given the ubiquity that is characteristic of cloud computing, customers might be reachable via a succession of ISPs as they move around, in a way which the customers themselves might not be able to control entirely,[58] much less the cloud computing provider. It is true that, in contrast with call termination, there is a greater chance that at any given point in time, a cloud computing customer might be reachable via more than one ISP, so that no situational monopoly would arise. Nevertheless, in the current state of technology, it is difficult for either the cloud computing provider or its customer to move rapidly and efficiently from one ISP to another to react to unfavourable conditions that an ISP might offer at any given point in time.

40 As far as geographical markets are concerned, clouds are built on the premise of ubiquity, mobility and pervasiveness, which is not easily captured into a geographic market defined as the area where competitive conditions are comparable.[59] The markets are presumably larger than purely national. After all, the ubiquity and portability of clouds leads towards a market scope that goes beyond national borders. For example, the market for business software, in which Oracle and SAP AG are key players, has traditionally been nationally oriented, bounded by language, physical software copies and local storage of data.[60] Relative newcomer Salesforce has disrupted these market characteristics by offering its SaaS services exclusively through clouds, without being established in all countries where its service is available. Similarly, cloud-based office applications such as OpenOffice, Googledocs and docs.com widen the geographic scope in comparison with shrink-wrapped office software, which was more nationally oriented. There is every indication so far that the market for cloud computing willbe global, though it cannot be excluded that, should linguistic and cultural preferences play a larger role in customer choices, national markets may remain.

41 Geography has more impact at the downstream ISP level. There one can observe significant differences in regulation among Member States. Roaming practices and interconnection regulation, for example, do have a (geographic) effect on clouds, yet possibly not to the extent that it constitutes a 'condition of competition ... appreciably different in [other geographic] areas'.[61] The geographic markets for ISPs that form the platform between end-users and clouds are more fragmented than the (potential) geographic market for the clouds themselves. After all, ISPs are connected to physical infrastructure that ties them to a specific jurisdiction, while clouds naturally operate across the internal market in a transnational manner. Therefore, considering path dependency and the presence of legal barriers, broadband provision markets would be national.

2. Interoperability, data portability and competition law

42 At first sight it may seem difficult to fit issues of data portability and interoperability under EU competition law. For the sake of argument, we will assume that interoperability and data portability constraints are potential results of anti competitive behaviour – which is often referred to in case law on this topic.[62] Difficulties in achieving interoperability and data portability in cloud computing can already lead to what would be classified as customer lock-in, by primarily technological means, further resulting in customer dependency on the services of CCP (especially when a strong element of outsourcing is present in moving to cloud computing). That lock-in effect can be aggravated by the abusive conduct of a CCP within the meaning of Article102 TFEU, whereby other CCPs are excluded from competing for the customers of that CCP. Furthermore, even in the absence of exclusionary conduct, a CCP could also abuse its dominant position by exploiting its customers.[63] On the scale of dominance issues, exclusion of competitors (or foreclosure) is generally held as more harmful than exploitation of customers. This is because exploitation may trigger entry (solving the competition problem), whereas foreclosure blocks the competitive provision that would benefit consumers and make exploitation impossible.[64] For the remainder of the discussion, we will leave exploitative abuse aside.

43 Before trying to assess whether a given course of conduct is abusive, however, dominance must first be established. Market dominance is generally understood to concern a situation in which a firm is able to set prices and other competitive parameters independently of competitive pressure. Relevant evidence includes market shares, potential for future expansion and entry, and buying power.[65] Case law testifies to a reliance on market shares as an indicator of dominance,[66] and a broad interpretation to entry barriers.[67] Generally, market shares of over 40% raise scrutiny. Even in the absence of clear-cut figures on market shares in the cloud computing sector, it seems unlikely that any active cloud service currently enjoys such market shares in any re-

levant market. We have defined three varieties of cloud computing services above, and there seems to be vigorous competition between the various firms active in these branches of cloud computing, such as Google, Microsoft, Amazon, Apple, Salesforce, IBM and so on.[68] Moreover, the entry of Amazon, for instance, into the cloud market demonstrates that though entry into the cloud computing market carries significant fixed costs, barriers to entry are not insurmountable. There may well be more firms like Amazon in other sectors with excess server capacity, keen on entering the IaaS market:

> *Entry barriers may also become less relevant with regard to innovation-driven markets characterised by ongoing technological progress. In such markets, competitive constraints often come from innovative threats from potential competitors that are not currently in the market. In such innovation-driven markets, dynamic or longer term competition can take place among firms that are not necessarily competitors in an existing 'static' market.*[69]

44 Were a single CCP to enjoy market shares of over 40% and be considered dominant, it would still need to be proven that such dominance is abused. In line with the approach put forward by the Commission in its Guidance Paper, this is a matter of identifying a theory of harm whereby the conduct of the dominant firm results in anti-competitive foreclosure (i.e. exclusion of competitors leading to consumer harm).[70] Here the conduct could be any conduct which creates or increases customer switching costs and lock-in – for instance, making it more difficult than technically necessary to port consumer data from one CCP to the other, or to work with two or more CCPs simultaneously. Thereby the customer acquisition costs of rivals would be raised or– in the extreme case – rivals would even be foreclosed altogether if they were deprived of a large enough potential customer base for viable entry and expansion. It is already apparent that this course of conduct does not fit neatly within the broad types of abusive conduct identified in the Guidance Paper.[71] Furthermore, it is in the essence of cloud computing services that – especially when the customer is outsourcing to the CCP – the customer is locked-in as a result of relationship-specific investments on its part to customize services and relocate its private/proprietary information on the CCP facilities. As was seen above, market forces will conceivably constrain CCPs on customer lock-in. Accordingly, evidence of 'intent' would likely play a large role in any finding of abuse on the part of a dominant CCP; 'intent' is here understood broadly as a deliberate and plausible plan on the part of the CCP.[72]

3. Vertical integration and EU competition law

45 As mentioned above, the literature on cloud computing has voiced concerns over vertical integration between CCPs and ISPs with potential anti-competitive effects.[73] In a European context, such vertical restraints can be dealt with under either Article101 or 102 TFEU. Of course, vertical integration can also occur through a merger between a CCP and an ISP, but we will set this hypothesis aside for now.[74]

a.) Under Article 102 TFEU

46 For ISPs, high market shares above the dominance threshold are a possibility, all the more so if product markets differentiate between fixed and mobile broadband and if, as caselaw so far indicates, the geographic scope of ISP markets seems national (or in the US context, state-level).[75] Under such circumstances, it would not be surprising to find that one or two ISPs are dominant in a given Member State.[76] Furthermore, if the termination market construction described above is followed, then all ISPs are dominant on a market formed by their own network.

47 Case law is growing rich in Article 102 TFEU cases related to European ISPs, as a result of which ISPs are severely hampered from abusing their dominance through means of predatory pricing[77] or margin squeeze,[78] for instance. Here we are looking at a situation where an ISP – which would have integrated into cloud computing or otherwise affiliated with a cloud computing provider – would refuse to deal with an unaffiliated CCP on the same terms as it deals with its own cloud computing operations or its affiliated CCP.

48 At first sight, this could be an instance of discrimination within the meaning of Article102 (c) TFEU.[79] Actually, it may not be: there are some difficulties involved in extending the concept of discrimination in Article102 (c) away from discrimination between two third parties and towards discrimination – in a vertical integration context – between an outside third party and the dominant firm's own operations that compete with that third party.[80] Even if there are some precedents for such an extension,[81] the Commission carefully avoidsstating clearly whether discrimination as such can constitute an exclusionary abuse in its Guidance Paper on Article102 TFEU and the preceding documents[82] – let alone whether discrimination between internal operations and third-party competitors is a stand-alone abuse. Indeed, the more competitive markets are, the more difficult it is to consider that dominant firms should as a matter of principle treat third parties on the same footing as their own internal operations. There is a 'gray zone' – that is, markets where a

firm holds a dominant position without being super-dominant because serious competitive alternatives exist. A similar issue appeared before the ECJ in *TeliaSonera*, where the Court held that a dominant firm could commit a margin squeeze even if the upstream product was neither an essential facility nor a regulated offering.[83] *TeliaSonera* did not concern discrimination, so the issue outlined in this paragraph remains open.

49 Leaving aside discrimination, another way to analyse the conduct of an ISP would be to treat it as refusal to supply.[84] A refusal to supply may be actual or constructive.[85] The Commission recognizes that refusal to deal cases are more likely to occur in cases of vertical integration,[86] where, for instance, clouds would integrate with ISPs and then foreclose rival CCPs upstream (or rival ISPs downstream). However, it is acknowledged that imposing duties to supply can have an adverse effect on innovation, both on the addressee and *ex ante* on future innovators, and lead to free-riding by less efficient competitors.[87] These are real concerns, particularly in emerging markets that depend on technological progress, such as cloud computing. It would therefore be advisable for the Commission and courts to take a prudent approach to refusal-to-supply cases when ISPs integrate vertically into cloud computing. Moreover, as laid out earlier, it seems unlikely that a refusal to give access to a competing CCP will materialize, given that there seem to be strong latent network effects for clouds:[88] the value of clouds for consumers will increase by the amount of consumers on the cloud, which is only reinforced by interoperability constraints.[89]

50 Even then, in the light of existing caselaw, it is uncertain how a refusal-to-supply case initiated by an ISP and affecting a cloud service provider would fit with the caselaw, in particular the so-called 'essential facilities doctrine' established by the European courts, most notably in *Bronner* and *Microsoft*.[90] Here *Bronner* is most relevant, considering that it involved access to a delivery network. The three-pronged test that *Bronner* outlined[91] has as its main question whether the essential facility (an ISP's infrastructure) is indispensable for a service (a cloud operator) to reach its consumers, regardless of whether alternative methods of carriage fall within the same market.[92] It is in any event unlikely that a cloud service provider will be willing and able to rollout its own network to reach endusers, even if in *Bronner* the threshold for liability is set high.[93] The tremendous sunk costs that come with building network architecture do amount to 'economic obstacles' that would make it 'impossible, or unreasonably difficult' for a cloud to access endusers. However, it is possible that the existence of competition on the ISP level would outweigh this obstacle for the ECJ. This brings us back to the discussion about market definition: if one takes a broader view and considers that there are a number of ISPs available to reach a given customer – whether competition is service- or facilities-based – it seems likely that this third prong of the *Bronner* test will not be met. If, on the other hand, one emphasizes the ubiquity of cloud computing and concludes that at any given point in time and location, there is only one ISP through which a customer can be reached, then the *Bronner* test might be met.

51 Even if one factors in *Microsoft* and reads it as loosening the severity of the *Bronner* test, the outcome would not be different. In *Microsoft*, the Commission and the General Court refused to follow Microsoft's line of argumentation, which would have privileged breakthrough innovation and competition for the market at the expense of incremental innovation and competition in the market.[94] Even then, the Court insisted that it had to be proven that access to the interoperability information held by Microsoft was indispensable to compete in the workgroup server market.

b.) Under Article 101 TFEU

52 Article 101 TFEU could also apply to vertical restraints arising from agreements between an ISP and a CCP. Here again the hypothetical case would be that a CCP and an ISP enter into a preferential arrangement, whereby that CCP is the 'exclusive' or 'privileged' partner of that ISP, and other CCPs are either excluded altogether or treated less well than the exclusive or privileged CCP.

53 The key legislative document in EU competition law on vertical restraints such as these is Regulation 330/2010 on Vertical Restraints (the block exemption), together with the Guidelines on Vertical Restraints that the Commission released at the same time.[95] As often in vertical cases, the assessment of such vertical agreements to a large extent depends on the existence of market power,[96] which in turn rests on the definition of relevant markets. Regulation 330/2010 automatically exempts vertical agreements when both suppliers and buyers hold less than 30% of their respective markets,[97] but whether this threshold is met in a particular case may depend on a whether a broad market for cloud computing is defined, or whether a more narrow definition – segmented along the lines of specific services such as SaaS, PaaS and IaaS – is retained, as discussed earlier. With a broad definition, few CCPs if any will hold a market share over 30%. A narrower definition might yield market shares of more than 30% or some CCPs, in which case any vertical restraint between a CCP and an ISP will fall outside the block exemption.[98] Furthermore, if, at the ISP level, each ISP is put on a separate relevant market on the model of the termination markets, then the block exemption will not apply in any event.

54 If, for the sake of argument, the market share thresholds were not exceeded, then the CCP and ISP must avoid the 'black list' of restrictions that defeat the application of Regulation 330/2010, including resale price maintenance.[99] The most relevant provision of Regulation 330/2010, however, concerns 'non-compete obligations' which, if they last more than fiveyears, will not be covered by the exemption.[100] Should a CCP-ISP agreement contain a clause whereby the CCP becomes the exclusive CCP to be accessible over the facilities of the ISP in question, that clause should not last more than five years. It is more likely, however, that the agreement would give preferential treatment to the affiliated CCP, as opposed to competing CCPs (rather than exclude competing CCPs altogether). Such preferential treatment would not qualify as a non-compete obligation within the meaning of Article 5 of Regulation 330/2010, and accordingly it would remain covered by the block exemption. Even if Regulation 330/2010 seems to apply, it was conceived with other types of agreements in mind and does not provide a good fit for the kind of arrangement under review here.

55 If, on the other hand, a preferential CCP-ISP agreement would fall outside of Regulation 330/2010 because either of the parties held more than 30% of its respective market, then the agreement would be assessed directly under Article 101 TFEU. Under Article 101(1), what would stand out is the fact that the agreement puts other CCPs in a disadvantaged position as regards access to the ISP's customers. Whether that constitutes a restriction of competition depends, unsurprisingly, on the extent to which other CCPs are hampered when compared to a counterfactual without the preferential treatment.[101] In other words, are there sufficient alternatives to the ISP for other CCPs to reach their customers? As was discussed above, given that cloud computing services are meant to be ubiquitous, at any given location and point in time it is quite likely that a given customer using a given device can be reached only via one ISP. If that is the case, then in all likelihood a preferential treatment clause in an agreement between an ISP and a CCP would restrict competition by applying different conditions to other CCPs and putting them at a disadvantage.[102] It would then become a matter of assessing whether Article 101(3) TFEU can apply to save the preferential treatment clause.[103] At first sight, difficulties are bound to arise with at least two of the conditions of Article 101(3) TFEU: the benefits from preferential treatment are hard to identify,[104] let alone the contribution to consumer welfare via passing those benefitson to consumers.[105]

4. Internal market fragmentation and EU competition law

56 As for the third concern – namely, that the internal market could become fragmented because of differing choices made by ISPs regarding their respective platforms, thereby making it difficult for CCPs to implement cloud computing as intended – little can be done under EU competition law. Indeed, as long as ISPs do not engage in discriminatory conduct within the meaning of competition law, they should not face liability under either Article 101 or 102 TFEU – even if they hold market power. Of course, the key issue is whether there is discrimination within the meaning of competition law. As long as all CCPs have access to the facilities (and to the customers) of an ISP on the same footing, then there should be no discrimination in the eyes of competition law. That does not imply that all CCPs must have the same terms and conditions; an ISP could very well offer different terms and conditions, depending on a CCP's requirements as to capacity and quality of service (and the corresponding willingness to pay). As long as all CCPs can purchase the same capacity and quality of service for the same price, competition should not be affected (even if CCPs end up in different situations because they make different choices).[106] What is more, competition law does not prevent different ISPs from offering different formulae and tariffs for capacity and quality of service.

5. Conclusion on EU competition law

57 In the previous paragraphs, we tried to outline whether and how EU competition law could help in dealing with the three concerns identified at the outset (to the extent that intervention is warranted).

58 In the end, competition law is only partially able to address the issues of data portability/interoperability and vertical integration, both of which have an effect on the further development of cloud computing facilities in Europe. Moreover, it is doubtful whether EU competition law can be of any use to prevent fragmentation of the internal market. The previous paragraphs point to a number of issues thatdeserve further research. First of all, market definition is by no means clear at either the CCP orthe ISP level. In the latter case, in particular, the competition law analysis hinges on whether the ubiquity required for cloud computing means that ISPs find themselves in a situational monopoly, along the same lines as terminating operators for fixed or mobile voice calls. Second, the notion of discrimination within the meaning of Article 101 and 102 TFEU needs further investigation, in particular as regards discrimination between third parties and a competing subsidiary of the dominant firm, and the need for super-domi-

nance or some form of essentiality for such discrimination to be relevant for competition law purposes.

III. Network regulation

59 In the following section, we will outline to what extent European network regulation addresses the concerns outlined above relating to interoperability and data portability, vertical integration, the European internal market.

60 EU electronic communications regulation applies in tandem with EU competition law: the core regulatory mechanism applies only to operators holding significant market power (SMP) in a predefined market in the electronic communications sector. In principle, the rationale behind this mechanism is that sector-specific regulation would be progressively scaled down as the sector develops and grows more competitive, so that in the end it could be policed through competition law alone.[107]

61 The EU regulatory framework for electronic communications that was revised in 2009 is based on a platform of four main directives: the Framework Directive, the Access Directives, the Authorization Directive and the Universal Service Directive.[108] These directives are implemented at the national level, with key tasks assigned to National Regulatory Authorities (NRAs).

1. Electronic communications regulation and data portability and interoperability

62 It remains to be seen whether the regulatory framework applies to cloud computing services at all. The first question to be asked is whether cloud computing services fall under the definition scheme. The scope of the regulatory framework, as far as cloud computing is concerned, is given by the definition of 'electronic communications service', which consists' wholly or mainly in the conveyance of signals on electronic networks, including telecommunications services', yet excludes 'services providing, or exercising editorial control over, content transmitted using electronic communications networks and services'.[109] Cloud computing services thus fall under the framework inasmuch as they limit themselves to 'wholly or mainly' sending signals on electronic communications networks.[110]

63 If anything, and as described before, clouds are concerned with the IT-related services of storing and processing of data, and in most cases need ISPs to facilitate the sending and receiving of their signals on networks. It seems clear that clouds are neither communications infrastructure nor 'associated' services, and are moreover not concerned 'wholly or mainly' with conveying signals on networks. This does not, however, automatically imply that clouds are concerned with 'providing or exercising editorial control' over content transmitted. In any event, it seems unlikely that the framework for electronic communications has a direct effect on cloud computing services.

64 The Access Directive contains general interconnection requirements with corresponding powers for NRAs,[111] yet in principle those requirements concern electronic communications service providers only. As a consequence, the regulatory framework seems of little help for enhancing data portability and interoperability of clouds: only interconnection of the networks is ensured, not of the services that run on these networks. This is yet another example of the vacuity of the network/content distinction of the framework: the provisions of the Access Directive concerning interconnection in general could apply to CCPs and empower NRAs to intervene should lack of interoperability and data portability ever become so prevalent that overall welfare would be affected.

2. Electronic communications regulation and vertical integration concerns

65 The above does not mean that the electronic communications regulatory framework has no bearing at all on the concerns outlined above. Quite to the contrary: ISPs are providing an 'electronic communications service' over 'electronic communications networks', and they therefore fall fully under the regulatory framework. As a consequence of cloud computing not being an electronic communications service, however, CCPs find themselves, for the purposes of the regulatory framework, in the same position as any end-user[112] of electronic communications services and networks.

66 As we saw above, EU competition law is available in situations where an ISP would vertically integrate – through merger or agreement – with a CCP, and would subsequently deny access to competing CCPs or offer them less favourable terms and conditions than the affiliated CCP. Next to competition law, perhaps the SMP regime contained in the regulatory framework for electronic communications could be used to police such behaviour.[113]

67 As a first step for the application of the SMP regime, the relationship between CCP and ISP should fall within a relevant market that has been selected for market analysis by the NRA. The Commission takes the lead in recommending which specific markets must be analysed by NRAs. The SMP assessment procedure is based on the definition of product markets[114] and geographic markets,[115] together with particularities of telecoms markets, such as a sub-

division of service markets and access markets,[116] and wholesale and retail access markets.[117] As mentioned above, CCPs are assimilated to endusers for the purposes of electronic communications regulation so that the interaction between them and ISPs takes place on a retail market. With the second Recommendation on relevant markets, in 2007, the Commission left out all retail markets (save for access to the telephone network at a fixed location).[118] The markets that have been selected as far as ISPs are concerned – wholesale network access and wholesale broadband access – are wholesale markets, where ISPs are dealing with other ISPs that are requesting access to their network in order to provide a competing ISP service to end-users. Of course, NRAs can select additional markets to those set out in the Commission Recommendation, but only under strict circumstances, including the three-criteria test set out in the Recommendation on relevant markets.[119] So far NRAs have hardly ever been successful in selecting additional markets.

68 Accordingly, the electronic communications framework is of very limited help for concerns related to vertical integration, since the market affected by the behaviour of the ISP is not part of the set of markets to be assessed and, if necessary, regulated under the SMP procedure. The regulatory framework stands idle in addressing this potential problem.

69 If ever a market for access to ISP facilities by CCPs or endusers – for the purpose of transmitting content – were selected for assessment, then the next step would be to assess whether one or more ISPs hold significant market power (SMP) on this market. Even if the Commission states there is a difference between dominance under EU competition law and SMP – the latter would not automatically imply the former[120] – in practice NRAs are directed to rely on Article 102 TFEU case law relating to dominance in their SMP assessments. The Commission stays close to ECJ case law[121] and stresses a number of factors beyond market share to determine SMP.[122] The assessment of SMP turns around the same issues as were identified above under Article 102 TFEU.

70 Defining a firm as having SMP allows NRAs to impose ex ante obligations from the framework to prevent SMP firms from restricting competition on theirown or adjacent markets.[123] Interestingly enough, on this point the Access Directive seems to be running ahead of the SMP regime. The recent set of amendments extended the definition of 'access' in the Directive to mean the making available of facilities and/or services to another undertaking, under defined conditions, on either an exclusive or non-exclusive basis, for the purpose of providing electronic communications services, *including when they are used for the delivery of information society services or broadcast content services*.[124] (emphasis added)

71 As will be demonstrated below under electronic commerce regulation, cloud computing services are likely to fall under 'information society services'. Does this mean that the access requirements of the framework[125] can also be invoked by clouds to get access to an ISP's network? It is unclear whether this is the case. Even though it should not matter in the first place for what purpose access to electronic communications services is being used, one can wonder whetherthis actually changes anything. For a cloud service provider to require access to an ISP network, it should thus also offer electronic communications services. As EU electronic communications law now stands, EU institutions have yet to acknowledge that content providers – including CCPs – can face access problems in relation to ISPs thatare not significantly different than those of electronic communications network or service providers, and could therefore usefully be dealt with under the electronic communications regulatory framework.

3. Electronic communications regulation and internal market fragmentation

72 In many ways, the relationship between clouds and ISPs is reminiscent of the network neutrality debate, which has been on-going for some years now. The network neutrality debate concerns the question whether the original end-to-end architecture of the Internet[126] should be changed into a model of differentiated Quality of Service (QoS) as broadband services become more time-sensitive.[127] Considering the growing bandwidth needs of cloud computing, the issue of network neutrality is of particular significance in this context. It has been claimed that introducing a differentiated pricing structure for bandwidth could frustrate the emergence of cloud computing by pricing its providers out of the market.[128]

73 Priority services and differentiated prices could enable clouds to perform more reliable services. However, this will take a sizable chunk out of an ISP's bandwidth, which is a scarce resource, especially in mobile broadband. This process will affect the market for network access. The electronic communications regulatory framework approaches the issue of network neutrality mainly from a transparency perspective. The rationale behind this policy is that regulators should refrain from direct intervention into the broadband market, and rather facilitate market mechanisms by informing consumers of the network management practices of their network operators.[129] In addition, the new framework has embraced an approach that is based on NRA powers to impose minimum quality of service as a measure of last resort.[130] Perhaps more than is customary in directives, that transparency policy[131] leaves much leeway for individual Member States to implement many diffe-

rent kinds of transparency regulation into national laws.[132] Therefore, transparency regulation is likely to differ across Member States with a possible adverse effect on the internal market for broadband access.[133]

74 In addition, as was mentioned above, once differentiated QoS offerings are introduced across the EU, it is quite conceivable that the business strategies and technological implementations chosen by the various ISPs will differ significantly, leading to a fragmentation of the internal market.

75 This may be particularly troublesome for content and service providers on the Internet, including the cloud computing market. After all, the market for clouds exceeds national borders, while clouds are still dependent on ISPs as a platform to reach consumers. These network operators are bound to different jurisdictions across Europe, with different access regimes and different transparency regulation to disclose network management. Not only does this add transaction costs for clouds to adapt to a variety of network management practices and their regulation, it also becomes increasingly difficult – if not impossible – to guarantee processing power and computational speed to consumers. Clouds are especially vulnerable to this situation as their main service comprises outsourced, computationally intensive – and thus bandwidth-hungry – processes, often for corporate clients with a strong demand for reliability as they depend on clouds to operate their business.

76 Against these developments, the regulatory framework offers the possibility of standardization procedures[134] (introducing standardized technical solutions to limit the fragmentation of the market) and harmonization procedures (harmonizing diverging regulatory solutions).[135] Practical developments in the telecommunications sector seem to be pointing in the opposite direction, however.

4. Conclusion

77 Concluding overall, EU electronic communications regulation relates to cloud computing in a peculiar way. For the first two concerns – interoperability/data portability and vertical integration – the regulatory framework is comparatively less helpful than competition law because of definitional problems. Clouds may lie outside the scope of the regulatory framework, yet the ISPs clouds depend on to communicate with their users are subject to this framework. However, the relationship between CCPs and ISPs does not fall under any of the relevant markets currently selected for regulatory scrutiny under the SMP regime. We can conclude that the regulatory framework for electronic communications is of little help in mitigating these issues. As for the third concern – fragmentation of the internal market – the regulatory framework currently contributes more to fragmentation than it prevents it, though it does contain provisions that could offer a basis to tackle the concern if necessary. It now remains to be seen whether European electronic commerce regulation can be of use in addressing those concerns.

IV. Electronic commerce regulation

78 The Electronic Commerce (eCommerce) Directive relies on a different set of definitions than electronic communications regulation;instead of 'electronic communications service',[136] it concerns 'information society services' as defined in Directive 1998/34,[137] meaning 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'.[138] This definition is more appropriate for cloud computing services than those provided in the Framework Directive as it avoids a narrow definition into telecommunications terms. As such, electronic commerce regulation arguably is where cloud computing finds its 'regulatory home' – i.e. a European regulatory regime that clearly includes cloud computing within its ambit. The eCommerce Directive affects cloud computing services in mainly two ways. First, the Directive offers some clarification on jurisdictional issues for cloud computing. Second, the Directive addresses secondary liability for cloud computing services. We will analyse these two prongs of jurisdiction and secondary liability briefly below, and the results of the eCommerce Directive in relation to the concerns set out above: vertical integration, internal market fragmentation, and interoperability and data portability constraints. On the latter we can, again, be brief. The eCommerce Directive is rather vertically oriented, and does not go into interoperability and portability issues between services engaged in electronic commerce (information society services)at all.

79 The eCommerce Directive was clearly drafted with the internal market in mind,[139] and this is reflected in its efforts to streamline jurisdictional issues in the borderless world of electronic commerce. Regrettably, the eCommerce Directive has arguably created more confusion about jurisdiction than before. The Directive states that it does not 'not establish additional rules on private international law nor does it deal with the jurisdiction of Courts'.[140] Moreover, the internal market provisions of Article 3 do not limit 'the freedom of the parties to choose the law applicable to their contract'.[141] However, the preamble of the Directive seems to undercut the wording of the aforementioned articles by still insisting that 'provisions of the applicable law designated by rules of private international law must not restrict the freedom to provide information society services as

established in this Directive'.[142] In any case, the Directive does lay down some jurisdictional guidelines,[143] and prohibits Member States from restricting the freedom to provide services by information society services providers from other Member States.[144] This makes a rich caselaw on freedom of establishment applicable to cloud computing services.[145] A problem that remains, however, is that the Directive does not address restrictions on cloud computing services that are not orchestrated by Member States' governments, but by private companies, such as network operators and ISPs. As a directive, it is unlikely for the eCommerce Directive to carry a horizontal direct effect – that is, to be invoked by parties in a private lawsuit. Nevertheless, these guidelines on jurisdiction do affect the internal market dimension of cloud computing, albeit not in a very helpful way. The eCommerceDirective would have been the appropriate regulatory tool to streamline operation on the internal market in terms of interaction with ISPs for innovative online services such as cloud service providers. For such aims, however, the Directive seems rather outdated.[146]

80 Another internal market-related aspect of the eCommerce Directive is of relevance when discussing cloud computing, namely the secondary liability provisions.[147] In the Internet context, secondary liability involves the question whether service providers are liable for the actions of their users. Whether clouds fall under this safeharbour is likely to depend on the specific type of cloud computing service involved. The secondary liability provisions distinguish between 'mere conduit',[148] 'caching'[149] and 'hosting' services.[150] The hosting category is most applicable to clouds, mainly because this article in the Directive is more inclusive. It concerns services that offer storage of information, provided that service providers have no knowledge of illegal activities taking place, illegal material is removed expeditiously upon notification of such, and the provider has no authority or control over the recipient of service. However, it should be noted that the safeharbour of hosting services does not protect against injunctive relief.[151] These secondary liability provisions of the eCommerce Directive, however, have increasingly come under debate, and have recently been under attack by governments as well as courts in Europe.[152] If anything, this tendency shows that the Directive may be in need of a revision on the topic of secondary liability to better reflect the tension between the genuine inability of information society service providers to monitor users, and the legitimate attempts by governments to fight cybercrime and spam and protect citizens' privacy.[153]

81 It appears that cloud computing fits well under eCommerce Directive – at least in terms of definitions – and particularly the safe-harbour provisions will be welcomed by players in the cloud computing market. At the same time, while it is encouraging for clouds to be protected against government interference when providing their services to EU citizens, this is not exactly where the main challenges liefor the further fruition of clouds as an emerging high technology market. If clouds will become subject to interference that hampers their innovative features, such interference is more likely to be coming from players out of reach of the eCommerce Directive: ISPs. If anywhere, this intersection is where European regulation should be active. In this respect, the eCommerce Directive will not be very helpful.

82 Even though the eCommerce Directive tries to streamline issues of jurisdiction and secondary liability in the developing digital realm, the breadth of the cloud computing sector exceeds the regulatory scope of the Directive. This leads to a situation in which the available regulation is many years behind the situation on the ground, and arguably is little more than a burden on innovative services such as cloud computing. At the same time, actual potentially problematic situations – such as data portability and vertical restraints – remain unaddressed.

83 The assessment of the three regulatory regimes scrutinized above (competition law, network regulation and content regulation) will be tied together in the conclusion below.

D. Conclusion

84 This paper is intended as the first in a series that will tackle issues related to cloud computing and European law. After a thorough analysis of the phenomenon of cloud computing, the demands for cloud computing and its challenges, we have applied a specific framework of European law to clouds. Our main questions were generally how European competition law, network regulation and electronic commerce regulation relate to the emergence of cloud computing, and more specifically, how the most pressing challenges for further innovation in the cloud sector are addressed by these legal fields. Especially given the ambitious Digital 2020 agenda, is Europe ready to embrace cloud computing for the sake of a stronger and more competitive digital internal market?

85 From this initial overview, it appears that a number of issues warrant attention. We have identified three concerns that could overshadow the further development of cloud computing: interoperability and data portability concerns as between CCPs; exclusionary practices flowing from vertical integration between clouds and ISPs; and fragmentation of the internal market due to diverging business plans and technological implementations of differentiated QoS offerings by ISPs. We can tentatively conclude that, should these concerns warrant intervention, the existing European legal framework would probably not be up to the task.

86 In the end, competition law is only partially able to address the issues of data portability/interoperability and vertical integration, both of which have an effect on the further development of cloud computing facilities in Europe; it is doubtful whether it can be of any use to prevent fragmentation of the internal market. A number of issues deserve further research. First of all, market definition is by no means clear, at the CCP and at the ISP level. In the latter case in particular, the competition law analysis hinges on whether the ubiquity required for cloud computing means that ISPs find themselves in a situational monopoly, along the same lines as terminating operators for fixed or mobile voice calls. Second, the notion of discrimination within the meaning of Article 101 and 102 TFEU needs further investigation, in particular as regards discrimination between third parties and a competing subsidiary of the dominant firm, and the need for super-dominance or some form of essentiality for such discrimination to be relevant for competition law purposes.

87 EU electronic communications regulation relates to cloud computing in a peculiar way. For the first two concerns – interoperability/data portability and vertical integration – the regulatory framework is comparatively less helpful than competition law because of definitional problems. Clouds may lie outside the scope of the regulatory framework, yet the ISPs on which clouds depend to communicate with their users are subject to this framework. But the relationship between CCPs and ISPs does not fall under any of the relevant markets currently selected for regulatory scrutiny under the SMP regime. We can conclude that the regulatory framework for electronic communications is of little help in mitigating these issues. As for the third concern – fragmentation of the internal market – the regulatory framework currently contributes to fragmentation more than it prevents it, though it contains provisions that could offer a basis to tackle the concern if necessary.

88 Finally, European electronic commerce regulation does little to address the concerns that competition law and the Regulatory Framework for Telecommunications have left open. The eCommerce Directive does cover issues of jurisdiction and secondary liability for cloud computing services, but this is of limited help for the regulatory issues raised here.

89 This overall conclusion is striking, as the European Commission is intent to foster 'a new Single Market to deliver the benefits of the digital era' in its digital agenda as part of the new 2020 strategy 'for smart, sustainable and inclusive growth'.[154] Indeed, '[c]itizens should be able to enjoy commercial services and cultural entertainment across borders. But EU online markets are still separated by barriers which hamper access to pan-European telecoms services, digital services and content'.[155] New services such as cloud computing demonstrate the level of convergence between network operators and ISPs, content providers and electronic commerce services. This situation calls for a streamlined approach in which the scope and reach that services like cloud computing afford is facilitated by regulatory frameworks. Now it seems the opposite situation is in place: certain features of clouds – such as jurisdiction and content requirements – are over-regulated, while potential problematic situations that would hamper the further development of clouds – such as discrimination arising from vertical integration, interoperability and data portability – are not adequately addressed. EU competition law and electronic communications regulation concentrate on making markets work at lower levels (networks) while the internal market dimension is neglected; and eCommerce regulation, which operates at a higher level, is more focused on the internal market but ignores how the internal market is impacted not just by Member State actions, but also by the decisions of private actors on competitive markets.

90 While the European institutions seem aware of some inefficiencies that European regulation causes for the further development of cloud computing,[156] the problems we outline seem inherent to the way EU competition law, network regulation and electronic commerce regulation operate and interact. Cloud computing brings to light the limits of three legal regimes addressing converging services in the e-commerce, telecommunications and technology sector. It is rather difficult to pigeonhole clouds in one of these three regulatory disciplines. This in itself would not be problematic were competition law, network regulation and electronic commerce regulation to form a 'penumbra' that would dovetail towards an integrated approach to convergent services. This is not the case. Even though competition law and regulation of networks and electronic commerce all have a profound effect on clouds, these three legal regimes seem to fail in covering cloud computing where it really matters.

91 This article has attempted to map the status of clouds under specific fields of European law. We have drawn tentative conclusions that attempt to be more provocative than definitive. Each of the issues addressed warrants more in-depth attention respectively, and more than anything else we have aimed to lay out a research agenda on the European legal context of cloud computing for the years to come.

■

* All authors are affiliated with the Tilburg Law and Economics Center (TILEC), Tilburg Law School, Tilburg University, PO Box 90153, 5000 LE Tilburg, the Netherlands, +31 13 466 8935,jasper.sluijs@tilburguniversity.edu; pierre.larouche@tilburguniversity.edu; wsauter@nza.nl. The authors acknowledge Ilse van der Haar, Verena Weber, Sharon Strover, Christopher Millar, Ian Walden, Damien Geradin and an anonymous reviewer for helpful comments on this article, and express thanks to LyndseyThomsin and Maurits Oskam for research assistance. Whereas this paper

forms part of a TILEC research program financially supported by the Microsoft Corporation, but the analysis and opinions voiced here are those of the authors alone.

1 *Battle of the clouds:Cloud computing,* 381 THE ECONOMIST 13; 71 (17 October 2009).

2 P. Jaeger, J. Lin &J. Grimes, *Cloud Computing and Information Policy: Computing in a Policy Cloud?*, 5(3) JOURNAL OFINFORMATION TECHNOLOGY AND POLITICS 35 (2008).

3 A. Odlyzko, *Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets*, 8 REVIEW OF NETWORK ECONOMICS 40 (2009), p. 57.

4 I. Van der Haar, *The Principle of Technological Neutrality: Connecting EC Network and Content Regulation,* PhD Thesis, Tilburg University 2008; P. Larouche, *Communications Convergence and Public Service Broadcasting*, (2001) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=832444>, accessed 13 August 2011.

5 *Digital Agenda: Commission outlines action plan to boost Europe's prosperity and well-being*, Press Release IP/10/581 (19 May 2010),<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/581&format=HTML&aged=0&language=EN&guiLanguage=en>, accessed 10 December 2011.

6 D. Svantesson & R. Clarke, *Privacy and consumer risks in cloud computing*, 26 COMPUTER LAW & SECURITY REVIEW 391–397 (2010); Paolo Balboni, *Data Protection and Data Security Issues Related to Cloud Computing in the EU*, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661437>, (last visited Mar 13, 2012); J. Bowen, *Legal Issues in Cloud Computing*, in R. Buyya,J. Broberg, A. Goscinski (eds.) CLOUD COMPUTING: PRINCIPLES AND PARADIGMS 593–613 (2011); Udo Helmbrecht, *Data protection and legal compliance in cloud computing*, 34 DATENSCHUTZ UND DATENSICHERHEIT - DUD 554–556 (2010).

7 M. Iansiti, *Principles That Matter: Sustaining Software Innovation from the Client to the Web*, 09 HARVARD BUSINESS SCHOOL TECHNOLOGY & OPERATIONS MGT. UNIT WORKING PAPER (2009), p. 3, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1420196>, accessed 9 December 2009.

8 W. Kim, *Cloud Computing: Today and Tomorrow*, 8 JOURNAL OF OBJECT TECHNOLOGY 65 (2009).

9 S. Lohr, *Google and I.B.M. Join in 'Cloud Computing' Research*, THE NEW YORK TIMES (8 October 2007) <http://www.nytimes.com/2007/10/08/technology/08cloud.html>, accessed 10 December 2011.

10 Oracle CEO Larry Ellison remarked that '[t]he interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements.' C. Boulton, *Oracle CEO Larry Ellison Spits on Cloud Computing Hype*, EWEEK (29 September 2008) available at<http://www.eweek.com/c/a/IT-Infrastructure/Oracle-CEO-Larry-Ellison-Spits-on-Cloud-Computing-Hype/>.

11 P. Jaeger, J. Lin & J. Grimes (n 2) p. 280; R.C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, JOHN M. OLIN LAW & ECONOMICS WORKING PAPER (2008), p. 6, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1151985>, accessed 9 December 2009; C. Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 2 JOURNAL OF TELECOMMUNICATIONS AND HIGH TECHNOLOGY LAW 360 (2010), p. 362.

12 S. Bandyopadhyay et al, *Cloud Computing: The Business Perspective*, (2009), p. 3, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1413545 >, accessed 13 August 2011.

13 P. Mell& T. Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology (NIST) (January 2011) Special Publications 2.

14 For a technical paper on virtualization in cloud computing, see M. Vouk, *Cloud Computing: Issues, Research and Implementations*, 16(4) JOURNAL OF COMPUTING & INFORMATION TECHECHNOLOGY 235 (2009) <http://cit.srce.hr/index.php/CIT/article/view/1674>, accessed 10 December 2009.

15 Thereby dispelling the cyclical model alluded to in n 10. It is accurate that cloud computing marks a break from the heavier user-side architecture typical of server-client computing, towards an architecture reminiscent of mainframe-terminal computing. At the same time, mainframe-terminal computing did not comprise an element of terminal mobility: delocalization/ubiquity sets cloud computing apart from mainframe-terminal architectures.

16 M. Donahue & D. Ypsilanti, *Cloud Computing and Public Policy: Briefing Paper for the ICCP Technology Foresight Forum,* (2009), p. 3 <http://www.oecd.org/dataoecd/39/47/43933771.pdf>, accessed 13 August 2011; R. Whitt, *Evolving Broadband Policy: Taking Adaptive Stances to Foster Optimal Internet Platforms*, 17 COMMLAW CONSPECTUS 417 (2009), pp. 446-448. For a technical exposé on the mobility of cloud computing, see X. Li, H. Zhang & Y. Zhang, *Deploying Mobile Computation in Cloud Service*, Lecture Notes in COMPUTER SCIENCE (2009), pp. 301-311.

17 M. Dodani, *Keeping Enterprises' Head Above The Clouds!,* 8(1) J OBJECT TECH 55 (2009), p. 59; S. Bandyopadhyay et al (n 11).

18 B.J. Pine, *Mass Customization: The New Frontier in Business Competition,* Harvard Business School Press 1993, p. 48. The term was originally coined by S. Davis, *Future Perfect,* Addison Wesley 1987.

19 Thereby fitting the definition of mass customization proposed by R.B. Chase, N.J. Aquilano & R.F. Jacobs, *Operations Management for Competitive Advantage*, McGraw-Hill 2006, namely 'effectively postponing the task of differentiating a product for a specific customer until the latest possible point in the supply network'.

20 B.J. Pine (n 17), p. 48.

21 A number of firms are actually specializing in the customization of cloud computing services, in symbiosis with the cloud computing provider: see, for instance, the list of 'Global Solution Providers' of Amazon Web Services at <http://aws.amazon.com/solutions/global-solution-providers/>, accessed 17 April 2011.

22 This has so far kept larger customers from fully embracing cloud computing: see S. Lohr, *The Business Market Plays Cloud Computing Catch-Up*, THE NEW YORK TIMES(14 April 2011) B1.

23 P. Jaeger, J. Lin & J. Grimes (n 2) p. 270; M. Dodani(n 16) p. 60.

24 Y. Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, Yale UP 2006, pp. 59-90.

25 W. Kim (n 7) p. 66; S. Bandyopadhyay et al (n 11).

26 D.Lippold&P. Stryszowski, *Innovation in the Software Sector* (2009), pp. 39-40, <www.oecd.org/sti/innovation/software>, accessed 13 August 2011; Picker (n 10) p. 6; P. Jaeger, J. Lin & J. Grimes (n 2) p. 271; W. Kim(n 7) p. 66.

27 This has prompted some commentators to argue for a regulatory approach to cloud computing that mimics the regulation of utilities. It should be noted that this is based on assumptions of a natural monopoly with regulated retail rates because competition is not available to keep prices down. This model should not be considered useful for cloud computing given that even in the traditional utilities sectors such as electronic communications, energy and transport it no longer applies. See H. Demsetz, *Why Regulate Utilities*, 11 J L& ECON 55 (1968) for the seminal article criticizing the natural monopoly argument for regulating utilities;see also M. Loeb &W. Magat, *A Decentralized Method for Utility Regulation*, 22(2) J L& ECON 399 (1979).

28 P. Mell& T. Grance (n 12) p. 2.

29 Ibid.

30 J.D. Lasica, *Identity in the Age of Cloud Computing: The Next-Generation Internet's Impact on Business, Governance and Social Interaction*, The Aspen Institute 2009, p. 7.

31 For the sake of simplicity, we assume that the enduser is a single person. Of course, in the majority of cases, the customer will be a firm, meaning that the endusers will be a set of individuals working for that firm and gaining access to cloud computing services as part of their employment.

32 M. Donahue & D. Ypsilanti (n 15), pp. 20-28; M. Iansiti (n 6) pp. 9-14; Picker (n 10), pp. 8-11.

33 S. Bandyopadhyay et al., (n 11), p. 31; D. Lippold& P. Stryszowski (n 25), pp. 146-152.

34 'Battle of the Clouds' (n 1), p. 13.

35 Google has recently announced thebuilding of its own fiber architecture in the US. See M. Ingersoll & J. Kelly, *Thinking Big with a Gig: Our Experimental Fiber Network*, Google Policy Blog (2010),<http://googleblog.blogspot.com/2010/02/think-big-with-gig-our-experimental.html>, accessed 13 August 2011.

36 Exceptions are conceivable, such as when a customer is reachable through two live devices, linked to different ISPs, or when the device can easily jump from one ISP to another. Nevertheless, for the sake of analysis, these remain exceptional situations and it is safe – at least in the current state of technology – to assume that a customer is reachable through one and only one ISP_{cust} at any given time and location.

37 In any event, a CCP will probably serve many customers, who can be on different ISP_{cust}; corporate customers will also require that many or all their employees can use cloud computing services through whichever ISP_{cust} they may be linked to.

38 M. Armstrong, *Competition in Two-Sided Markets*, 37 RAND J ECON668 (2006); J. Rochet & J. Tirole, *Platform Competition in Two-Sided Markets*, 1 J EEA 990 (2003).

39 Such evolution is at the heart of the debate on 'network neutrality' thathas been raging for years now, first in the USA and now in the EU and worldwide. J.P. Sluijs, *Network Neutrality Between False Positives andFalse Negatives: Introducing a European Approach to American Broadband Markets*, (2010) 62 FEDERAL COMMUNICATIONS LAW JOURNAL 77 (2010).

40 An ISP, however, may lack in reach to provide on their own the ubiquity and mobility that cloud computing affords. Outside of the reach of its own network, an ISP providing cloud computing services would be as dependent as any other CCP on having access to the networks of other ISPs.

41 This could occur if a given CCP would have such a strong brand that it would be a 'must-have' provider on a given platform. An ISP could very well unilaterally decide to give preferential treatment to that CCP, under certain circumstances.

42 A. Odlyzko (n 3), p. 57.

43 J. Rochet& J. Tirole (n 37).

44 AT&T and Verizon.

45 T-Mobile and Sprint, with T-Mobile and AT&T planning to merge.

46 As set out by the Commission Decision 2003/707 in *Deutsche Telecom* (Case COMP/C-1/37.451, 37.578, 37.579) [2003] OJ L263/9, para. 54. The Commission was confirmed on this point by the ECJ, Case C-280/08, *Deutsche Telekom,* [2010] Judgment of 14 October 2010, not yet reported.

47 Council Directive 140/2009/EC of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services;2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities;and 2002/20/EC on the authorisation of electronic communications networks and services [2009] OJ L337/37, recital 5: 'The aim is progressively to reduce ex-ante sector specific rules as competition in the markets develops and, ultimately, for electronic communications to be governed by competition law only'.

48 See generallyP. Larouche, *Competition Law and Regulation in European Telecommunications*, Hart 2001; P. Nihoul& P. Rodford (eds), *EU electronic communications law: competition and regulation in the European telecommunications market*, Oxford UP 2004; K. Coates & W. Sauter, 'Communications (Telecoms, Media and Internet)' in J. Faull and A. Nikpay (eds), *The EC Law on Competition*, Oxford UP 2007.

49 See I.Van der Haar (n 4), pp. 135-138.

50 Ibid.

51 Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1.

52 J. Hills and M. Michalis, *Restructuring Regulation: Technological Convergence and European Telecommunications and Broadcasting Markets*, 7 REV OF INTL POL ECON 434 (2000).

53 Consolidated Version of the Treaty on European Union [2008] OJ C115/1, arts. 101 and 102.

54 Commission Notice on the definition of relevant market for the purposes of Community competition law [1997] OJ C372/5, paras 7-24. It should be noted that the Commission's approach in the Notice departs slightly from the method employed by the Court of Justice in*Commercial Solvents*, for instance,which put emphasis on demand substitution. ECJ, Joined Cases 6 and 7-73,*IstitutoChemioterapicoItalianoS.p.A. and Commercial Solvents Corporation v Commission*, [1974] ECR 223.

55 Commission Decision 92/163/EEC relating to a proceeding pursuant to Article 86 of the EEC Treaty *(Tetra Pak II)* [1992] OJ L72/1, para. 94.

56 Even if in a number of locations (especially in the new Member States) there is evidence that mobile and fixed communications are competing intensely with one another;Commission 'Explanatory Note to the Recommendation on Relevant Product and Service Markets (Second Edition)' SEC (2007) 1483 final 20.

57 Recommendation 2003/311 of 11 February 2003 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21 [2003] OJ L114/45.

58 As when roaming on mobile networks.

59 Commission Notice on the definition of the relevant market for the purposes of Community competition law [1997] OJ C372/5, para. 8: 'relevant geographic markets' are defined as follows: 'The relevant geographic market comprises the area in which the undertakings concerned are involved in the supply and demand of products or services, in which the conditions of competition are sufficiently homogeneous and which can be distinguished from neighbouring areas because the conditions of competition are appreciably different in those area'.

60 Exact's accounting software suite is a good example of this local strategy – the company is established in 125 countries individually, and offers its products in 40 different languages.

61 See Commission Notice (n 58), para. 90.

62 For instance, ECJ, Case T-201/04, *Microsoft Corp. v Commission,* [2004] ECR II-4463, para. 319.

63 Even though exploitative abuses are rarely prosecuted in practice. For a critical discussion of this phenomenon, see B. Lyons, *The Paradox of the Exclusion of Exploitative Abuse*, 08(1) CCP WORKING PAPER (2007) <http://ssrn.com/abstract=1082723>, accessed 13 August 2011.

64 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 [2009] OJ C45/7.

65 SeeCommission Guidance, ibid., paras 11-12. The SSNIP test is usually employed to establish geographic and product markets, but the test has also increasingly been applied to measure market power (in which case the hypothetical monopolist is replaced by the defendant, and the inquiry bears on movements between firms as a results of price increases).

66 ECJ, Case 27/76, *United Brands v Commission,* [1978] ECR 207.

67 ECJ, Case 85/76, *Hoffmann-La Rochev Commission,* [1979] ECR 461.

68 'Battle of the Clouds' (n 1), p. 13.

69 Commission recommendation (n 56), p. 10.

70 Commission Guidance (n 63), para. 19.

71 Commission Guidance (n 63), paras 32-46 (exclusive dealing); paras 47-62 (tying and bundling); paras 63-74 (predation); paras 75-90 (refusal to deal and margin squeeze).

72 ECJ, Case T-340/03, *France Télécom SA v Commission,* [2007] ECR II-107, para. 197.

73 P. Jaeger, J. Lin & J. Grimes (n 2); A. Odlyzko (n 3).

74 Following the judgment of the ECJ, CaseT-210/01, *General Electric v Commission,* [2005] ECR II-5575 and the new Commission Guidelines on the assessment of non-horizontal mergers [2008] OJ C265/6, it is more likely that vertical mergers would be allowed to go through, knowing that possible anti-competitive practices arising as a consequence of vertical integration could be caught by Articles 101 or 102 TFEU.

75 See, for instance,*Wanadoo Interactive*, where the Commission established the French DSL provider Wanadoo to have held average market shares of 50 to 60%. Commission Decision, *Wanadoo Interactive* (Case COMP/38.233), [2003] para. 389.

76 Essentially the incumbent (or its cable-base rival) or whoever has a large enough share of the mobile market.

77 See ECJ, C-202/07 P, *France Telecom v Commission,* [2009] ECR I-02369 (referring to COMP/38.233, WanadooIneractive, n 74).

78 Commission Decision, *WanadooEspaña vTelefónica* (Case COMP/38.784), [2008] OJ C83/6.

79 This provision lists, as an example of abusive conduct, 'applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage'.

80 P. Larouche (n 47), pp. 218-231.

81 Ibid.

82 It can be argued that Art. 102(c) TFEU was meant to cover exploitative discrimination (e.g. first-degree price discrimination).

83 ECJ, Case C-52/09, *TeliaSonera*, [2011]Judgment of 17 February 2011, not yet reported.

84 Cf. ECJ, Case C-7/97, *Oscar Bronner v MediaprintZeitungs- und Zeitschriftenverlag and others,* [1998] ECR I-07791; ECJ, Joined cases C-241/91 P and C-242/91 P, *Radio TelefisEireann (RTE) and Independent Television Publications Ltd (ITP) v Commission (Magill),* [1995] ECR I-00743; ECJ, Case C-418/01, *IMS Health v NDC Health,*[2004] ECR I-5039; ECJ, T-201/04, *Microsoft* (n 61).

85 I.e. the terms of access offered by an ISP are such that the CCP is denied access for all intents and purposes.

86 Commission Guidance (n 63), para. 76.

87 Ibid. para. 75.

88 P. Jaeger, J. Lin & J. Grimes (n 2), p. 280.

89 D. Lippold& P. Stryszowski (n 25), pp. 146-152.

90 For a thorough analysis of the essential facilities case law in relation to network neutrality and particularly *Microsoft*, see K.Maniadaki, *Network Neutrality in the EU:Is There Scope for the Application of Competition Rules?*, THE 38TH RESEARCH CONFERENCE ON COMMUNICATION, INFORMATION AND INTERNET POLICY, WASHINGTON, DC, (October 2010), pp. 17-18.

91 The test in *Bronner* builds on the previous standard set in *Magill* (n 83) by stipulating that a refusal to deal by an essential facility needs to meet the (*Magill*) criteria of (1) eliminating all competition downstream, and (2) not being objectively justified, plus the new criterion of (3) the essential facility in question being indispensable for a third party to offer its service;*Bronner* (n 83) para 41. For a legal analysis of this case, see L. Evrard, *Essential Facilities in the EU: Bronner and Beyond*, 10 COLUMBIA J EUR L 491 (2004).

92 ECJ, C-7/97, *Bronner* (n 83), para. 43.

93 Ibid. para. 44.

94 See P. Larouche, *The European Microsoft case at the crossroads of competition policy and innovation*, 75 ANTITRUST LJ 933 (2009).

95 Commission Regulation 330/2010 of 20 April 2010 on the application of Article [101(3) TFEU] to categories of vertical agreements and concerted practices [2010] OJ L102/1. See also the Commission Guidelines on Vertical Restraints [2010] OJ C130/1. The seminal case in which vertical restraint complaints were pursued through an Art. 101 procedure was *Grundig*;see ECJ Cases 56 and 58/64, *Consten and Grundig v Commission* [1966] ECR 299.

96 See Vertical Guidelines, ibid., paras 88-99 for a more specific outline of market definition for the purpose of applying Regulation 330/2010.

97 Regulation 330/2010 (n 94), Art. 3. Note that in addition, individual exemptions are available based on the application of the Guidelines on Vertical Restraints in the context of Article 101(3) TFEU.

98 *AMR Research Ranks Salesforce.com as Market Share Leader with 44% of Hosted Customer Management Market* (2006),<http://www.salesforce.com/company/news-press/press-releases/2006/08/060820.jsp>, accessed 8 April 2010.

99 Regulation 330/2010 (n 94), Art. 4. In principle, a CCP-ISP agreement should not involve resale price maintenance, unless the ISP would act as a distributor or reseller of cloud computing services (as opposed to a mere agent for the CCP). Note that the maximum price setting is nonetheless allowed under the block exemption, and minimum retail price maintenance can still be allowed under an Art.101(3) efficiency defence. Commission Guidelines (n 94), paras 223-229. Recall that resale price maintenance as a whole is no longer illegal in the US;see *Leegin Creative Leather Products, Inc. v PSKS, Inc.* 551 U.S. 877 (2007). For a comparative analysis, see J. Cooper et al., *A Comparative Study of United States and European Union Approaches to Vertical Policy,* 13 GEORGE MASON LREV 289 (2006).

100 Regulation 330/2010 (n 94), Art. 5(1)(a). If the non-compete obligation can be severed from the rest of the agreement, then the rest of the agreement remains covered by the block exemption. If a non-compete clause falls outside of the block exemption, it is likely to be objectionable under Art. 101 TFEU, unless a strong justification can be put forward under Art. 101(3).

101 Regulation 330/2010 (n 94), para. 97.

102 A situation thatcomes close to the case listed at Art.101(1)(d) TFEU.

103 Or the whole agreement if the preferential treatment clause cannot be severed from it.

104 Even when taking into account the extensive list of benefits at para. 107 of the Vertical Guidelines (n 94).

105 See Commission Guidelines on the application of Art.[101(3) TFEU] [2004] OJ C101/97, para. 83 and ff.

106 Unless the ISP has set up its tariffs in such a way as to indirectly discriminate in favour of one CCP over the others.

107 On the relationship between sector-specific regulation and competition law under the 2002 framework, see P. Larouche, *A closer look at some assumptions underlying EC regulation of electronic communications*, 3 J NETWORK IND'S 129 (2002).

108 These are Directive 2002/19 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) [2002] OJ L108/7; Directive 2002/20 on the authorisation of electronic communications networks and services (Authorisation Directive) [2002] OJ L108/21; Directive 2002/21 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L108/33; Directive 2002/22 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) [2002] OJ L108/51;to which one should add Directive 2002/77 on competition in the markets for electronic communications networks and services [2002] OJ L249/21. These separate directives were amended in the course of the 2007 review by Directive 2009/136 amending Directive 2002/22, Directive 2002/58 and Regulation 2006/2004 (Citizens' Rights Directive) [2009] OJ337/11 and Directive 2009/140 (n 46). These amending directives were complemented by Council Regulation 1211/2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office [2009] OJ L337/1.

109 Art. 2(c) Framework Directive, ibid. For the purposes of the discussion, we leave aside the definitions of 'electronic communications networks', as well as 'associated facilities' and 'associated services'.

110 From the wording of the Directive it may be unclear what this 'wholly or mainly' criterion exactly entails, yet communication from the Commission during the 1999 review process that resulted in the 2002 Regulatory Framework – whose contours are still present today – sheds more light on what is covered under the framework and what is not. A distinction is made between communications infrastructure and 'associated services' such as access services – which both fall under the framework – and 'services provided over networks' such as broadcasting and electronic banking – which fall outside the scope of the framework. See Commission, 'Towards a New Framework for Telecommunications and Associated Services: The 1999 Communications Review' [1999] COM (99) 539 final, p. 21.

111 See Access Directive of 2009/140/EC (n 107), Art. 5(1):'National regulatory authorities shall ... encourage and where appropriate ensure, in accordance with the provisions of this Directive, adequate access and interconnection, and the interoperability of services, exercising their responsibility in a way that promotes efficiency, sustainable competition, efficient investment and innovation, and gives the maximum benefit to end-users.'

112 As defined in Framework Directive (n 107), Art. 2(n).

113 SMP is established if '[an undertaking] either individually or jointly with others, ... enjoys a position equivalent to dominance, that is to say a position of economic strength affording it the power to behave to an appreciable extent independently of competitors, customers and ultimately consumers.' Framework Directive **2009/140/EC** (n 107), **para. 14(2).** SMP inquiry is used as 'an overall forward-looking assessment of the structure and the functioning of the market under examination' and does not look for cartels or abuse cases per se. Commission guidelines on market analysis and the assessment of significant market power under the Community regulatory framework for electronic communications networks and services [2002] OJ C165/6 8. Note that the markets can only be subjected to ex ante regulation according to the SMP procedure when three cumulative criteria are met: 1) the presence of high and non-transitory barriers to entry; 2) a market structure not tending towards effective competition soon; and 3) merely competition law would not adequately address the market failure(s) concerned. Commission Recommendation (n 56).

114 Commission Guidelines (n 112), paras 44-54.

115 Ibid., paras 55-60.

116 Ibid., para. 64.

117 Ibid., para. 67.

118 Commission Recommendation 2007/879/EC of 17 December 2007 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services [2007] OJ L344/65, Annex I.

119 Framework Directive 2009/140 (n 46), para. 15(3).

120 Commission Guidelines, Commission Guidelines (n 112), paras 30-31. At the same time, the Commission is not entirely consistent in distinguishing between dominance under competition law and the SMP process: Art. 14(2) of the Framework Directive (n 46) states that SMP is 'equivalent' to dominance.

121 Commission Guidelines (n 112), paras 75.

122 Such as 'overall size of the undertaking, control of infrastructure not easily duplicated, technological advantages or superiority, absence of or low countervailing buying power, easy or privileged access to capital markets/financial resources, product/services diversification (e.g. bundled products or services), economies of scale, economies of scope, vertical integration, a highly developed distribution and sales network, absence of potential competition, barriers to expansion';ibid., para. 78.

123 Ibid., para. 16.

124 See Access Directive of **2009/140/EC** (n 46), Art. 2(a).

125 Ibid., Art. 2(a): 'access to network elements and associated facilities, which may involve the connection of equipment, by fixed or non-fixed means (in particular this includes access to the local loop and to facilities and services necessary to provide services over the local loop); access to physical infrastructure including buildings, ducts and masts; access to relevant software systems including operational support systems; access to information systems or databases for pre-ordering, provisioning, ordering, maintaining and repair requests, and billing; access to number translation or systems offering equivalent functionality; access to fixed and mobile networks, in particular for roaming; access to conditional access systems for digital television services and access to virtual network services.'

126 For a technical definition of the end-to-end principle, see J. H. Saltzer, D. P. Reed & D. D. Clark, *End-to-end arguments in system design*, (1984) 2(4) ACM TRANSACTIONS ON COMPSYS 288 (1984).

127 On network neutrality in Europe, see e.g. J.P. Sluijs (n38); F. Chirico, I. Van der Haar&P. Larouche, *Network Neutrality in the EU*, TILEC DISCUSSION PAPER No. 2007/30 (2007); D. Sieradski&W. Maxwell, *The FCC's network neutrality ruling in the Comcast Case: towards a consensus with Europe?*, 74 COMM'S & STRAT'S 73 (2008); Valcke et al., *Guardian knight or hands off: the European response to network neutrality. Legal considerations on electronic communications reform*, 72 COMM'S & STRAT'S 89 (2008).

128 P. Jaeger, J. Lin &J. Grimes (n 2), p. 13.

129 Commission, 'Commission Staff Working Document: Impact Assessment', SEC (2007) 1472 95-96.

130 Art.22(3) of the new Universal Service Directive (n 107).

131 The new Consumer Protection Directive states the following: 'Member States shall ensure that national regulatory authorities are able to oblige undertakings providing public electronic communications networks and/or publicly available electronic communications services to publish transparent, comparable, adequate and up-to-date information on applicable prices and tariffs, on any charges due on termination of a contract and on standard terms and conditions in respect of

access to, and use of, services provided by them to end-users and consumers. 'These undertakings should also inter aliainform subscribers of any change to conditions limiting access to and/or use of services and applications, where such conditions are permitted under national law in accordance with Community law;and,provide information on any procedures put in place by the provider to measure and shape traffic so as to avoid filling or overfilling a network link, and on how those procedures could impact on service quality.' Directive 2009/136/EC, ibid.,Art. 21(3)(c) and (d).

132 National Regulatory Authorities (NRAs) 'may specify additional requirements regarding the form in which such information' is provided transparently; are to encourage 'the provision of comparable information to enable end-users and consumers to make an independent evaluation of the cost of alternative usage patterns'; and should encourage '[publishing of] comparable, adequate and up-to-date information for end-users on the quality of their services',while the Directive leaves to the Member States to determine means to pursue this transparency, either through NRAs, third parties or otherwise. Ibid. Art. 21(1); Arts. 21(2) and 22(1).

133 See J.P. Sluijs, F. Schuett, & B. Henze, *Transparency regulation in broadband markets: Lessons from experimental research*, 35 TELECOMMUNICATIONS POLICY 592 (2011), for an experimental study on the feasibility of transparency regulation in broadband.

134 Framework Directive (n 46), Art. 17.

135 Ibid., Art. 19. The Commission can also try to achieve some measure of harmonization via its supervisory power over NRA decisions in SMP procedures, pursuant to Arts. 7 and 7a.

136 Ibid., Art. 2(c).

137 Council Directive 98/34/EC of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services [1998] OJ L204/37, last amended by Council Directive (EC) 2006/96/EC [2006] OJ L363/81.

138 Ibid., Art. 1(2).

139 Ibid., rec. 5 'The development of information society services within the Community is hampered by a number of legal obstacles to the proper functioning of the internal market which make less attractive the exercise of the freedom of establishment and the freedom to provide services';*and* at rec. 6 '[T]hese obstacles should be eliminated by coordinating certain national laws and by clarifying certain legal concepts at Community level to the extent necessary for the proper functioning of the internal market'.

140 Ibid., Art. 1(4).

141 Ibid., at annex: derogations from Art. 3.

142 Ibid., rec. 23.

143 The place of establishment of an information society service is not necessarily the place where supporting technology for the economic activity pursued is located, but rather the place where the actual economic activity is pursued. If there are multiple such places, the place from where the service is provided is determined to be the place of establishment. If again there are many such places, the place of establishment is deemed to be where the firm's centre of activities is located – without specifying what this 'centre' is supposed to entail.

144 eCommerce Directive (n 136), Art. 3(2). The exemptions to this should pass a cumulative test of being (i) necessary for public policy, public health, public security, or consumer protection reasons; (ii) directed at an information society service that endangers any of the values under (i); and (iii) proportionate to those objectives. Ibid., Art. 3(4)(a). Moreover, these measures can only be taken if the Member State in which the service is established has failed to do so, and the Commission has been notified, ibid., Art. 3(4)(b).

145 Recital 19 provides an elaborate test analogous to case law in freedom of establishment cases; Treaty on the Functioning of the European Union (n 52), Arts. 49-55. For relevant case law, see ECJ, Case C-70/95, *Sodemare and others v RegioneLombardia,*[1997] ECR I-3395 *and* ECJ, Case C-55/94, *Gebhard v Consiglio dell'OrdinedegliAvvocati e Procuratori di Milano,* [1995] ECR I-4165.

146 M. Hellner, *The Country of Origin Principle in the E-Commerce Directive: AConflict with Conflict of Laws?,*2 EUR REV PRIV L 193 (2004).

147 eCommerce Directive (n 136), Arts. 12-14.

148 Ibid.,Art. 12.

149 Ibid.,Art. 13.

150 Ibid.,Art. 14.

151 Ibid.,Art. 14(3).

152 The Italians seem particularly concerned with the eCommerce Directive's safe harbour provisions, judging by a recent proposed law that holds streaming video portals such as YouTube liable for copyright infringement by endusers. See D. Flynn, *Internet companies voice alarm over Italian law*, (26 January 2010),<http://www.reuters.com/article/idUSLDE60E28B20100126>, accessed 13 August 2011. Moreover, an Italian district court judge ignored the eCommerce Directive when ruling against Google in a privacy violation case involving (again) YouTube footage, and even sentenced Google executives with suspended imprisonment. R. Donadio, *Larger Threat Is Seen in Google Case*, THE NEW YORK TIMES (24 February 2010), available at <http://www.nytimes.com/2010/02/25/technology/companies/25google.html?_r=1>, accessed 13 August 2011.

153 On the intersection of privacy law and electronic commerce, see C.Kuner, *Beyond Safe Harbor: European Data Protection Law and Electronic Commerce*, 35 INTL LAWYER 79 (2001).

154 Commission press release (n 5).

155 Ibid.

156 See, e.g., European Commission, Cloud Computing: Public Consultation Report (December, 2011) available at <http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf>, accessed 13 March 2012.

Global Standards: Recent Developments between the Poles of Privacy and Cloud Computing

by **Philipp E. Fischer**, Munich, LL.M. (IP, London/Dreseden), Data Protection Officer & -Auditor (TÜV)

Abstract: The development of the Internet has made it possible to transfer data 'around the globe at the click of a mouse'.[1] Especially fresh business models such as cloud computing, the newest driver to illustrate the speed and breadth of the online environment, allow this data to be processed across national borders on a routine basis. A number of factors cause the Internet to blur the lines between public and private space: Firstly, globalization and the outsourcing of economic actors entrain an ever-growing exchange of personal data. Secondly, the security pressure in the name of the legitimate fight against terrorism opens the access to a significant amount of data for an increasing number of public authorities. And finally, the tools of the digital society accompany everyone at each stage of life by leaving permanent individual and borderless traces in both space and time. Therefore, calls from both the public and private sectors for an international legal framework for privacy and data protection have become louder. Companies such as Google and Facebook have also come under continuous pressure from governments and citizens to reform the use of data. Thus, Google was not alone in calling for the creation of 'global privacystandards'.[2] Efforts are underway to review established privacy foundation documents. There are similar efforts to look at standards in global approaches to privacy and data protection. The last remarkable steps were the Montreux Declaration, in which the privacycommissioners appealed to the United Nations 'to prepare a binding legal instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights'. This appeal was constantly repeated, lastly in 2010 at the 33rdInternational Conference of Data Protection and Privacy Commissioners. In a globalized world, free data flow has become an everyday need. Thus, the aim of global harmonization should be that it doesn't make any difference for data users or data subjects whether data processing takes place in one or in several countries. Concern has been expressed that data users might seek to avoid privacy controls by moving their operations to countries which have lower standards in their privacy laws or no such laws at all. To control that risk, some countries have implemented special controls into their domestic law. Again, such

Keywords: International data transfer, international legal framework, global privacy standards, cloud computing, data protection, privacy rights infringement, data controller, data processor, European Data Protection Directive, EU-DPD, safe harbor, Standard Contractual Clauses, adequacy, adequate level of data protection, APEC, OECD, UN, accountability, Binding Corporate Rules

Recommended citation: Philipp E. Fischer, Global Standards: Recent Developments between the Poles of Privacy and Cloud Computing, 3 (2012) JIPITEC 1, para 33.

A. Introduction

1 During the 2012 CeBIT IT fair this March in Hannover, René Obermann, CEO of Deutsche Telekom, highlighted that 'the present PC architecture is outdated; the post-PC era has begun. [...] We want to play an important role in the ecosystem cloud'.[3] This is not surprising, given that Germany's BITKOM[4] association recently issued a study finding that the annual turnover in cloud computing businesses in Germany will end up at around 5.3 billion euros in 2012, a steep increase of 50% compared with the previous year. The prediction for 2016 is even about 17 billion euros per year, a third of it through business-to-private consumer relations. Market analyst 'Gartner' recently determined the global returns of cloud computing in 2012 at 77 billion euros.[5]

2 Big market players are now pushing forward their own business models for cloud computing and installing new data centres worldwide. This dramatically increases the quantity – but not necessarily the quality – of cloud computing services offered to consumers. This development leads to a large amount ofdata transfer' around the globe at the click of a mouse',[6] data which is to be processed across national borders on a routine basis.

3 The shady side of these new opportunities for the global web community has been addressed not only by Germany's chancellor Angela Merkel – 'The more natural technologies become, the more important is the necessity of trust'[7] –but also by Viviane Reding, Commissioner of the European Union (EU):

> *Let's take cloud computing: storing information in the cloud holds much economic promise and many consumer benefits. Cloud computing is becoming one of the backbones of our digital future. However, new technologies also raise challenges for policy makers. A cloud without robust data protection rules is not the sort of cloud we need.*[8]

4 Reding went on to say that 'privacy nowadays has become a moving target: new risks need better legal remedies'.[9]

5 Few companies take data protection issues in cloud computing seriously. The Deutsche Telekom seems to understand that in order to serve the B2B market with cloud computing services, it needs some hard work on data protection measures and politics of trust. According to Mr. Obermann, 60 out of 90 data centres outside of Germany already do comply with all technical standards under German law. The negative example to prove the opposite is – again – Google: even after having suffered strong criticism because of its newest privacy policy, Eric Schmidt, a member of Google's board of directors, didn't say a word at the CeBIT fair about data protection in cloud computing surroundings; he preferred to praise the neutrality of the Net.

6 To tackle concerns of privacy and data protection in the cloud, calls from both the public and private sectors for an international legal framework for privacy and data protection have become louder. Companies such as Google and Facebook have come under continuous pressure from governments and citizens to reform the use of data.

7 Efforts are underway to review the established privacy and data protection legal framework:

8 The first remarkable step was the Montreux Declaration,[10] in which the privacy commissioners appealed to the United Nations 'to prepare a binding legal instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights'. This appeal was repeated in 2008 at the 30th International Conference of Data Protection and Privacy Commissioners held in Strasbourg,[11] at the 31st conference held in 2009 in Madrid,[12] and at the 32nd conference held in 2010 in Jerusalem.[13] At the 33rd conference in 2011 in Mexico City,[14] the working group for the 'Promotion of the International Standards' resumed their efforts:

> *In line with the Jerusalem resolution, the Conference will continue to promote the Joint Proposal for International Standards in all relevant international fora (e.g. OECD, Council of Europe, APEC) and its efforts to organize an intergovernmental conference for developing a binding international instrument. In this regard, it could be envisaged to convey government's representatives at the next Conference meeting in 2012 in order to engage a dialogue in that perspective.*[15]

9 French President Nicolas Sarkozy decided to put the Internet at the top of the agenda of the French presidency of the G8/G20 in 2011. At the G8 summit in Deauville last May, all member states expressed the strong political commitment of the G8 members concerning the protection of personal data and individual privacy:

> *The effective protection of personal data and individual privacy on the Internet is essential to earn users' trust. It is a matter for all stakeholders: the users who need to be better aware of their responsibility when placing personal data on the Internet, the service providers who store and process this data, and governments and regulators who must ensure the effectiveness of this protection. We encourage the development of common approaches taking into account national-legal frameworks, based on fundamental rights and that protect personal data, whilst allowing the legal transfer of data.*[16]

10 The EU Commission addressed these issues in its factsheets on proposed data protection reform:

> *The rapid pace of technological change and globalisation have profoundly transformed the scale and way personal data is collected, accessed, used and transferred. There are several good reasons for reviewing and improving the current rules, which were adopted in 1995: the increasingly globalised nature of data flows, the fact that personal information is collected, transferred and exchanged in huge quantities across continents and around the globe in milliseconds and the arrival*

of cloud computing. In particular, cloud computing – where individuals access computer resources remotely, rather than owning them locally – poses new challenges for data protection authorities, as data can and does move from one jurisdiction to another, including outside the EU, in an instant. In order to ensure a continuity of data protection, the rules need to be brought in line with technological developments.[17]

11 In a globalized world, free data flow has become an everyday need. Thus, the aim of global harmonization should be that there is no difference for cloud users whether the processing of their personal data takes place in one or in several countries. Concern has been expressed that data processors might seek to avoid data protection controls by moving their operations to countries that have lower standards in their data protection laws or no such laws at all. To control that risk, some countries have implemented special controls in their domestic law. Again, such controls may interfere with the need for free international data flow.

12 A formula has to be found to make sure that privacy at the international level does not prejudice these goals. It is a long journey.

B. The polar caps: Cloud computing and privacy

I. Definitions of 'privacy' and 'data protection'

13 To those outside the privacy world it must seem incredible that lawyers are still debating the central issue in privacy: What are we trying to protect?[18] On an international level we are weighed down with divergences of usage with a non-uniform interpretation of this concept: privacy can rely upon a 'human right' ora 'social need'; it can be interpreted comprehensively as 'privacy of the person', 'privacy of personal behaviour', 'privacy of personal communications' and 'privacy of personal data'.

14 This article follows a definition influenced by Article 8 of the European Convention on Human Rights (ECHR)[19] and the European Data Protection Directive (EU-DPD):[20] In European privacy law, privacy is explicitly mentioned as a fundamental right. Through the Lisbon Treaty,[21] Article 8 of the 'Convention for the Protection of Human Rights and Fundamental Freedoms' (ECHR)[22] became mandatory to reach the aims of European data protection. Article1 of the EU-DPD and of the Directive 2002/58/EC[23] clearly state the ultimate purpose of the rules contained therein: to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy, with regard to the processing of personal data. The 'Article 29 Data Protection Working Party'[24] issued a document defining'personal data' in order to clarify the EU-DPD's approach. It was divided into four key elements: 1) any information 2) relating to an 3) identified or identifiable 4) natural person.

15 This illustrates that within the E.U. the concepts of data protectionand privacy are "twins, but not identical"[25], and that data protection law "seeks to give rights to individuals in how data identifying them or pertaining to them are processed, and to subject such processing to a defined set of safeguards"[26], while privacy can be seen as a "'concept which is broader than data protection, though there can be a significant overlap between the two'.[27]

16 Thus, the author of this article will keep in mind that data protection is one key element within people's privacy rights, but the scope of this element goes from protecting their 'right to be left alone'[28] to their 'right to be forgotten'.[29] The former means protecting personal data from being collected, transmitted, stored and used in an unlawful way. The latter means the possibility to manage data protection risks online; when the right owners no longer want their data to be processed and there are no legitimate grounds for retaining it, the data must be deleted. Henceforth, the author will look at issues of 'data protection 'only; other elements of people's privacy rights have to be left aside.

II. Definition of 'cloud computing'

17 Although cloud computing services have been on offer for many years, the significantly increased use of social media sites as Facebook and Google+ in cloud computing surroundings opened the public debate on the definition of 'cloud computing'.

18 The relevant players in cloud computing surroundings are as follows:

- The resource owner

A cloud computing model is composed of three service models, depending on the type of resources offered by the resource owner:

- Infrastructure as a service ('IaaS'):
IT services such as hardware components.

- Software as a service ('SaaS'):
Application packages, email, ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), ECM (Enterprise Content Management).

- Platform as a service ('PaaS'):
Resources and infrastructure-software, e.g. webserver, databases.

- The cloud provider

There are four models for deploying these resources bundled in a cloud computing service:

-Private cloud:
Services are exclusively used by one institution, even if supporting public processes are running in the background. Resource, cloud provider and cloud user are the same entity (e.g. one company).

-Public cloud :
Services can be used by everybody. All physical resources are not owned by the cloud user.

-Hybrid cloud:
A hybrid cloud mixes elements of both the public and private cloud.

-Community cloud:
The cloud infrastructure is commonly used by different organizationsthathave their common standards (e.g. security, privacy, compliance) and support a specific community.

- The cloud user
The advantages of cloud computing for the end user include the following: anytime and broad network access, hardware cost reduction, efficiency, rapid elasticity, measured service. But its key feature is what is called the 'scalability' of service, meaning that services and resources can be scaled up or down depending on the users' demand.

III. Effects of cloud computing on data protection

19 Using cloud computing to process personal data raises legal and technical questions that have yet to be adequately addressed. The use of cloud computing may become relevant for data protection in mainly six juridical dimensions.

20 Issues of solely technical risks within the cloud will – at this point – not be an object of this article. These include missing or insufficient separation/isolation of different data processing processes, lock-in effects, system and network failure and non-availability of rented resources and services, misuse of data by malicious insiders or employees and loss of data.

1. Processing of personal data

a.) Processing

21 Article 2 (b) EU-DPD provides that

> *Processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*

b.) Personal data

22 It has to be determined what type of data is normally processed in a cloud. From a data protection perspective, cloud computing becomes relevant only if this data is 'personal data'.

23 The Article 29 Working Party states that

> *personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to oneor more factors specific to his physical, physiological, mental, economic, cultural or social identity.*[35]

24 Data protection laws don't apply if sufficient aliasing of formerly personal data can be provided by the cloud provider. But it has to be remembered that aliased data can also become re-identifiable through additional information, e.g. because other cloud users or cloud providers have additional knowledge with which a re-identification is possible. One can assume identifiability regularly through individual records of persons. Especially electronic evaluability and the integration into a global network may increase the probability of the existence of a priori information that enables identification of those who are affected.

2. Ubiquity and different data protection levels

25 A cloud is by its nature not necessarily tied to any particular location; in fact, as many other IT services nowadays, it is ubiquitous. Thus, data traffic in a cloud can take effect in different countries, each withitsdifferent laws relating to acts taking place on itsterritory. As a result, each cloud computing process would have to comply with different privacy laws and levels of data protection.

26 This leads to the second dimension, which is the territorial level of data protection that exists in states

in which the above-mentioned data is processed in a cloud.

27 National rules provide that after the classification of personal data as 'sensitive data', this data may be moved only if the processing meets special requirements. From a German point of view, the application of national rules come with only minor restrictions in the EU region, but significant restrictions whenever processing is carried out in the US and other third countries, as very different levels of data protection exist in countries beyond the EU.

28 The EU provides a strict legal regime and high level of data protection under the EU-DPD. The Directive requires that any country to which European personal data is sent must have an adequate level of data protection as measured by EU standards. As many cloud computing providers are based outside the EU but wish to conduct their business within the EU, they must ensure an adequate level of protection. This fact forced the US and EU to a bilateral convention, the safe harbor agreement.[36]

29 But even within the EU, different ways of implementing the Directive's Article17 into national laws do exist. The Article 29 Working Party will hopefully contribute an expert's opinion to the necessity of common standards regarding 'technical and organizational measures'. At the moment we face a disparity of such standards, with the result that each EU-based computer centre must first comply with the laws of its own jurisdiction, including the regulations of its own data protection authorities; second, it must take into account that the cloud usually is a cross-border issue, to comply with other national laws.

3. Issues of accountability between controller and processor

30 In cloud computing surroundings, the distinction between controller and processor is not always clear in practice and has to be subjected to a comprehensive consideration of all circumstances, especially if a cloud service is offered on a cross-border basis or cloud sub-providers are included in the supply chain.

31 At this point, the focus of the EU-DPD has to lie on the concept of 'data controller' and 'data processor' .A controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law (Art. 2 (d) EU-DPD), while a processor shall mean 'a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller' (Art. 2 (e) EU-DPD).

32 The basic concept is that a controller makes decisions about what data to collect and how to use it, while a processor performs operations on data only on behalf of the controller and according to the controller's instructions. Recommendations[37] of the Article 29 Data Protection Working Party are helpful to differentiate: The crucial question becomes who determines the purpose ('why?') and the essential means ('how?') of the processing. It is decisive which data transmitter is actually authorized to decide on these questions. Whoever determines the purpose or decides on essential elements of technical means of the data processing automatically becomes a data controller. The member states developed one helpful question on that differentiation. In Germany, for example, this question is who appears towards the affected persons as responsible for the data, or with whom the affected person has a legal relation or for whose business purposes the processing is carried out.

33 In cloud computing, the person or entity that 'determines the purposes and means of the processing' initially is the cloud user who makes the decision to use the cloud and feeds the data into it. Basically, a responsibility is not limited to the data controller's actual sphere of influence; it extends to contract data processing as well. Article 17 EU-DPD establishes that, when data is processed under contract, the controller is responsible for compliance with data protection requirements. This means that a person or entity cannot evade its responsibility by contracting with third parties.

34 The controller is responsible primarily for ensuring that the processing is allowed under substantive law, which can have implications under administrative, civil and criminal law. The Directive also brings a set of principles to be observed by the member states. Article 23 EU-DPD directs the member states to guarantee the protection of personal data by a corresponding national regulation on liability. Every instance of unlawful data processing, as well as any infringement of national laws having implemented this Directive, shall raise liability, in particular omitted information and clarification duties or the omitted conclusion of a contract for the purposes of Article 26 (2) EU-DPD. The resulting damage must be causally proven. The affected person has to meet the burden of proof concerning his damages as well as the legal cause, so causality must be proven or a 'sufficient causal link 'relating the data controller's or data processor's actions to the damage in question.

35 Although the wording of Article 23 (1) EU-DPD leaves unanswered whether the liability is dependent on fault, a fault-based liability has to be presumed or the exculpation rule of Article 23 (2) EU-DPD would

not be necessary. It is doubtful whether only material or also immaterial disadvantages are meant with 'damage' for the affected person. Even in the recitals of the EU-DPD, no statements can be found on this issue; hence, a margin of discretion can be assumed when it is turned over to any member state.

4. Jurisdiction, applicable lawand enforcement

36 Conflict of laws is central to cloudcomputing because the Internet, thevery basis of the'cloud',is multinational. While cloud computing and other e-commerce innovations are giving new prominence to this area of law, private international law is not a creation of cyberspace. It is a series of national rules and principles that have been developed over centuries to assist legislatures and courts in dealing with three questions that arise in transactions with one or more international or at least multi-jurisdictional elements. Which courts may take jurisdiction over the parties or the transaction? Which laws apply? When will the courts of one jurisdiction enforce a judgment rendered by the courts of another jurisdiction?[38]

a.) Private cloud vs. public cloud

37 Robert Gellman of the World Privacy Forum highlighted the issues raised by data location:

38 The European Union's Data Protection Directive offers an example of the importance of location on legal rights and obligations. Under Article 4 [...] [o]nce EU law applies to the personal data, the data remains subject to the law, and the export of that data will thereafter be subject to EU rules limiting transfers to a third country. Once an EU Member State's data protection law attaches to personal information, there is no clear way to remove the applicability of the law to the data.[39]

39 As a result, it becomes important which national laws are applicable to the (first) processing of personal data in a cloud solution. It has to be considered where the relevant data is processed and from which legal system this data may originate.

40 The geographical location of personal data in the cloud has an important impact on the legal requirements of a court's jurisdiction and the law that applies to the case. At this point, the differentiation between private cloud and public cloud becomes crucial. For instance, for a private cloud solution thatprocesses 'German data'– data processed on servers, computers and storage systems exclusively operated in Germany–only German law applies. Thus, a private cloud poses no special problems in international private law (IPL) as lon gas the transfer of personal data into a cloud is carried out on German territory. Whenever personal data is processed in a public cloud, however, it has to be assumed that this data is being processed on computers and storage systems in different states. The exact place where data is located is not always known, and it can change in time. In a public cloud, the cloud services are not aimed at specific countries but as ubiquitous services. In this case, questions of jurisdiction and applicable law have to be examined.

b.) Jurisdiction

41 The choice of forum for settling disputes between the cloud provider and the cloud customer can be included in the terms and conditions of the contract. Providers usually specify a jurisdiction where the headquarters is based or its main business is carried out.

42 In the absence of a choice of forum provision, courts generally will take jurisdiction if there is a 'real and substantial connection' between the jurisdiction and either the people involved (personal jurisdiction) or the subject matter of the dispute (subject matter jurisdiction). The courts will take jurisdiction over people resident or domiciled in their jurisdiction as well as over property situated in their jurisdiction. They may also take jurisdiction where an accident occurred or damages were suffered in the jurisdiction.

43 If a person or company is domiciled or based in a member state of the EU, it shall be sued in the courts of that member state. If these are not nationals of the member state in which they are domiciled or based, they shall be governed by the rules of jurisdiction applicable to nationals of that state (Art. 2 Brussels I).[40] They can be sued in the courts of another member state only by virtue of the rules set out in Sections 2 to 7 of Brussels I Regulation.

44 Article 5 Brussels I provides that

> *a person domiciled in a Member State may, in another Member State, be sued: 1. (a) in matters relating to a contract, in the courts for the place of performance of the obligation in question; (b) for the purpose of this provision and unless otherwise agreed, the place of performance of the obligation in question shall be: [...] in the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided.*

45 Asserting jurisdiction can become a significant problem whenever the ubiquity of cloud computing services imposes questions such as the following:

46 What are the international elements in the case at hand and what is the question that we are seeking to answer? Are we asking if the court in the jurisdiction of the customer will take jurisdiction over a dispute

between an online supplier of cloud computing services and a customer? Or are we asking whether the criminal laws of Oregon apply to a Russian website that allows you to store and play your music from anywhere around the globe?[41]

c.) Applicable law

47 The contract statute may result from an effective choice of law, from the perspective of European IPL determined by Article 3 (1) Rome I.[42]

48 In its absence, the law of the state applies where the provider of the service – given that a cloud computing service is qualified as a tenancy law issue – has its 'habitual residence' (Art. 4 (2) Rome I). If rules of an employment contract shall govern cloud computing, Article 4 (1b) Rome I leads to the same result.

49 Furthermore, it has to be considered that, for the benefit of consumer protection rules, atypical choice of law clauses are inapplicable; in this case, the national law remains applicable in which the consumer resides (Art. 6 (1b) Rome I). Mandatory national consumer protection rules always remain applicable in favour of the consumer (Art. 6 (2) Rome I).

50 For companies wanting to store data in the cloud, there is a minefield of data protection laws to negotiate, so it is essential to know in which country your data is physically stored. 'Most organizations don't even know what data they have,' says Tony Lock, program director at IT services consultancy Freeform Dynamics. 'They are unsure where all the data is and once they've found it they are unsure how to protect it.'[43] But which laws apply, for example, to a German company storing data about German customers via a contract with a US cloud provider whose servers are located in Poland? At the moment, the answer is all three due to the very debatable rules of applicable law in the EU-DPD.

d.) Subcontracting

51 Whenever a cloud provider uses a third-party subcontractor to carry out its business, issues of jurisdiction and applicable law get even more complex, because the existence of a subcontracting relationship is likely to be invisible for the cloud user and the location of the subcontractor or the data processed by him difficult to ascertain.

e.) Enforcement

52 As a consequence, the question arises whether the flow of data adequately meets the regulatory requirements of each jurisdiction through which it flows. In theory, each controller could be sued in various states worldwide for a breach of data protection laws. But in practice, law enforcement is more difficult.

53 Whenever the violation of data protection laws is committed outside European territory, there is generally no way to investigate it, because under the law, the oversight of supervisory authorities is limited to the territory of each state. An administrative assistance, provided in inner-European cases, doesn't apply to cases beyond the EU.

54 Thus, data controllers processing data in third-party countries that want to evade data protection authorities' oversight can use clouds specifically for that purpose. Another negative effect of the cloud is that any monitoring is contingent on contractual monitoring rights granted by the cloud and resource providers, and furthermore these rights must be exercised by the cloud user, which generally has no vested interest in data privacy oversight.

5. Contract data processing

55 The element of contract data processing has been implemented in Article17 EU-DPD in order to secure personal data within the collecting, processing or use of data on behalf of others. Article17 EU-DPD applies if

> *a contract between a controller and processor has been concluded, requiring that the processor act only on instruction of the controller;*

and

> *a (cross-border) data processing takes place within the member states of the European Union (EU) or European Economic Area (EEA).*

56 Article17 (2) EU-DPD then requires a controller to 'implement appropriate technical and organizational controls to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access'.

57 Article17 EU-DPD remains inapplicable if the processor can be qualified as a third entity that does not act on the instruction of the controller, or the processing of personal data is carried out outside of the EU. In this case, the data transfer is lawful only if the cloud provider complies with the provisions set out in Articles25, 26 EU-DPD.[44]

58 The EU-DPD states clearly that data cannot leave the EU unless it is transmitted to a country with 'adequate level of protection'. That means that many cloud providers outside the EU have to study and follow one of four different methods to ensure adequate protection as long as they wish to conduct cloud services business inside the EU: first, be one

of the countries that have laws enacted that the EU deems to be adequate protection; second, achieve adequacy through compliance with safe harbor provisions; third, use a standard contractual clause prepared and adopted by the EU; or fourth, use binding corporate rules.[45]

6. International data transfer

59 Cloud providers established in countries outside the EU and EEA have to conduct a two-step test whenever they want to process personal data of a European data subject in a lawful way. First, the transfer of personal data into the cloud and the processing in the cloud must have a legal basis. Secondly, an adequate level of data protection must be ensured at the cloud location outside the EU/EEA. For the latter, safe harbor, binding corporate rules and EU standard contractual clauses (or model contracts) are mainly relevant. Unfortunately, several data protection offices and authorities do not always clearly distinguish these two basic steps.

60 Article 25 ff. EU-DPD is relevant regarding the second step. Article 25 (1) EU-DPD requires that member states prohibit the transfer of personal data to third countries lacking similar legal protections, unless a) the national supervisory authority (Art.25 (2) EU-DPD) or the European Commission approves the data transfer, b) one of several limited exceptions apply (Art.26 (1) EU-DPD) or c) approved safeguards are in place (Art. 25 (6), Art.26 (2), Art. 26 (4) EU-DPD).

61 The European Commission has recognised through 'adequacy tests' (Art.25 (4) EU-DPD, Art.25 (6) EU-DPD, Art.31 (2) EU-DPD) a sufficient level of protection (Art.25 (1) EU-DPD) for only a few countries.[46] EU member states must allow a data transfer to one of these countries (Art. 31 (2), Art. 25 (6) EU-DPD). Other countries should soon be under review for a possible addition to the white list if their laws are deemed adequate.[47] For the remaining countries, an adequate level of data protection must be guaranteed individually. Four of these are most often used: unambiguous consent and several contractual instruments ensuring accession to safe harbor principles, the conclusion of standard contractual clauses (SCC) or the adoption of binding corporate rules (BCR).

62 It has to be carefully taken into account where Article 26 EU-DPD stands within the system of principles and derogations on a European and on a national basis. The Article 29 Data Protection Working Party states that

> *[t]he juxta position of these different rules on transfers of personal data may givea paradoxical impression, and can easily give rise to misunderstanding. [...] Under these provisions, the data controller originating the transfer neither has to make sure that the receiver will provide adequate protection nor usually needs to obtain any kind of prior authorisation for the transfer from the relevant authorities, if this procedure would be applicable. Furthermore, these provisions do not require the data receiver to comply with the Directive requirements as regards any processing of the data in his own country (e.g. principles of purpose, security, right of access, etc.).*[48]

63 On the one hand, derogations of Article 26 (1) EU-DPD can apply, e.g. Article 26 (1) a) EU-DPD: Such consent must be given by the person whose personal data is to be transferred. It must be 'clear, freely, given and informed' (Art.26 (1) EU-DPD). Consent can be refused and withdrawn at any time. Technological measures to ensure a consent that may be evidenced and enforced later on can greatly vary from one another. For instance, the range includes user pop-ups with an option to consent by ticking the box of their choice before they may continue entering the website. A problematic issue is the freedom of consent in an employment context. The Article 29 Data Protection Working Party has released a document in which it states that employees would not be able to freely give their consent due to their subordination link with their employer ('reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment'[49]). In practice however, this form of consent can be a valid derogation under certain circumstances, as when the data transfer is submitted to the works council or it is made clearly for the benefit of the employee, without small print. Nevertheless, the Article 29 Data Protection Working Party considers that 'consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question'. This opinion is clearly opposed to the exemptions in Article26 (1) EU-DPD.

64 On the other hand, to transfer the derogation provisions of Article26 (2), (4) EU-DPD into practice, several instruments have been developed: safe harbor-principles, PNR, BCR, SCC I,[50] SCC II[51] andSCC-DP.[52]All of these instruments with their beautiful abbreviations differ in terms of standardization level and liability rules and remain to be mentioned below under 'Perspectives of global standards'.

C. The present means of travel: Perspectives of global standards

65 Answers for the above-mentioned problems could be found in global data protection legislation. In recent years, an increasing number of states have adopted data protection legislation, and a fundamental, legally binding right to privacy is recognized both in the national law of numerous states –particularly in Europe –and in certain regional legal instruments. The questions that then arise are whether privacy is similarly recognized in international law as a bind-

ing legal concept, whether existing models of privacy are diverse and how privacy is considered in data protection legislation.

I. Public law

1. US legal framework

a.) Facts

66 The US approach deals with data protection in so many narrow sectors that this article can't claim to touch all of them and will have to focus on the most important ones:

67 The implications of the 'Graham-Leach-Bliley Act'[53] (GLB) on cloud providers is that the cloud provider has to comply with the relevant parts of GLB by demonstrating how it prevents unauthorized access to personal data and/or contractually agree to prevent this unauthorized access. The safeguards rule mandated by the GLB and enforced by the Federal Trade Commission (FTC) requires that all cloud providers involved in financial services and products must have a written security plan to protect customer information.

68 The FTC promulgated so-called 'Red Flag Rules' in 2007, based on the 'Fair and Accurate Credit Transaction Act of 2003'[54] (FACTA). These flags also apply to cloud providers that are creditors as well as to other companies in online spaces. Therefore, the cloud provider must also have a written security plan and monitoring systems in place.

69 A data breach is a loss of unencrypted electronically stored personal data that can occur, for example, if a laptop has been stolen or a server has been compromised. Almost all 50 states now require notification from cloud providers of the affected persons and coordination with the cloud users.

70 In the US health sector, the 'Health Information Technology for Economic and Clinical Health Act' (HITECH Act) requires notification of any breach of unencrypted health records for all entities that have to comply with the 'Health Insurance Portability and Accountability Act'[55] (HIPAA). A service provider cannot use or disclose health records in a way that conflicts with the HIPAA standards. Thus, an entity covered by HIPAA could violate HIPAA by processing patient records through a cloud providers' service that allows the publication of any information stored on its facilities on the basis of its terms and conditions.

71 The 'USA Patriot Act'[56] has important effects on cloud provider behaviour in the US. The Act widens the US government's possibilities to, for example, install devices to record all routing, addressing and signalling information kept by a (cloud) computer and gain access to personal financial information and student information stored in the cloud. The only legal requirement for the US government lies in a governmental certification that the information obtained be relevant to provide information to an on-going criminal investigation. This concept basically leads to the gathering of personal data in the cloud – without any suspicion of wrongdoing.

72 The 'Electronic Communications Privacy Act'[57] (ECPA) applies to 'any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature', as long as it is transmitted electronically. Although this law is difficult to apply, particularly because the law is old and based on a model of electronic mail and Internet activity that is generations behind the current technology, it appears to provide probable protection for most data processed by cloud providers.

73 Besides the data breach laws (see above), many states[58] require that technology vendors (including cloud providers) provide adequate security in their contractual guarantees.

74 Customers of tax preparers enjoy some statutory and regulatory privacy protections. These customer protections in turn limit the ability of a tax preparer to use a cloud provider.[59]

75 The 'Violence Against Women Act'[60] prohibits all disclosures not compelled by statute or a court, except disclosures with the consent of the data subject. Thus, the terms and conditions of a cloud provider have to comply with this non-disclosure standard.

76 The US approach reflects a 'basic distrust of government; markets and self-regulation rather than government oversight shape information privacy in the U.S. and as a result the legislation that does exist is reactive and issue-specific; protection tends to be tort-based and market orientated rather than legislative or regulatory'.[61] Therefore, this approach is also called a 'patchwork of rules'[62] or 'piecemeal model'[63] that deals with data protection in specific sectors and problems in a 'haphazard manner'.[64]

77 On the other hand, they address specific and sometimes narrowly targeted privacy issues.[65] Self-regulation is another pillar of the US system and could be a useful contribution to global standards. An online privacy seal program exists, e.g. for labelling schemes. But authorities such as 'TRUSTe'[66] or 'BBBOnline'[67]have faced some criticism that they do not go far enough to punish seal holders that break the rules, and that the organizations are not quick

enough in revoking the seal on companies that violate privacy standards.

b.) Observations

78 The self-certification of US companies to safe harbor alone is not enough to reach a data security level corresponding to EU standards. Cloud contracts that are orientated by safe harbor are also insufficient. Safe harbor, however, cannot handle the stricter data security regulations in Europe. Cloud suppliers such as Google or Salesforce with headquarters in the US identify themselves for purposes of proof of trustworthiness with a SAS-70-Typ-II certificate. This means that the data centres should be checked by an independent third party. This measure is only partially enough for the requirements of the order data processing. For example, it does not consider the material and procedural interests of affected persons in transmissions. It is also possible that the companies involved in a cloud present themselves to BCRs, by which an adequate level of protection after Article 26 par. 2 EU-DPD could be reached.

2. EU legal framework

a.) Facts

(1) CoE Convention 108

79 The principles that the EU-DPD establishes are based on a range of Articles 7 and 8 ECHR and the CoE Convention 108.[68] The CoE Convention 108 was based on the 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' and called for national implementation of data privacy laws by individual European states. However, it is also envisaged to be potentially more than an agreement between European states (Art. 23). The CoE Convention 108 is not intended to be self-executing, and it permits derogations in some significant areas (Art. 3, 6 and 9). In addition, depending on the rules in national law regarding the adoption of international conventions, if a convention is implemented into domestic law, then the relevant provisions can be amended under the constitutional law of that state, regardless of its obligations under international law. Still, these legislations had no effect on international legislation.

(2) European Data Protection Directive and its reform

80 On 25 January 2012, Viviane Reding, European Commissioner for Justice, presented plans to enhance data protection rights for individuals across Europe and increase the responsibility and accountability of organizations processing personal data. The draft 'guidelines' show a growing concern about the way in which personal datais collected, processed and used. Viviane Reding's aim is that the rules will be implemented with consistency and clarity across all European Union member states and also apply to organizations based outside Europe that do business within the community.

81 The new legislation will replace the present EU-DPD, an important component of EU privacy and data protection legislation under which organizations in both the public and private sector have been operating for now thirteen years.

82 These are the key elements of the proposed reform:

- A 'right to be forgotten' will help people better manage data-protection risks online. When they no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.
- Whenever consent is required for data processing, it will have to be given explicitly, rather than be assumed.
- Easier access to one's own data and the right of data portability, i.e. easier transfer of personal data from one service provider to another.
- Companies and organizations will have to notify serious data breaches without undue delay, where feasible within 24 hours.
- A single set of rules on data protection, valid across the EU.
- Companies will only have to deal with a single national data protection authority – in the EU country where they have their main establishment.
- Individuals will have the right to refer all cases to their home national data protection authority, even when their personal data is processed outside their home country.
- EU rules will apply to companies not established in the EU if they offer goods or services in the EU or monitor the online behaviour of citizens.
- Increased responsibility and accountability for those processing personal data.
- Unnecessary administrative burdens such as notification requirements for companies processing personal data will be removed.
- National data protection authorities will be strengthened so they can better enforce the EU rules at home.[69]

83 Christian Toon, Head of Information Security Europe, Iron Mountain, is on the right track by stating that

> *it remains to be seen how much of the draft proposal makes it into the final legislation; but the announcement of the plans has given organizations across Europe a valuable opportunity to review and enhance their information handling policies. We must seize that opportunity. Once the new EU legislation is finalised and comes into effect, it will be too late.*[70]

(3) European Cookie Directive

84 The Directive 2009/136/EC71 requires consent for the placement of cookies on the Internet by tightening existing legislation in this regard, namely the e-Privacy Directive (2002/58/EC).

85 The Cookie Directive requires end user consent to the storing of cookies on their computer. It states that a cookie can only be stored on the computer or accessed from the computer if 'the user has given his or her consent, having been provided with clear and comprehensive information'. The cookie can only be placed when it is absolutely necessary for the provision of a service that has been requested by the user or information storage is for the sole purpose of carrying out an online communication. This Directive is relevant for cloud computing issues only if cloud providers include advertising into their services; then they need users' consent for the provision of cookies.

86 In practice, this Directive is likely to affect mainly organizations offering applications that attempt to access personal data; this will require user consent via the opt-in principle.

(4) EuroSOX

87 The 'Sarbanes–Oxley Act'[72] of 2002, more commonly called SOX, is a US federal law thatset new or enhanced standards for all US public company boards, management and public accounting firms. It has been drafted as a reaction to the stocktaking scandals around the companies of Enron and Worldcom.

88 'EuroSOX'– the nickname for the 8th EU Company Law Directive 2006/43/EC[73]–is a reaction to the US SOX initiative, though EuroSOX is less similar to US Sabanes-Oxley (SOX) than the nickname may try to imply. In Germany the Directive is adopted in the new law called 'Bilanzrechtsmodernisierungsgesetz' (BilMoG). From a data protection point of view, the Directive demands high conditions for information security systems and internal IT control systems. Although the Directive doesn't mandate a specific standard or framework, 'it clearly shows that established international standards and frameworks such as ISO 27001/27002, COBIT and COSO (Enterprise Risk Management) are very solid instruments to ensure that the company will pass the audit of their internal IT control and information security management system.'[74]

89 Thus, central goals to meet the requirements of this Directive are as follows:

- transparent and documented business processes,
- transparent and documented IT architecture,
- identity management, and
- compliance through internal control system (ICS).

b.) Observations

(1) General

90 Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, including EU data protection reform and cloud computing, tried to summarize the positive impacts of the data protection reform for cloud businesses:

> *[..W]e have proposed rules more relevant to a networked, connected world. Clouds cross borders, and so does the data they hold. So we will make it easier to operate Clouds both within and outside our Single Market.[...] Globally operating businesses will benefit from changes to the use of binding corporate rules. They only have to get authorisation from a single authority; and there is more recognition of the variety of structures used in Cloud Computing. That will make the use of BCRs less burdensome and more effective.This legal framework is a sound basis for the Cloud. But I am confident that many Cloud providers will choose to go further, and take additional steps. Because strong protection and respect for privacy make good business sense. From our public consultation, we know people are concerned about which Cloud providers they can trust. And let's not forget that even in established areas like online shopping today less than one in five people feel in complete control of their personal data. [...] our proposal balances protection with efficiency. Safeguarding Europeans' rights – without putting the development of valuable new products and services 'off limits'. These three concrete things – Cloud-friendly data protection rules, a Cloud Partnership to make our public money count, and a supportive home for legal content – only make up a part of the European Cloud Computing Strategy.[...]*[75]

91 In the author's opinion, there are still some issues that have to be addressed in the reform's further consultations:

(2) Concept of personal data

92 The current definition of personal data in the EU-DPD is unclear. Information may be personal data or not depending on how it is encrypted or anonymized before being processed. In many cases, cloud providers may not even know if data processed by their services is personal data. Liability for cloud provid-

ers outside the EU or EEA depends on their customers' choices.

93 Thus, the future concept of personal data in the cloud should be based on the realistic risk of identification. Whether data protection rules apply or not should be based on all facts of the situation that carry the risk of harm.

94 It should also be clarified which procedures for encryption or anonymization are accepted by the updated EU-DPD.

(3) Jurisdiction and applicable law

95 The current legal uncertainties (see above) may discourage the use of European data centres or European cloud computing service providers. This could lead to a significant disadvantage for European e-commerce. It is clear that data protection laws may differ between EU member states, and that practical recommendations are needed relating to whether the Directive can be enforced in non-EU countries. Therefore, clarification is needed by the Commission on which and when a country's security requirements and other rules apply to a cloud computing user or provider. The European framework on data protection is still based on the country-of-origin rule, so data protection obligations should apply to entities based on this rule within the EU, and based on directing or targeting their services to EU consumers for non-EU providers. The present EU-DPD does not adequately balance the interests of data protection and the free flow of data, especially if services of cloud providers in third countries beyond the EU are concerned. Clearer rules are needed on the determination of 'establishment' and 'context of activities' for controllers in Article 4 (1a) EU-DPD.

(4) Accountability

96 The Directive fails to acknowledge the interacting positions between controller and processor in a cloud surrounding. They may overlap, and cloud computing service providers may be unaware that the data they process or store on behalf of a customer is classified as 'personal data', possibly because the controller fails to inform the processor. Ian Walden, professor of information and communications law, says:

> *The law should be updated to treat cloud computing service providers, in certain circumstances, as neutral intermediaries with immunities from data protection obligations. [...] If they unwittingly store 'personal data' they should have defences based on lack of knowledge or control. There should be different levels of responsibility depending on the nature of the service being provided.*[76]

(5) International data transfer

97 The Directive places restrictions on personal data being exported out of the EU, which seems outdated, particularly as remote access is now the norm on the Internet. 'We suggest that the Directive's focus on data location and the restriction on exporting data outside the EU should be replaced by requirements on accountability, transparency and security. It is not where information is stored, but how securely it is stored, and who can access it, that matters most,'[77] says Kuan Hon, paper co-author and researcher on the Cloud Legal Project.[78]

98 Until then, European users of non-EU/EEA clouds should make sure that their cloud agreements include both the EU standard contractual clauses and comply with their respective national rules regarding contract data processing. Furthermore, the parties should give specific attention to the description of the locations of data processing facilities and the identity of the cloud's operators; they also should agree on data security certifications or independent third-party audits. In the best case, cloud providers do offer different options for security levels and data processing locations.

3. Bilateral conventions

a.) Facts

99 Cloud computing businesses take place primarily between the big players in this area, the US and the EU. To avoid difficulties of a multilateral convention, it could be helpful if the US and EU led the way by preparing and exemplarily drafting a bilateral convention, at the same time getting over the never-ending story of transatlantic dispute.

100 The last decade illustrated significant EU-US differences about the meaning of privacy and data protection. Such a dispute became evident when 1) the impact of data protection regulation could not be limited to the geographic territory of the originating jurisdiction, and 2) state capabilities and authorities in other affected jurisdictions were 'constrained to the point where impacts cannot be mitigated'.[79]

101 Particularly the EU-DPD had an impact on transatlantic conflicts. This Directive was designed to protect Europe's data privacy. As mentioned above, in a world where data flow is likely to be a cross-border issue, 'that regulation must reach beyond the EU if it is to be meaningful, it must apply wherever the data are transferred and processed'; thus, 'domestic legislation' has a transnational footprint'.[80]

(1) Transfer of Air Passenger Name Record (PNR) Data

102 Following the terrorist attacks of 9/11, the US passed legislation in November 2001 providing that air carriers operating flights to, from or across US territory had to provide US customs authorities with electronic access to the data[81] contained in their automated reservation and departure control systems, called 'passenger name records' ('PNR'). The following political negotiations between the European Commission and the US Department of Homeland Security (DHS) concerned the transfer and use of European air passengers' data to US authorities in the fight against terrorism and other serious crimes.

103 A new, controversial PNR interim agreement between US and EU was signed in July 2007 and expired on 31 July 2007. On 1 August 2007, a new agreement, which has a maturity of seven years, entered provisionally into force, replacing the interim agreement.[82]

104 On 5 May 2010, the European Parliament decided to postpone the vote on PNR until the use of PNR is clarified with respect to EU law and European Parliament concerns about privacy, proportionality and redress. Nevertheless, the European Parliament clarified its conditions for approval:

- PNR data can only be used for fighting terrorism and organized crime.
- Use of PNR data must be in line with EU data protection standards.
- Use of PNR for data mining and profiling is to be forbidden.
- Forwarding of data to third countries must be limited to a specific need and regulated by means of a binding international treaty.
- PNR data may only be provided on request – i.e. the push method.

105 On 21 September 2010, the new package of proposals was presented by Commissioner Malmström. 'The Commission's proposals largely reflect the requirements set out by the European Parliament,' said Sophie in 't Veld, rapporteur for the resolution on the agreements with the US and Australia on the transfer of PNR, in her initial reaction. She continued,

> *One of the main demands, namely that the use of passenger data has to be drastically restricted, has been accepted. The proposals will have to be studied by Parliament's Civil Liberties committee but they have been welcomed by Liberals and Democrats as a constructive package that represents a big improvement on the past. The main outstanding point of criticism is that the need for massive storage of data still has not been proven. It is not enough to say that the collection of data of passengers is 'useful' or 'valuable'. It must be 'necessary' and 'proportional'.*

106 As far as Ms In 't Veld is concerned, the Commission proposals still need some improvement on these points.'We will carefully scrutinise the outcome of the negotiations. The European Parliament will pull the plug if it is not satisfied with the progress,' she continued. 'The EP, under the Lisbon Treaty, has the right to vote down the agreements already in place, as well as giving its consent to any new agreements.'[83]

(2) Safe harbor

107 The objective of the US-EU negotiations leading to the 'safe harbor agreement'[84] was to find a solution that would ensure the adequacy of protection of European data consistent with American preferences for reliance on self-regulation and market mechanisms. Safe harbor includes principles thatare consistent with both the OECD Privacy Guidelines and the EU-DPD. An organization can enter safe harbor by either joining an approved self-regulatory program or developing its own compliant privacy policy and certifying it annually to the Department of Commerce. Each organization subscribing to these principles would be presumed to be providing adequate privacy protections. Enforcement of safe harbor is achieved by prosecution for unfair or deceptive advertising or promises by the FTC. Kobrin describes safe harbor as 'not an overwhelming success on either side of the Atlantic',[85] and Reidenberg argues that it is a 'weak, seriously flawed solution for e-commerce' that is no more than a mechanism to 'delay facing tough decisions about international privacy'[86]. European criticism about safe harbor concerns the fact that the number of organizations self-certifying under safe harbor is lower than expected, many of those do not really meet the requirements of the agreement and less than half of those organizations post privacy policies that reflect all seven safe harbor principles.

108 German data protection authorities have placed a significant new duty on German companies transferring personal data to the US. The joint panel of the German data protection authorities (so-called DüsseldorferKreis) passed a resolution on 28/29 April 2010,[87] setting stricter due diligence requirements for the personal data transfer under the safe harbor principles. German companies should now document their due diligence inquiries and responses. US companies importing data from Germany should accordingly expect requests for appropriate documentation and be prepared to assist their German counterparts with this new due diligence process.

> *With regard to the US, the European Commission adopted the decision on safe harbor whereby for the purposes of Article25 (2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the safe harbor privacy Principles [...] as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked*

questions [...] are considered to ensure an adequate level of protection for personal data transferred from the Community to organizations established in the United States.[88]

109 Safe harbor principles and the accompanying Frequently Asked Questions[89] set forth the provisions ensuring the adequate level of data protection. Nevertheless, national supervisory authorities often look critically at the level of protection in these principles. Sometimes the representation by a US entity that it is safe harbor-certified is not enough now according to national supervisory agencies because, in their view, EU and US regulators currently do not ensure that the US companies comply with the self-certification.

b.) Observations

110 Concurrent to European Commissions consultations on the reform, a new bilateral EU-US agreement could be drafted as a first important step in bridging the existing differences on the application of data protection laws that 'would make it then easier to achieve a common approach on protecting personal data online in the businesses world'.[90] Although the EU is negotiating with the US on data protection in judicial and police cooperation in criminal matters, it will not constitute in itself the legal basis for transfers of personal data related to cloud computing issues. Such transfer of personal data will still require a specific agreement providing a legal basis. An EU-US agreement could become the reference for data protection standards that apply whenever personal data needs to be transferred across the Atlantic. It would also save time and energy in any future negotiation of data transfer agreements because these talks would be based on this umbrella agreement. The aim has to be to negotiate a data protection agreement that contains all the necessary high-level data protection standards. It could lead to a win-win situation: The US could benefit immediately since high data protection standards would guarantee legal certainty and facilitate data transfers to and from the US much more easily than is currently possible. At the same time, the EU should continue to promote the development of high data protection standards at the international level by cooperating with relevant international organizations and actors (e.g. the OECD, the CoE, and the UN).

4. Multilateral conventions

a.) Facts

(1) United Nations (UN)

111 International recognition of privacy as a human right can be traced back to Article 12 UDHR.[91] The UDHR was the first international instrument to deal with the right to privacy. Because of its form as a resolution it is not legally binding; the same applies to the 'International Covenant on Civil and Political Rights' (ICCP).[92] The only instrument explicitly mentioning privacy issued so far by the UN also takes the form of a non-binding guidance document, the 'UN Guidelines concerning computerized personal data files'.[93] These guidelines contain minimum guarantees in privacy law that should be implemented in national legislation and are expressed in basic principles. But the UN has not made privacy principles enforceable within UN organizations.

112 The UN Computerized Guidelines were the earliest such guidelines to contain high-level data protection principles, but as they are not legally binding they have been of limited practical relevance. The OECD Privacy Guidelines 1980 are also not legally binding but have been highly influential in inspiring the enactment of privacy legislation in many regions around the world.[94]

113 The International Standards on the Protection of Personal Data and Privacy adopted in Madrid on 5 November 2009, at the 31st International Conference of Data Protection and Privacy Commissioners was the turning point for global data protection standards.[95] It is a non-binding resolution, but the intention was to pave the way for an internationally binding agreement, probably via the UN. The advantage of the Madrid Resolution is that it has been backed by representatives from the major Internet companies[96] as well as by data protection authorities; this gives it some authority. The key element of the agreement could be that it is based on the higher data protection standards of the EU rather than the lowest common denominator, so it harmonizes up rather than down. The language used is very close to that of European data protection law, which suggests that it would require non-EU privacy standards to be significantly improved. Thus, 'the agreed international standards are a milestone for modern privacy. Now it all depends on filling these standards with life.'[97]

114 The 32nd International Conference of Data Protection and Privacy Commissioners continued this trend by enacting a resolution, this time with special respect to the adoption of global privacy standards. It called for an intergovernmental conference to negotiate a binding international agreement guaranteeing respect for data protection and privacy and facilitating cross-border coordination of enforcement efforts. It repeated the same appeal in 2012:

In line with the Jerusalem resolution, the Conference will continue to promote the Joint Proposal for International Standards in all relevant international fora (e.g. OECD, Council of Europe, APEC) and its efforts to organize an intergovernmental Conference for developing a binding international instrument. In this regard, it could been visaged to convey govern-

ment's representatives at the next Conference meeting in 2012 in order to engage a dialogue in that perspective.[98]

(2) Organisation of Economic Cooperation and Development (OECD)

115 In 1980 the OECD published the OECD Privacy Guidelines, whose core is made of eight privacy principles for both the private and the public sector. The Guidelines are not legally binding on OECD member states but have been 'highly influential on the enactment and content of data protection legislation in countries outside Europe' and for the APEC Privacy Framework.[99] The following OECD Guidelines dealt not directly with privacy but with information society,[100] cryptography policy[101] and consumer protection in electronic commerce.[102] Some OECD declarations and reports have served as the basis for the OECD privacy protection work since 1985.[103]

(3) Asia-Pacific Economic Cooperation (APEC)

116 Far from the EU perspective, privacy is treated as a consumer concern, taking personal data as marketable goods and trying to balance their protection with private interests. This was the approach when drafting the' APEC privacy framework'.[104] The significance of the APEC economies cannot be doubted, as they are located on four continents, with more than a third of the world's population and almost half of the world trade.[105] The goal – and the advantage of the framework compared with the EU-DPD–is to 'establish a more flexible framework within which member economies can develop their own laws and policies that are compatible with other economies in the region'.[106] The framework consists of nine 'APEC Privacy Principles' in part III.

117 These principles can be criticized in several points. First, they are based on the 'OECD Privacy Guidelines' principles, which are no longer adequate to deal with the new dimensions of privacy related, for example, to the Internet. Secondly, the framework further weakens the OECD principles, does not reproduce all of the OECD principles, lowers the content of principles and improves on some OECD principles in only minor ways. The only new principles 'carry inherent dangers and have little to recommend them'.[107] Furthermore, the APEC framework does not include any considerations on how to treat the EU adequacy (Art. 25 EU-DPD) issue. Last, it ignores the regional legislation and experience of privacy law.[108] Thus, the APEC framework is largely consistent with the OECD Privacy Guidelines, and was therefore only an acceptable framework on privacy principles from twenty years ago. Particularly, the principles are 'for the most part unremarkable and deal with issues normally covered by international privacy laws'.[109] It might eventually emerge as a counterweight to European efforts because of its flexibility, its facilitation oftrans-borderdata-flows and the positive impact on economies in the Asian-Pacific region without any privacy legislation, but 'it remained a policy document with little implication for cross-border regulation'.[110]

118 On 13 November 2011, the APEC leaders endorsed the APEC Cross-Border Privacy Rules[111] (CBPR) system at an APEC meeting in Honolulu, Hawaii. The leaders agreed, among other things, to 'implement the APEC Cross-Border Privacy Rules System to reduce barriers to information flows, enhance consumer privacy and promote interoperability across regional data privacy regimes.' It is necessary to understand the opportunities and challenges offered by the CBPR system.

119 The ratification by the Ministers established the Joint Oversight Panel (JoP), commenced the recognition of Accountability Agents (AAs), and facilitated participation by economies in the CBPR system.The work plan of 2012 includes the development of the website that will list participating businesses, recognized AAs and Privacy Enforcement Authorities (PEAs), and further promotion and explanation of the system. It remains to be seen which economies will agree to put resources into the JoP – a minimum of three economies need to join the JoP. Those with existing privacy and data protection laws and PEAs may not, given their existing requirements for international data transfers. The whole system of the CBPR programme requirements is hard to understand, and participating businesses could possibly face a more onerous application process and bureaucratic requirements than they do in those APEC member economies with privacy laws, and arguably even than they do in EU member states, whose 'notification' regimes the APEC initiative was designed to avoid replicating. However, if the CBPR certification process and subsequent monitoring are carried out in good faith (a big 'if'), then the result could be a higher level of proactive compliance with privacy rules than most regimes have managed to achieve to date.[112]

(4) Other non-binding policy standards

120 Various groups have issued non-binding policy documents, e.g. the 'Global Privacy Standard'[113] by the Ontario Information and Privacy Commissioner or the 'Global Network Initiative' by a number of companies, non-governmental organizations, and academics, which is defined as 'a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector'.[114]

b.) Observations

121 A multilateral convention could produce a greater degree of harmonization, since it results in a single text that is legally binding on states that enact it.

But such a binding nature can also make states reluctant to do so. The possible convention could be faced with reservations made by states that are party to it, which can result in a diminution of the very harmonization that the convention was supposed to accomplish, and a convention can be difficult to amend in the face of changing practices or technological evolution.[115] Furthermore, the drafting of any such convention could take many years. Moreover, although a multilateral convention is legally binding in international law, it may still not produce a harmonized legal framework.

122 It is also doubtful which international body could bridge these differences. In the author's opinion, there are only a few bodies nearly sufficiently strong, dynamic and representative. A multilateral convention on privacy could be drafted by the International Law Commission (ILC). The ILC was established in 1948 under a resolution of the UN General Assembly;[116] it is charged with promoting 'the progressive development of international law and its codification'[117] and has adopted the 'protection of personal data in trans-border flow of information' in its long-term work program,[118] which could potentially result in the draft of an international convention. Another option could be to sling this issue over the shoulders of the General Agreement on Trade in Services (GATS) under the auspices of the World Trade Organization (WTO). The focus of the GATS is on trade liberalization and promoting economic growth.[119] Thus, although the commercial purposes of ubiquitous data flows across national borders seem to fit with the WTO focus, it is doubtful whether the WTO would have the ability to negotiate such an agreement quickly and efficiently; its ability would be 'hampered by its commercial bias'.[120] Other international organizations such as the United Nations Educational, Scientific and Cultural Organisation (UNESCO) and the International Telecommunications Union (ITU) are too specialized and may not be well prepared to produce standards in an area as diverse and multi-faceted as privacy.

123 The APEC framework is designed to be a more flexible system than the adequacy approach. It can be implemented in the vastly differing cultural and legal frameworks of the twenty-one APEC member states, but it would likely take years for it to become widely accepted on an international scale. Although the APEC model of self-regulation is likely to spread widely, it would spread thinly. And although the Asia-Pacific Privacy Authorities Forum (APPA) since 2005 'is becoming more organised and purposeful, it has not yet found a substantive role in the region's privacy protection'.[121]

124 The suggestions from the APEC consultations in 2011 of meeting the CBPR programme requirements was taken further in a paper that addressed the problems of interoperability. This paper was drafted by the International Chamber of Commerce (ICC) and stated that businessescould be recognized as compliant with the APEC Privacy Framework Principles without having to go through the processes established for the CBPR system. This illustrates that CBR still needs some work on bridging problems of interoperability. A positive effort of APEC is encouraging to see participation in APEC processes by more NGOs; the Electronic Frontiers Foundation (EFF), Center for Democracy and Technology (CDT), the Internet Society (ISOC) and Privacy International attended some of the 2011 meetings. The EU's system of binding corporate rules has some similarities with the CBPR system, reflecting its overall non-binding approach. It also remains uncertain whether, or how, the CBPR will be implemented over the next few years.

II. Private law

1. Terms and conditions

a.) Terms of use

125 Terms of use could provide an adequate protection of personal data if some key issues have been observed in the contractual relationship between cloud provider and cloud user:

- Anonymization of the data for trans-border data flow is possible
- Movement of data will be controlled
- Data encryption is provided
- Cloud user can access all of data anytime anywhere
- Exit scenarios for the future transfer of the data to other cloud providers
- Backup/restore plan
- Data breach notification
- Service levels and emergency plan in case of unavailability
- Commitment can be obtained regarding
  - the place where the data will be processed;
  - the exact chain of supply;
  - contract parties, their roles, rights and obligations, especially in case of multiple cloud platforms involved; and

- the period of data retention and treatment of data after termination or insolvency.

b.) Consent

126 The processing of data in a non-EU/non-EEA country may be lawful if the affected people (e.g. customers or employees) have agreed expressly and voluntarily to the processing of their personal data in an 'unsafe' third country. However, because of the strict requirements for a legally binding approval and the possibility of cancellation at anytime, this instrument is not often practicable.

2. Standard contractual clauses (SCC)

127 The Council and the European Parliament have given the Commission the power to decide, on the basis of Article 26 (4) of Directive 95/46/EC, that certain SCCs offer sufficient safeguards as required by Article 26 (2). However, it is admitted that individual contracts do not, of course, provide an adequate level of protection for an entire country. The European Commission has approved two alternative sets of SCCs for use in transferring personal data to a data 'controller' outside the EU/EEA (SCC I and SCC II), and a set of SCCs to be used when transferring data to a 'processor' (SCC-DP).

128 SCCs are contract defaults, complementing and specifying the demanded minimum standards of data protection (Art. 25 (2) EU-DPD). The rights and duties of the parties are regulated and must be adopted consistently. The member states are bound by the decisions of the EU commission. Thus, the member states must recognize that the companies which use the SCCs show an adequate data protection level. Then permission by the supervisory authority is not obligatory if the supervisory authorities are able to check the use of the contractual clauses and they are presented to the authority on inquiry. As soon as modified contractual clauses are used, however, an official authorization by the supervisory authority must be caught up.

129 SCCs are not used where data is being transferred to a US company that participates in the safe harbor program, or to a company relying on informed consent, Binding Corporate Rules approved by one national supervisory authority, or one of the other derogations under Article 26 EU-DPD. US companies that have not self-certified for safe harbor and other countries beyond the EU still have a further possibility to ensure an adequate level of protection. According to EU-DPD, a transfer to a third country that does not ensure an adequate level of protection may take place in cases 'where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights'; the Directive continues by stating that 'such safeguards may in particular result from appropriate contractual clauses' (Art.26 (2) EU-DPD).

130 In some way,the SCCs recognize the difficulty of data subjects to seek compensation–not only by establishing the applicable law and the responsibility of the data exporter, but also by providing that alternative dispute resolution (ADR) could be used as well as that the data subject could be represented by entities (recitals number 20, 21 and 22 of Decision 2010/87/EU). In case it is not possible for the data exporter to seek compensation, the same decision says that the data importer should offer the means for ADR.

131 The SCC I was adopted by the EU in 2001. However, it appeared afterwards in practice that the realities of the data transfers as well as the application of current business models had not been adequately considered. Thus, practitioners often did not apply these contract defaults. The most practice-related case in which data should be transferred by a data controller to a data processor was not covered, and the bureaucratic requirements were relatively high. This hindered the application of SCC I although SCC I was especially intended to facilitate the data flow. Besides, companies often did not accept their obligation to agree on conciliatory proceedings over liability.

132 Under SCC I, the data exporter and data importer were jointly and severally liable. They were indemnified from it only if neither would have been found responsible for the violation of personal data (clause 6 (1)). Between the parties, data exporter and data importer are obliged to declare indemnity if they have included the optional clause 6 (3) in the contract. In particular because of the problems thatresult from this joint and several liability, SCC I wascriticized and seldom used.

133 From 15 November 2010 on the new SCC II must be used; the old clauses were amended. Already-existing arrangements keep their validity as long as data is transferred and transmission as well as processing remains unchanged in the contractual relationship. The concerns addressed in SCC II are that processors today often subcontract some processing, storage and technical support functions to third parties. This is common in cloud computing, where several entities might be involved in handling and storing the data. SCC II is designed to ensure that the company that remains responsible as the data controller in Europe is informed about any proposed subcontracting, and that all parties handling the data are subjected to the same obligations of confidentiality and security. It contains a mandatory arbitration clause to which many companies have objected. Four different liabilities for the breach of data protection rules can be identified: contractual liability according to SCC II (either between the contracting

parties or against third person), and tortious liability (based on SCC II or national law).

134 Between the parties of SCC II, every contracting party is liable 'inter partes' for the damages caused by an offence against the clauses. This liability is limited to the de facto suffered damage; 'punitive damages' are therefore excluded.[122]

135 In case of damages to a third person, every party is liable for damages caused by the infringement of rights that arise for an affected third person directly from the SCC II. The affected person can immediately assert his right against the data importer or data exporter as a third-party beneficiary under one condition: if the data importer infringes obligations from the SCC II, the data exporter must first take action for the affected person and act upon the data importer to fulfil the latter's obligations. Only if the exporter is not able to remedy the wrong conduct of the data importer within one month can the affected person proceed directly against the importer.

136 When the tortious liability is to be applied, the data exporter is liable for offences conducted by the data importer because of fault through the poor choice of one's vicarious agent (culpa in eligiendo) if he did-not assure himself within a reasonable scope of time that the data importer was able to fulfil his juridical obligations. Nevertheless, the data exporter can absolve himself from liability if he proves that he has taken all reasonable efforts to fulfil his obligations of choice (Annex, Clause III b s. 2).

137 All the SCC II regulations mentioned do not change the liability of the data exporter according to national data protection laws, which remain untouched because these cannot be excluded by contractual arrangement between the contracting parties of the SCC II. If the SCC II default documents are adopted by the parties without changes, an authorization by a data protection authority of an EU member state is not necessary. The current SCC II permits the simplified employment of subsidiaries. Indeed, an EU-based company must make sure that the subsidiary complies with the European data security level.

138 If personal data is transmitted within the scope of contracted data processing from the EU in a third country, the SCC-DP[123] applies. Contracted data processing is when a company orders personal data – for example, customer data or employee data – to be processed by a foreign company (see above). In this particular respect,relevant areas of contracted data processing are forms of IT outsourcing (external data servers, external human resources data management, etc.). The SCC-DP covers transfers from the EU to a data in a third country, although data protection authorities 'may' allow use of the SCC-DP in such situations as well.

139 Annex Clause 6 (1) SCC-DP obliges the parties to grant to the affected person a contractual claim for compensation against the data exporter because of certain breaches of obligations of the data importer and/or the subcontractor. Annex Clause 3 (1) SCC-DP provides direct claims of the affected person against the data exporter. Exceptionally, the affected person can also proceed directly against the data importer if the latter or his subcontractor is responsible for a breach of obligations and the data exporter no longer exists on a factual or juridical basis (Annex Clause 3 (2) SCC-DP). The arbitration clause has been deleted.

3. Binding corporate rules (BCR)

140 BCRs serve to create a uniform contractual basis for the exchange of personal data in an affiliated group (Privacy Policy). An adequate data protection level can thereby be guaranteed at all companies of the group but not to group-external companies. This solution, also called 'Safe Haven', is based on the expression of safe harbor.

141 A liability regime corresponding to Article 22, 23 EU-DPD has to be included in the BCR. If the head office of the affiliated companies involved in the data transfer is inner-European, this office is liable for the breaches of contract of all itsaffiliated companies beyond the EU. If it is not seated in the domestic market, a group member resident in the EU must be named by the group of companies. This 'liable team member' must prove that it has sufficient assets to pay compensation for damages resulting from the breach of the BCRs.[124] If the involved companies have their seats in different EU countries, the regulations in the BCR must be approved by everysingle responsible authority (in Germanythis is coordinated with the 'DüsseldorferKreis'[125]). The liable team member must not compensate for breaches of other inner-European team members.[126]

142 The same rights must be granted to the affected person towards the liable team member, as if the liable action had been committed by a member within the EU. This regime has contractual rather thanlegal liability. Its results are determined by the applicable (substantive) law – e.g. in Germany or Spain, according to the BCR. This shows how important the determination of the applicable law is for cases of data transfers to third countries. Another significant question then remains: To what extent are restrictions of liability allowed? The Article 29 Data Protection Working Party gives no exact statement on this.

4. Observations

143 An adequate data security level is thereby guaranteed at all companies of the group, but not to com-

panies beyond this group. Besides, until recently the implementation of these required company regulations was still relatively complicatedin spite of some simplifications. It is also possible for the companies involved in a cloud to submit themselves to BCRs, by which an adequate level of protection (Article 26 par. 2 EU-DPD) should be produced by contract. According to the recommendations of the Article 29 Working Party, the head office or one group member named by the group of companies must answer within the scope of BCR for the offence of all affiliated companies beyond the EU. These BCRs need authorization by the responsible data protection authorities.

144 At the international level, the Cloud Security Alliance[127] (CSA), dominated by the US, has been formed; its aim is to compile guidelines for secure cloud computing. With the advent of EuroCloudDeutschland_eco[128] there is also a new organization for the German cloud computing industry, which is integrated into the European EuroCloud network. EuroCloudDeutschland_eco has come along to the assignment to create more transparency for the users, to introduce a quality seal, to clear legal questions, to promote the dialogue between suppliers and users and to provide cloud computing competence. An international framework would certainly make it possible to lift the local dependence of data processing and to exclusively apply the legal framework where the cloud user or the direct contracting partner of the user as a cloud supplier is based. Up to now, however, attempts in this direction have not been evident. In view of the non-uniform and partially lacking and insufficient national laws for data processing in general and especially for data security, international norms are not yet realistic. Hence, there is no alternative to the enforcement of a clear juridical protective regime that begins at the responsible place where the cloud user is based. Researchers, economists and supervisory authorities are asked to compile standards – to elaborate so-called Protection Profiles for Clouds with the responsible organizations – as well as to develop auditing procedures. Specific standard contract clauses still to be compiled or Binding Corporate Rules can serveas a preliminary stage for a global standard. The still-existing basic principle of a 'free cloud' is not enough for the requirements of modern data security; it can be understood only as an experimental application from which 'trusted and trustworthy clouds'[129] have to be developed with integrated data security guarantees. These trustworthy clouds must be made available in the market.

145 If the requirements of contract data processing are fulfilled, the SCC should be used for processing to a third-country service provider. If the transmission of the data must be considered not as contract data processing but as a transfer of function, then the use of the SCC-DP is recommended. If both purposes overlap – for example, if parts of a data transfer are contract data processing while other parts are classified as a function transfer – given that both parts of the data are separable, the SCC should be used for the first and SCC-DP for the second part. If such a separation is not possible or practical the SCC should apply.

III. Technological and private sector perspectives

146 An exhaustive review of the necessary technical and organizational precautions is impossible in this legal analysis, but it is vital to illustrate some of their most important impacts on the regulation of cloud computing issues. Based on common technological solutions, businesses and technology companies could turn to a single instrument for evaluating whether their practices or systems are actually meeting data protection laws and enhancing privacy.

147 Professor Lawrence Lessig famously proclaimed that 'code is law', that 'the software and hardware that make cyberspace what it is regulate cyberspace as it is'.[130] Technical standards for data processing could probably lead to globally harmonized data protection practices more swiftly and effectively than an international convention could. They have been promulgated by international bodies such as the International Telecommunications Union (ITU) and the World Wide Web Consortium (W3C). Regional bodies and several organizations are also working on data protection standards.[131] These 'have proven highly influential for the processing of personal data'.[132] Similar to the advantages of the accountability principle, technical standards may be more influential in determining how personal data is processed than most laws are. One weakness of technical standards is that they may be implemented differently in different regions and sectors; thus, European regulators are taking steps toward drafting them carefully and integrating them into the framework of data protection laws. They must also be rapidly adapted to new technological developments; otherwise they could be overtaken by them. Thus, while technical standards are likely to play an increasingly important role to support data protection laws if the goals and techniques of social and economic regulation are clearly distinguished, they are unlikely to be a complete solution.

1. The technical and organizational data security measures required by Article 17 EU-DPD 1

148 These measures must be expressly set out in the cloud computing service contract. Security by trans-

parency together with state-of-the-art security measures should be the aim.

149 This could be achieved with a multi-level access regime, encryption capabilities and possibly aliasing tools. In cloud computing, multiple users work on the same computers and platforms—a practice that presents risks unless stored data are adequately separated. To ensure compartmentalization of individual contract relationships, the cloud contract must clearly specify the methods used to separate data from different principals. If this is achieved with encryption, tests must be run to ensure that the system offers adequate security and cannot be easily compromised by other users or by the provider itself. The user must be given access to the abovementioned range of options via a convenient interface, along with the support required to implement user-driven application security. Both the cloud provider and the entire cloud network must implement a documented data privacy management system, to include IT security management and an event management system. We have already discussed the need for transparent audits by an independent entity. Unfortunately, however, the laws regulating this type of audit remain extremely limited.[133]

2. Certificate authorities, guidelines and elements of self-control

a.) German guidelines of BITKOM and BSI

150 The German 'Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V' (BITKOM) issued guidelines on cloud computingin October 2009. The BITKOM focuses mainly on cloud computing as a business innovation, a business model, its integration in IT architecture and its scenarios for application.

151 The 'Federal Office for Information Security'(BSI) defined minimum requirements for cloud computing providers. Cloud computing/compliance is explicitly addressed on page 16 of the guidelines.134

b.) ENISA

152 The European Network and Information Security Agency offers a risk assessment on cloud computing business model and technologies. The result is an in-depth and independent analysis[135] that outlines some of the information security benefits and key security risks of cloud computing. The report also providesa set of practical recommendations.

c.) Observations

153 Elements of self-control do in fact support compliance with data protection laws only if each partner of the cloud service contract meets the guidelines' requirements. The problem remains for cloud users to prove that the contract partner fulfils all requirements set out in the contract. Approaches could be as follows:

- conclusion of a Service Level Agreement (SLA);
- periodic control/audit (not realizable in a dynamic cloud surrounding);
- ISO 27000;
- reliance on BSI (cloud user within Germany) or ENISA (cloud user within EU) Guidelines;
- agreement upon a Privacy Seal, e.g. the Privacy Seal of the Data Protection Authority of Schleswig-Holstein;[136]
- common criteria; or
- restriction on networks of trusted partners instead of direct audits.

3. International standards

a.) Ontario Global Privacy Standards and Privacy by Design

154 In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, a Working Group was convened for the purpose of creating a single Global Privacy Standard. This Group tried to harmonize various sets of fair information practices into one Global Privacy Standard. The first step was a 'Gap Analysis', a process of comparing leading privacy practices and codes from around the world, comparing their various attributes and the scope of the privacy principles enumerated therein. After identifyingstrengths and weaknesses of the major codes in existence, the Group tabled its Gap Analysis with the Working Group of Commissioners. The work on harmonizing the principles into a single set of fair information practices led to the development of the Global Privacy Standard (GPS),[137] which builds upon the strengths of existing codes containing privacy principles and reflects an enhancement by explicitly recognizing the concept of 'data minimization' under the 'collection limitation'principle. After some subsequent drafts, the final version of the GPS was formally tabled and accepted in the UK on 3 November 2006 at

the 28th International Data Protection Commissioners Conference.

155 Privacy by Design is a concept brought to light by Ann Cavoukian, Information & Privacy Commissioner from Ontario, Canada:

> *Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation. Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS Plus — taking a positive-sum (full functionality) approach, not zero-sum. That's the 'Plus' in PETS Plus: positive-sum, not the either/or of zero-sum (a false dichotomy). Privacy by Design extends to a 'Trilogy' of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure. Principles of Privacy by Design may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.*[138]

b.) Privacy Toolkit

156 The 'Privacy Toolkit',[139] published by the Task Force on Privacy and the Protection of Personal Data of the International Chamber of Commerce (ICC), is an example of another private sector instrument. This toolkit is an international business guide for policymakers and aims at governments seeking an innovative approach to privacy that balances the needs of governments, individuals and the economy as a whole. It outlines guiding principles for privacy that draw upon the OECD privacy guidelines and suggests practical ways to put the principles to work:

> *ICC fully supports the fundamental right to privacy and encourages businesses to comply with national and international privacy rules. But working with governments to implement privacy protection requires early policy input into how privacy rules are created while keeping in mind that overly restrictive or conflicting privacy requirements can be a big barrier to international business. Privacy Toolkit was developed to communicate the business approach to privacy protection and to serve as a guide for governments developing their own policies. It outlines the characteristics and benefits of flexible privacy protection regimes that are built into business processes. The booklet was prepared by the ICC Commission on E-Business, IT and Telecoms. Christopher Kuner, Partner, Hunton & Williams, Brussels, and Chair of ICC's data protection task force, said: 'Privacy and business competitiveness are not either/or options. Appropriate privacy protection is a business enabler, not a barrier. But it's an ongoing process that needs to be responsive to new technology, business methods and opportunities. Flexibility is essential. Privacy Toolkit shows that the most important aspect of privacy protection is not how it is achieved, but simply that it works.' The booklet also includes a series of steps for governments to achieve appropriate and effective privacy protection regimes. Following Privacy Toolkit recommendations will ensure that the resulting privacy regime serves both business and the consumer without running the risk of stifling development, innovation and growth.*[140]

c.) ISO and IEC

157 ISO, the International Organization for Standardization, developed international standards in many areas that are essential to everyday life. On technology standards ISO and IEC, the International Electrotechnical Commission, which is responsible for standards in the field of electrics and electronics, are cooperating together.

158 In addition to legal standards, technical standards for effective data protection have a high priority because a large number of technical standards affect privacy interests to a considerable extent. Through a privacy-friendly design in these standards at an early stage, potential risks for privacy of individuals could be reduced or entirely eliminated. Unfortunately, the Data Protection Authorities rarely have an adequate possibility to apply their expertise in the relevant bodies, due to their existing equipment and staff and the great variety of technical standards.

159 The German Data Protection Authority of Schleswig-Holstein (ULD)[141] is involved in the joint Working Group 'Identity Management and Data Protection Technology' of ISO and IEC. Central standards the ULD is working on include the 'ISO 29100 - Privacy Framework', a framework standard that defines basic concepts and principles regarding privacy, and 'ISO 29101 - Privacy Reference Architecture', which outlines privacy-friendly IT architecture.

D. The destination: A privacy regime across the globe

160 Bygrave states that 'the chances of achieving, in the short term, greater harmonization of privacy regimes across the globe are slim'.[142] There are still substantial cultural and legal differences between various states and regions regarding their approach to data protection, and most of them still have no data protection law at all. In addition, there is increasing tension between the global nature of data processing and the still mainly national or regional nature of data protection law. Thus, there do not yet seem to be sufficient grounds for recognizing a global legal right to data protection in the same way that other fundamental, universal human rights are recognized.

161 Nevertheless, there is still hope, consisting in a mixture of many little steps and one simultaneous big stride. But what steps must be taken? The former

should combine some main rationales of the different legal frameworks on a short-term basis:

- The avoidance of gaps in data protection. The lack of harmonized standards for data protection around the world and the lack of any data protection legislation in most states create risks for the processing of personal data.[143]

- The facilitation of global data flows. A growing number of databases are made accessible globally on the Internet. Thus, the same data transfer may be subject to a large number of differing data protection standards, which creates substantial compliance burdens and uncertainty for business, and particular problems with transatlantic data conflicts.

- The installation of an international body, responsible for further consultations towards an international legal analysis of a draft paper on global data protection. As data protection law is a mixture of various legal areas – such as human rights law, public law, private law, and others – it makes it difficult to find a sufficiently strong, dynamic and representative international body. The WTO is occasionally named as such a body, but it is hampered by its commercial bias. The ILC already has produced instruments in many areas of public international law, but it does not seem well suited to deal with a strongly politically charged area like data protection. Institutions such as the Council of Europe seem to be too closely tied to one region, and the OECD has a limited membership. Other international organizations such as the ITU, UNESCO or the WTO seem too specialized. Thus, the draft of a truly international convention within the framework of the UN seems more promising, initiating a UN Human Rights Council-sponsored process with a view to a future global treaty.

- The recognition of the technology itself as a third party between data controllers and data subjects, using new technologies towards information and communication technology (ICT) privacy measures. The authorities charged with data protection must penetrate the forums[144] where important decisions are being made-about technical network infrastructure, communication protocols and the characteristics of our browsers.

- The unification of the most eminent specialists worldwide in data protection law under the ILC authority, as the official legal advisor for the UN and responsible for the further development of worldwide principles. These should require the following: the principles of openness in personal data systems, liability in operation of the systems and responsibility of the data-keepers for following legal and procedural guidelines. Furthermore, data held should not be excessive in relation to the stated purposes of the systems, proscribing release or sharing of data held in files without the consent of the individual, and foreseeing creation of national-level public offices charged with monitoring and enforcing individuals' interests in treatment of 'their' data.[145]

162 Solve problems within the EU-DPD's reform, which Professor Millard, leader of the Cloud Legal Project at Queen Mary, University of London, perfectly outlines:

> *Unless further changes are made to clarify and harmonise data protection rules across the EU, the draft Regulation may drive business away from Europe, and still fail to deliver effective protection for individuals. Uncertainty will persist as to whether particular non-European cloud providers and cloud users are regulated in the EU and, if so, which law(s) will apply to them. This may discourage the development of EU data centres and the use of EU cloud services generally. Furthermore, the draft Regulation fails to close a loophole which may undermine protection for some EU residents when they use services provided by non-EU cloud providers. The use of cloud computing may also be inhibited by additional restrictions on the transfer of personal data outside Europe, including cumbersome regulatory approval requirements. Given the ease of global data transmission and remote access over the Internet, and the increasingly fragmented nature of data storage, what matters most for privacy and security is who can access the data in intelligible form. This is now more important for privacy than data location. The draft Regulation will impose substantial new compliance obligations on businesses, as well as greatly expanding the roles of the European Commission and national regulators, all of whom will need extra resources. It is unclear how this will be financed, especially in the current economic climate. The proposed abolition of registration fees is a step towards reducing red tape, but proper provision for the adequate funding of supervisory authorities in performing their expanded duties will be essential if the draft Regulation is to protect individuals and facilitate the free flow of data.*[146]

- The political integration of APEC into the draft of an international convention, maybe through a membership of the trade-friendly but at the same time EU-friendly WTO into the APEC Community, accessing APEC states to the CoE Convention 108 and to the Additional Protocol.

- The reduction of the scope of instruments to data protection, perhaps containing exceptions such as data processing by law enforcement.

- The finding of a balance between security and privacy issues. Maintain the efforts to prevent future terrorist attacks without infringement of individual privacy rights and civil liberties.

- The adaption of the level of strictness of global data protection standards. Kuner states that this balance puts future data protection law in a dilemma, because

if global standards were set too high, then it is likely that many States would be reluctant to enact them, while if they were set too low, then States and entities with a long tradition of data protection law might oppose them as watering down their existing standards (this could be a particular problem for the European Union).[147]

163 The latter should not let the ultimate goal out of sight of a globally binding convention of data protection. This big stride should be realized through a globalization of the CoE Convention 108. It is true that it would take longer to draft and approve such a multilateral convention, and experience shows that states tend to give a low priority to the implementation of such conventions; in addition, this convention would be subject to many more political hurdles, especially because of the difficulty of re-opening an existing instrument. But there are more advantages that cannot be ignored. The CoE initiative under Article 23 (1) signals a possible way of side stepping the cumbersome process of developing a new convention on privacy by starting with an instrument already adopted 'within the region with the most concentrated distribution of privacy laws, Europe'.[148] Thus, it would be a much quicker solution than waiting for some new globally enforceable treaty. Its membership includes forty European states, twenty of whichhave acceded to its Additional Protocol; five accessions are from outside the EU. The CoE Convention 108 is based on the most important minimal right of data protection law, the human right of privacy. This principle is recognized worldwide. The CoE Convention 108 and Additional Protocol could provide a reasonable basis (a common and moderate privacy standard) for guarantee of free flow of personal data between parties to the treaty, both as between Asia-Pacific countries and as between those countries and European countries. Such invitation and accession to both would be likely to carry with it the benefits of a finding of adequacy under the EU Directive, or make one irrelevant.[149]

164 Summing up the problems between the poles of privacy and cloud computing, a truly remarkable recommendation[150] has been issued by the European Network and Information Security Agency (ENISA). The agency determined legal recommendations to the European Commission: 'Most legal issues involved in cloud computing will currently be resolved during contract evaluation (i.e., when making comparisons between different providers) or negotiations. The more common case in cloud computing will be selecting between different contracts on offer in the market (contract evaluation) as opposed to contract negotiations. However, opportunities may exist for prospective customers of cloud services to choose providers whose contracts are negotiable. Unlike traditional Internet services, standard contract clauses may deserve additional review because of the nature of cloud computing. The parties to a contract should pay particular attention to their rights and obligations related to notifications of breaches in security, data transfers, creation of derivative works, change of control, and access to data by law enforcement entities. Because the cloud can be used to outsource critical internal infrastructure, and the interruption of that infrastructure may have wide ranging effects, the parties should carefully consider whether standard limitations on liability adequately represent allocations of liability, given the parties' use of the cloud, or responsibilities for infrastructure. Until legal precedent and regulations address security concerns specific to cloud computing, customers and cloud providers alike should look to the terms of their contract to effectively address security risks'[151]

■

1 Christopher Kuner, 'An international legal framework for data protection: Issues and prospects'', Computer law & Security Review, 2009, vol. 25, p. 307-317 [308]; cited as: ''Kuner, An international legal framework for data protection''.

2 ''Google is calling for a discussion about international privacy standards which work to protect everyone's privacy on the internet. These standards must be clear and strong, mindful of commercial realities, and in line with oftentimes divergentpolitical needs. Moreover, global privacy standards need to reflect technological realities, taking into account how quickly these realities can change''; <http://googlepublicpolicy.blogspot.com/2007/09/call-for-global-privacy-standards.html>.

3 Die Welt, 'Die Post-PC-Ära hat begonnen', 6 March 2012, p. 11

4 http://www.bitkom.org/

5 Frankfurter Allgemeine Zeitung (FAZ), 4 March 2012.

6 Christopher Kuner, 'An international legal framework for data protection', p. 308.

7 Speech of Angela Merkel at the CeBIT fair, FAZ, 6 March 2012.

8 Viviane Reding, 'Privacy standards in the digital economy: Enhancing trust and legal certainty in transatlantic relations', 23 March 2011, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/210>.

9 Viviane Reding, 'Privacy matters: Why the EU needs new personal data protection rules', 30 November 2010, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700>.

10 <http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf>.

11 <http://www.privacyconference2008.org/>.

12 <http://www.privacyconference2009.org/>.

13 <http://www.privacyconference2010.org/>.

14 <http://www.privacyconference2011.org/>.

15 <http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_R_001_Intnl_Standards_ENG.pdf>.

16 http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html

17 <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf>.

18 Hazel Grant, 'Data protection 1998-2008', in: Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 44-50 [p. 44].

19 Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950, CETS No. 194.

20 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities of 23 November 1995, No L. 281, p. 31.

21 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 13 December 2007, <http://europa.eu/lisbon_treaty/full_text/index_en.htm>.

22 Last amended by its Protocol No. 14 (CETS No. 194) as from the date of its entry into force on 1 June 2010.

23 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

24 <http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm>.

25 Paulde Hert / Eric Schreuders, 'The Relevance of Convention 108. European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future', from DP Conference (2001) Reports, p. 63-76, The Council of Europe (ed.), <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/events/conferences/DP%282001%29Proceedings_Warsaw_EN.pdf>, p.42.

26 ChristopherKuner, 'An international legal framework for data protection', p. 308.

27 ChristopherKuner, 'An international legal framework for data protection', p. 309.

28 Stated already in the 19th century by Warren/Brandeis, 'The Right to Privacy', Harvard Law Review, vol. IV no. 5, 15.12.1890, <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

29 Now addressed by the European Commission during its consultations for the proposal of a comprehensive reform of the EU's 1995 data protection rules, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf

30 as an example on the image from right to left: storage, print, compute.

31 Ina Schiering / Markus Hansen: Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

32 Ina Schiering / Markus Hansen: Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

33 Ina Schiering / Markus Hansen: Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

34 Ina Schiering / Markus Hansen: Sind Privacy und Compliance im Cloud Computing möglich? Heise-Forum Sicherheit und IT-Recht, CeBIT 2010, 4 March 2010

35 Art. 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>.

36 See below.

37 Art. 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"', 16 February 2010, WP 169

38 C. Ian Kye, / Gabriel M.A. Stern, 'Where in the World Is My Data? Jurisdictional Issues with Cloud Computing', 30 March 2011, p. 1, <http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf>.

39 Robert Gellman, 'Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing', 23 February 2009, <http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf>.

40 Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 12, 16 January 2001, p. 1–23.

41 C. Ian Kye, / Gabriel M.A. Stern, 'Where in the World Is My Data? Jurisdictional Issues with Cloud Computing', 30 March 2011, p. 5, <http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf>.

42 Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), Official Journal of the European Union, L 177/6 EN.

43 Juliette Garside, 'How global laws protect your data', The Guardian, 17 October 2011, <http://www.guardian.co.uk/cloud-technology/global-laws-protect-your-data>.

44 See below.

45 These methods will be examined below.

46 Switzerland, Canada, Andorra, Faeroe Islands, Argentina, Guernsey, Isle of Man, Israel.

47 Some Latin American countries and Morocco, which has recently adopted new legislation to protect personal data.

48 Art. 29 Data Protection Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC', 24 October 1995, WP 114, p. 6.

49 Art. 29 Data Protection Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context', 13 September 2001, WP 48, p. 3.

50 Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, Official Journal L 181 , 04/07/2001, p. 0019 – 0031.

51 Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, Official Journal L 385 , 29/12/2004, p. 0074 – 0084.

52 Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal-data to processors established in third countries under Directive95/46/EC of the European Parliament and of the Council, Official Journal L39, 12/02/2010, p. 0005 – 0018.

53 Pub.L. 106-102.

54 Pub.L. 108-159.

55 Pub.L. 104-191.

56 Pub.L. 107-56, 115 Stat. 272 (2001).

57 Pub.L. 99-508.

58 As an example, on the basis of its data security regime (201 C.M.R. 17.00), Massachusetts requires entities to develop and implement a written information security plan to create technical and physical safeguards for the protection of personal data of Massachusetts residents.

59 26 U.S.C. §§ 6713, 7216; 26 C.F.R. § 301.7216.

60 After 2005 amendments, 26 C.F.R. §301.7216-3(b)(4).

61 Stephen J. Kobrin, 'Safe harbours are hard to find: The transatlantic data privacy dispute, territorial jurisdictions and global governance', Review of International Studies, British International Studies Association, 2004, iss. 30, p. 111-131 [p. 115].

62 Stephen J. Kobrin, 'Safe harbours are hard to find: The transatlantic data privacy dispute, territorial jurisdictions and global

governance', Review of International Studies, British International Studies Association, 2004, iss. 30, p. 111-131 [p. 115].

63 Cécile de Terwangne, 'Is a Global Data Protection Regulatory Model Possible?', in: Reinventing Data Protection?, Gutwirth, Poullet, De Hert, de Terwangne, Nouwt (ed.), Springer Science, 2009, p. 179.

64 Michael P.Roch, 'Filling the Void of Data Protection in the United States: Following the European Example', Santa Clara Computer and High Technology Law Journal, February 1996, p. 71-96 [p. 93].

65 Video Privacy Protection Act, 18 U.S.C. 2710.

66 TRUSTe is an independent, privately held organization best known for its web privacy seal. TRUSTe runs the world's largest privacy seal program, with more than 2,000 websites certified, including the major Internet portals and leading brands such as IBM and eBay; <http://www.truste.com/index.html>.

67 <https://www.bbbonline.org/reliability/Rel_EN.asp>.

68 'CoE Convention 108', Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.01.1981, <http://conventions.coe.int/treaty/en/treaties/html/108.htm>.

69 <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf>.

70 Christian Toon, 'The new EU data protection guidelines', 23 February 2012, <http://www.continuitycentral.com/feature0957.html>.

71 Official Journal of the European Union, L 337/11, 18 December 2009.

72 Pub.L. 107-204, 116 Stat. 745, enacted July 29, 2002.

73 Official Journal of the European Union, L 157/87, 9 June 2006.

74 GuidoSanchidrian, 'EuroSOX is not US-SOX ', 20 March 2009, <http://www.symantec.com/connect/articles/eurosox-not-us-sox>.

75 NeelieKroes, Vice-President of the European Commission responsible for the Digital Agenda, EU Data Protection Reform and Cloud Computing 'Fuelling the European Economy' event, Microsoft Executive Briefing Centre Brussels, 30 January 2012, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/40&format=HTML&aged=0&language=EN&guiLanguage=en>.

76 Ian Walden / Christopher Millard / Kuan Hon,'Data protection law creates cloud of uncertainty for cloud computing', 21 November 2011, <http://www.ccls.qmul.ac.uk/news/2011/59982.html>.

77 Ian Walden / Christopher Millard / Kuan Hon, 'Data protection law creates cloud of uncertainty for cloud computing', 21 November 2011, <http://www.ccls.qmul.ac.uk/news/2011/59982.html>.

78 <http://www.cloudlegal.ccls.qmul.ac.uk/>.

79 Stephen J. Kobrin, 'Safe harbours are hard to find: The transatlantic data privacy dispute, territorial jurisdictions and global governance', Review of International Studies, British International Studies Association, 2004, iss. 30, p. 111-131 [p. 111].

80 Stephen J. Kobrin, 'Safe harbours are hard to find: The transatlantic data privacy dispute, territorial jurisdictions and global governance', Review of International Studies, British International Studies Association, 2004, iss. 30, p. 111-131 [p. 112].

81 While the minimum data for completing a booking is quite small, a PNR data typically contains 34 fields of data of a sensitive nature, like the passenger's full name, date of birth, home and work address, telephone number, e-mail address, credit card details, as well as the names and personal information of emergency contacts.

82 Council Decision 2007/551/CFSP/JHA of 23 July 2007, OJ L204/16.

83 Sophia In't Veld, 'New PNR proposals an improvement on past', Press Release, 22 September 2010, <http://www.alde.eu/press/press-and-release-news/press-release/article/new-pnr-proposals-an-improvement-on-past-33971/>.

84 <http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2000:215:SOM:DE:HTML>.

85 Stephen J. Kobrin, 'Safe harbours are hard to find: The transatlantic data privacy dispute, territorial jurisdictions and global governance', Review of International Studies, British International Studies Association, 2004, iss. 30, p. 111-131 [p. 121].

86 Reidenberg, 'E-Commerce and Transatlantic Privacy', in: Houston Law Review, 2001, iss. 38, p. 717-749 [717], <http://reidenberg.home.sprynet.com/Transatlantic_privacy.pdf>, cited as: 'Reidenberg, E-Commerce and Transatlantic Privacy'.

87 <https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_10neu.pdf>.

88 Art. 1 of the Decision regarding the Safe Harbor Principles as an Adequate Level of Protection; [2000] O.J. L 215/7.

89 <http:///www.export.gov/safeharbor> [Last accessed: 30 May 2011].

90 Viviane Reding, 'Privacy standards in the digital economy: Enhancing trust and legal certainty in transatlantic relations', 23/03/2011, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/210>.

91 On December 10, 1948 the General Assembly of the United Nations adopted and proclaimed the 'Universal Declaration of Human Rights' (UDHR), http://www.un.org/en/documents/udhr/index.shtml

92 'ICCP', 16 December 1966, http://www.un.org/millennium/law/iv-4.htm

93 'UN Computerized Guidelines', 14 December 1990, UN Doc E/CN.4/1990/72

94 LeeBygrave, 'Data Protection Law: Approaching Its Rationale, Logic and Limits', The Hague/London/New York, Kluwer Law International, 2002, p. 32

95 http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24464/20091.pdf

96 http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24465/20092.pdf

97 <http://www.bfdi.bund.de/bfdi_forum/showthread.php?t=689>.

98 <http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_R_001_Intnl_Standards_ENG.pdf>.

99 LeeBygrave, 'International agreements to protect personal data', in: Global Privacy Protection: The First Generation, James B. Rule & Graham Greenleaf (ed.), 2007, p. 28.

100 'Guidelines for the Security of Information Systems', in the following 'OECD 1992 Security Guidelines', 26 November 1992; Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, in the following 'OECD 2002 Security Guidelines', 25 July 2002.

101 Guidelines for Cryptography Policy, in the following 'OECD Cryptography Guidelines', 27 March 1997.

102 Guidelines for Consumer Protection in the Context of Electronic Commerce, in the following 'OECD Consumer Protection Guidelines', 9 December 1999.

103 The 'Declaration on Transborder Data Flows', the 'Declaration on the Protection of Privacy', the report 'Privacy Online: OECD Guidance on Policy and Practice', the report 'Making Privacy Notices Simple: An OECD Report and Recommendations' and the 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy'.

104 <http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+privacy+Framework.pdf/$file/APEC+privacy+Framework.pdf>.

105 Graham Greenleaf, 'Five years of the APEC privacy framework: Failure or promise?', in: Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 28-43 [p. 28].

106 Gabriela Kennedy / Sara Doyle / Brenda Lui/ et al., 'Data protection in the Asia-Pacific region', Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 59-68 [p. 60].

107 Graham Greenleaf, 'Five years of the APEC privacy framework: Failure or promise?', in: Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 28-43 [p. 31]; see also a critical examination of these principles in Kennedy / Doyle / Lui / et al., p. 61; de Terwangne, p. 184.

108 Graham Greenleaf, 'Five years of the APEC privacy framework: Failure or promise?', in: Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 28-43 [p. 32].

109 Gabriela Kennedy / Sara Doyle / Brenda Lui / et al., 'Data protection in the Asia-Pacific region', Computer Law & Security Review, 2009, vol. 25, iss. 1, p. 59-68 [p. 61].

110 Abraham L. Newman, 'Protectors of Privacy: Regulating Personal Data in the Global Economy', Cornell University Press, 2008, p. 103.

111 <http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_009.pdf>.

112 Nigel, 'APEC Cross Border Privacy Rules: Ready to party but will anyone come?', 30 September 2011, <https://www.privacyinternational.org/article/apec-cross-border-privacy-rules-ready-party-will-anyone-come>.

113 <http://www.ipc.on.ca/index.asp?navid¼46&fid1¼575>.

114 <http://www.globalnetworkinitiative.org/index.php>.

115 Souichirou Kozuka, 'The economic implications of uniformity in law', in: Uniform Law Review, 2007, part 4, p. 683-696, <http://www.unidroit.org/English/publications/review/articles/2007-4-kozuka-e.pdf>, p. 693, stating that 'ironically, the more popular a Convention is, the more difficult it is to amend the uniform law in a timely manner'.

116 UNGA Res 174(II) (21 November 1947).

117 Statute of the International Law Commission, Art.1(1).

118 ILC, Report on the Work of its Fifty-Eighth Session, UN Doc A/61/10 para. 257.

119 Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations: Annex 1b, General Agreement on Trade in Services (GATS), Preamble.

120 LeeBygrave, Lee, 'Privacy protection in a global context: A comparative overview', in: Scandinavian studies in law, Peter Wahlgren (ed.), Stockholm Institute for Scandinavian, Law, iss. 47, 2004, p. 348, cited as: 'Bygrave, Privacy Protection in a Global Context'.

121 GrahamGreenleaf, p. 41.

122 This limitation is probably also valid for the relation to the third person affected by the offence.

123 Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/ECof the European Parliament and of the Council, Official Journal L39, 12/02/2010, p. 0005 – 0018.

124 Art. 29 Data Protection Working Party, 'Working document setting up a table with the elements and principles to be found in Binding Corporate Rules',24 June 2008, WP 153.

125 The 'DüsseldorferKreis' is a working group of representatives from Germany's sixteen state data protection authorities that provides a uniform 'German' approach to data protection questions.

126 Art. 29 Data Protection Working Party, 'Working document setting up a framework for the structure of Binding Corporate Rules', 24 June 2008, WP 154.

127 <http://www.cloudsecurityalliance.org/>.

128 <http://www.eurocloud.de/>.

129 <http://www.tclouds-project.eu/>.

130 Lawrence Lessig,'Code and other laws of cyberspace', Basic Books, 1999, p. 6.

131 For example, the International Organization for Standardization (ISO), TMB Task Force on Privacy, June 2008.

132 ChristopherKuner, 'An international legal framework for data protection', p. 314; for example, the ITU's international allocation of radio-frequency spectrum has established a de facto standard that is followed in 191 ITU member states, and the W3C has published over 110 technical standards for the World Wide Web; see <http://www.w3.org/consortium>.

133 Thilo Weichert, 'CloudComputing & Data Privacy', p. 10-11, <https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf>.

134 <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile>.

135 <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport>.

136 <https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm>.

137 <http://www.ipc.on.ca/images/Resources/gps.pdf>.

138 <http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf>.

139 <http://www.iccwbo.org/uploadedFiles/TOOLKIT.pdf>.

140 <http://www.iccwbo.org/policy/ebitt/id5289/index.html>.

141 <https://www.datenschutzzentrum.de/>.

142 LeeBygrave, 'Privacy protection in a global context: A comparative overview', p. 48.

143 Christopher Kuner, 'An international legal framework for data protection', p. 308.

144 Many international private organizations are defining specifications of the network´s and terminal functioning without oversight or control by governments, such as the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN) or the World Wide Web Consortium (W3Consortium)

145 James B. Rule, 'Conclusion', in: 'Global privacy Protection: The First Generation', James B. Rule and Graham Greenleaf (ed.), Edward Elgar Publishing, 2009, p. 262-263

146 Christopher Millard, 'Proposed EU Data Protection laws unlikely to promote cloud computing, warns Professor Millard', 1 February 2012, http://www.qmul.ac.uk/media/news/items/hss/63123.html

147 Christopher Kuner, „An international legal framework for data protection', p. 316.

148 Graham Greenleaf, p. 41.

149 Graham Greenleaf, p. 42.

150 http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

151 ENISA Report, 'Benefits, risks and recommendations for information security', p. 6, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Along the Road to Uniformity – Diverse Readings of the Court of Justice Judgments on Copyright Work

by **Mireille van Eechoud,** PhD., Amsterdam, Insitute for Infomation Law University of Amsterdam.

Abstract: For a long time, EU law's impact on the meaning of copyright work seemed limited to software and databases. But recent judgments of the CJEU (Infopaq, BSA, Football Association [Murphy], Painer) suggest we have entered an era of harmonization of copyright subject matter after decades of focus on the scope of exclusive rights and their duration. Unlike before, however, it is the Court and not the legislator that takes centre stage in shaping pivotal concepts. This article reviews the different readings and criticisms evoked by the recent case law on copyright works in legal doctrine across the EU. It puts them in the wider perspective of the on-going-development towards uniform law and the role of the preliminary reference procedure in that process.

Keywords: Copyright; Databases; CJEU; Infopaq; BSA; FA Premier League; Painer;

Recommended citation: Mireille van Eechoud, Along the Road to Uniformity Diverse Readings of the Court of Justice Judgments on Copyright Work, 3 (2012) JIPITEC, 1, para 60.

A. Introduction

1 It was with slight apprehension but still a fair amount of confidence that we wrote in our 2009 book on the harmonization of EU copyright law[1] that after nearly two decades of EU copyright-specific legislation, the subject matter of copyright protection was only harmonized to a limited extent. The Berne Convention and subsequent international treaties had already had a certain unifying effect on domestic copyright laws, of course, but the EU directives had not gone beyond those international norms, with the exception of software, databases and photographic works. The slight apprehension arose when, just after the final proofs had been sent off to the publishers, the *Infopaq* judgment was handed down. After some pleading the publisher agreed to a last-minute change to the paragraphs on the transient copying exemption of the Information Society Directive, which after a quick read seemed the bigger issue addressed by the Court.

2 In retrospect, of course, in a short space of time *Infopaq* became regarded as the landmark judgment in which the Court of Justice started to elaborate an EU-wide concept of copyright 'work'. A string of cases followed in which the Court explicitly addressed when something is a copyrighted work: *BSA* (2010), *Football Association Premier League* (also known as 'Murphy', 2011), *Painer* (2011), and *Football Dataco* (2012),[2] with more cases pending.

3 It is still too early to establish the exact impact of the Court's judgments on the copyright laws of Member States, even if national courts have started to refer to the CJEU's judgments. Meanwhile, notably *Infopaq* and *BSA* have already generated lots of commentary from copyright scholars across the EU. In this article, my primary aim is to analyse the reception of these cases, exploring the type of readings legal scholars take. This should give us a more comprehensive understanding of the issues at stake. I distinguish 'positivist-comparative' readings, which address what the harmonized law now is and what impact this has on national laws, from methodological-critical readings of the case law. The latter comprise a variety of criticisms on the tools the Court uses for its apparent construction of an EU-wide work standard, which is the most controversial outcome of the cases.

4 The preliminary reference procedure plays a crucial role in legal practice as it is the primary instrument through which the Court shapes EU copyright law. We know surprisingly little about how it operates in copyright, though, and in the final part I advocate

that scholars engage with the role of the preliminary reference procedure as an instrument of further harmonization and its limitations. But first, by way of introduction, a brief reminder of how the existing directives deal with the copyright work.

B. The Europeanized copyright landscape

5 Until 1991 there was no secondary EU law on copyright. But the Court of Justice had begun to apply primary law to intellectual property in the 1970s and 1980s. First came judgments on how territorially defined national copyrights and related rights were to be viewed in light of the EC Treaty provisions aimed at ensuring the free movement of goods in the internal market. From the 1990s onwards the Court also addressed equal treatment of citizens (non-discrimination) and the impact of competition law on the exercise of copyright, especially as regards the prohibition to abuse a dominant position of what is now Article 102 TFEU.[3]

6 Work on the approximation of domestic copyright laws for the purpose of establishing the single internal market started in earnest in the late 1980s. In fact, of today's seven copyright-specific directives, all but one can be traced back to the first major policy documents: the Commission Green Paper on the Challenge of Technology of 1988 and its 1991Follow-up.[4]These set the stage for the 1991 Computer Programs Directive (91/250/EEC, codified by 2009/24/EC), the 1992 Rental and Lending Directive (codified by 2006/115/E), the 1993 Satellite and Cable Directive (93/83/EEC), the 1993 Term Directive (codified by 2006/116/EC, amended by 2011/77/EU), the 1996 Database Directive (96/9/EC) and the 2001 Resale Right Directive(2001/84/EC).

7 Some of the topics in the 2001 Information Society Directive (2001/29/EC) were already on the 1988 agenda also. But the more comprehensive ideas on its scope are found in the 1995 Commission Green Paper on Copyright and Related Rights in the Information Society and the 1996 Follow-up.[5] Limitations and exceptions, which are an important part of the Information Society Directive, were initially not really on the agenda. The 1995 Green Paper was all about adapting exclusive rights to the digital environment, with a heavy focus on the scope of economic rights online and on the protection of digital rights management information and technological protection measures.

8 As is well known, the process thatled to the Information Society Directive ran in tandem with the creation of the 1996 WIPO Copyright Treaty (and the WPPT), which entered into force for the EU and its Member States as the WCT on 14 March 2010. The WCT, too, is primarily concerned with making international copyright norms more suited tothe digitally networked environment and contains no new norms on subjectmatter beyond those already laid down in the BC and the TRIPS Agreement.

C. Works in the directives

9 With the exception of the Information Society Directive then, all instruments basically deal with a very limited set of copyright issues (duration), for only certain kinds of works (software, databases) or certain types of exploitation (rental and lending, satellite and cable, resale). From that perspective it is not surprising that, taken together, the directives shed little light on what the constitutive requirements for copyright are. If one considers the green papers and legislative preparatory materials, clearly there were only two harmonization projects where the requirements for protection as a copyright work were a key issue: the Computer Programs and Database Directives.

10 The respective directives provide that a computer program or database is protected on condition that'it is original in the sense that it is the author's own intellectual creation'. It is generally accepted that this standard represents a compromise criterion. It evens out different local standards of originality and also meant do away with other adjacent criteria (such as merit or certain aesthetic appeal)[6] that were sometimes applied to these fairly young branches of the copyright tree. Crucially, both directives do not just lay down the originality test, but also specify what kind of 'work' a database or computer program is and to what elements protection applies. Because the Database Directive introduced a sui generis intellectual property right in databases in addition to 'normal' copyright, it obviously made particular sense to elaborate what the object of either right is.

11 Computer programs were not defined as a distinct genre, but classed in the broader category of literary works as named in Article 2 Berne Convention. At the time it was not at all universally accepted that software was to be regarded as a literary work under the Berne Convention. In its 1988 Green Paper, the European Commission also professed that a change to the Berne Convention would be needed to bring software within its scope.[7] In the event, of course, international protection was secured through the TRIPs Agreement (1992) and the WCT (1996), which essentially impose an obligation on contracting states to treat computer programs as literary works within the meaning of the Berne Convention.

12 The directive may not define the meaning of 'computer program', but it does specifyin some detail what characteristics are protected: 'the expression in any form of a computer program', but not'ideas and prin-

ciples which underlie any element of a computer program, including those which underlie its interfaces' (Art. 1 Computer Programs Directive, cf. Art. 9(2) TRIPs, Art. 2 WCT). The recitals give additional pointers on the protection of logic, algorithms and programming languages.

13 The Database Directive does not classify a database as a literary work or other type. In fact, the directive does not even speak of the database directly as a 'work' of any kind, just as an 'intellectual creation'. So does TRIPs (Art. 9) and in its wake the WCT (Art. 5). Of course, all these references echo Article 2(5) Berne Convention, which deals with the protection of collections of literary or dramatic works.[8] A database is 'a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means' (Art. 2 Database Directive). Its original character must show in 'the selection or arrangement of the contents', and protection for the database as such does not extend to its contents (Art. 3 Database Directive, cf. Art. 5 WCT).

14 Photography is the third area where blackletter law is explicit about subsistence. Harmonization of the originality test here is accidental, one could say, as it is a side effect of the harmonization of the term of protection for all genres of copyright works. Some Member States have a two-tier regime for photographs (e.g. Austria, Germany). In the past, in these states photographs only qualified for copyright protectionas artistic works when they met a higher than average originality standard ('*Lichtbildwerke*' in the German copyright act).[9] A related right protects photographs as such ('*Lichtbild*').[10] When the term of protection was harmonized for all literary and artistic works, it had to be clarified that the new default term of 70 years post mortem auctoris applies to original photographs only.

15 Initially the Commission and European Parliament did not think the Term Directive would have to specify what constitutes a photographic work, or harmonize the originality test. This is what the Explanatory Memorandum to the original proposal for the Term Directive suggests. It states:

16 To secure proper harmonization of the term of protection, Article 3 provides that the term for photographic works is always to be seventy years, even though the actual substance of the right may be different, notably in Member States where there are different rules for different categories of photograph. Of course if the photograph is not protected under the law of the Member State in which the protection is claimed this paragraph will have no effect, as the substance of copyright entitlements is outside the scope of the Directive.[11]

17 The proposed article read: 'Protected photographs shall have the term of protection provided for in Article 1'. No amendments to this article and its accompanying recital were proposed by the European Parliament.[12] The subsequent Commission proposal amended in 1993 did not contain changes on photographic works either.[13] So it must have been in the Council that the decision was made to lay down a harmonized standard. Article 6 Term Directive now provides that '[p]hotographs which are original in the sense that they are the author's own intellectual creation shall be protected in accordance with Article 1 [meaning: term of protection of life of the author plus 70 years, mve]. No other criteria shall be applied to determine their eligibility for protection. Member States may provide for the protection of other photographs.'

18 The originality standard of Article 6 is viewed as lower than the traditional standard for photographic works in Austria and Germany.[14] The preparatory documents and the text of the Directive itself do not make clear whether the test for photographs is the same as that for software under the Computer Programs Directive.

19 Turning to the other directives, the term 'intellectual creation' is absent there, but obviously the term 'work' is also to be found. After all, it is the normal descriptive term to denote copyright subject matter and it is difficult to specify rights without referring to their object. The references to 'work' tend to be a function of whatever the core issue is that the provision regulates. For example, the Term Directive mentions different types or works such as joint works, collective works and anonymous works; for these the general rule for calculating the term of protection cannot be applied, so special rules were needed.

20 There is no indication, however, that by giving special calculation rules the legislator intended to harmonize notions of collaborative works. The most recent change to the Term Directive confirms this reading. For co-written musical works, a new calculation rule was added in 2011, precisely because in some jurisdictions musical compositions with lyrics are treated as a joint work, whereas in others they are viewed as separate works.[15] This can lead to differences in the term of protection for songs. Under the old rule, for example, the musical compositions of George Gershwin (d. 1937) would have become public domain in the UK and the Netherlands around 2008, while the lyrics by brother Ira (d.1983) remained in copyright. In these countries, lyrics and composition are viewed as separate works, not as a joint work. Obviously, if there was such a thing as a harmonized concept of a 'joint work', a special term rule for co-written music would be superfluous.

21 In the area of applied arts, EU design law clearly recognizes that although design protection and co-

pyright protection are cumulative, the requirements for protection under copyright are a matter for Member States. As recently as 2002 the Community legislator expressly provided that the standard of originality for copyright in works of applied art remains a matter for Member States to determine (Community Design Regulation Art. 96; similar in Art. 17 Design Directive).[16] The *Flos* judgment of January 2011 throws up many questions about the effect of this provision (see discussion below at para 5.1.2).[17]

22 The Resale Right Directive grants visual artists the right to a share in each sale of an artwork. It therefore contains a very particular reference to the subject matter it covers: the resale right exists for certain categories of 'art', namely 'original works of graphic or plastic art'made by the artist, as either a unique artefact or in a limited edition. Finally, in the Information Society Directive and other directives there are some very general references to 'the work'. Arguably this is to distinguish it from other protected subject matter that the directive also covers in the related rights area (rights of performers, etc.).

23 From this overview it seems clear that policy makers and legislators essentially did not give much thought to the constitutive requirements of copyright subject matter. The 'work'and its categories were generally not seen as concepts requiring a uniform EU interpretation, other than for software and databases. A similar chequered picture can be drawn for that other pivotal concept in copyright: the notion of author. The acquis communautaire has very little to say about who qualifies as (co-)author or initial owner of copyright, beyond some provisions for software, databases and film.

D. Works in the Court of Justice's case law: *Infopaq*, *BSA*, *FA Premier League* and *Painer*

24 So what has happened? How do we find ourselves in a situation where – as a matter of EU law, it seems – a harmonized originality standard is upon us? The reactions on the *Infopaq* judgment were still quite mixed in terms of what its impact would be. But the subsequent *BSA* ruling on the scope of the Computer Programs Directive brought home that the Court of Justice is actually extending the 'author's own intellectual creation' test from the Software and Database Directive to other areas. What is more, *BSA* also confirmed that the Court of Justice is moving towards a harmonized concept of 'the work of authorship'. The *Football Association Premier League* (*FAPL* aka Murphy) judgment on broadcasting of sports eventstows this line.[18] *Painer*is so recent most analysis is yet to come; this is even more true for *Football Dataco*.[19] In the former judgment the Court considered the subsistence of copyright in photographs under the Term Directive, but with reference to its earlier 'work' judgments. To help the analysis of the readings and criticisms the four judgments have evoked, a short reminder of the cases and the principal findings of the court are in order.

I. Infopaq: Reproduction in part of newspaper articles

25 The questions asked by the referring Danish court in *Infopaq*[20] concerned the interpretation of the reproduction right of Article 2 Information Society Directive and the exemption for acts of transient or temporary copying of Article 5.

26 *Infopaq* is a media monitoring and analysis business that provides customers with tailor-made summaries or snippets of newspaper and journal articles. The company digitizes print newspapers by scanning them. It then runs customized searches and stores the hits on a search term with surrounding words. The search results are then mailed to the customers. The judgment contains an example of what they would report back, in this case to a customer who is interested in the company TDC, the largest Danish telecom company:

> *4 November 2005 – Dagbladet Arbejderen, page 3:*
>
> *TDC: 73% 'a forthcoming sale of the telecommunications group TDC which is expected to be bought'.*

27 To determine whether (combinations of) such quotes constitute reproduction in part within the meaning of Article 2 Information Society Directive, the Court asked itself this preliminary question: To what subject matter does the reproduction right apply? According to Article 2, the short answer is 'works'. For copyright lawyers this is obvious shorthand for works of literature and art in a broad sense, to be distinguished from the other subject matter of related rights (in broadcasts, records, performances, first fixations of films) for which the reproduction right also exists. This is so obvious that we may overlook the possibility that to the non-specialized Court, the reproduction right of Article 2 Information Society Directive 'for authors, of their works' requires elaboration. Maybe that is why the Court set out to arrive at a more extensive answer.

28 It first lists what it considers to be the relevant international and EU law. The TRIPs Agreement is relevant because by approving this agreement, the EU obliged itself to comply with Article 2 Berne Convention as it elaborates which productions count as works of literature. It also lists the provisions on subject matter of the Computer Programs, Database and Term Directives. It then concludes that '[c]opyright...

[within the meaning of Art. 2(a) *Infosoc*] is liable to apply only in relation to a subject-matter which is original in the sense that it is its author's own intellectual creation'.

29 For newspaper articles –the type of text at issue here– the Court says that since individual words are not copyrightable, '[i]t is only through the choice, sequence and combination of those words that the author may express his creativity in an original manner and achieve a result which is an intellectual creation'. It then addresses whether short extracts of the kind made by *Infopaq* constitute reproductions in part under Article 2 Information Society Directive (consideration 47):

> *That being so, given the requirement of a broad interpretation of the scope of the protection conferred by Article 2 of Directive 2001/29, the possibility may not be ruled out that certain isolated sentences, or even certain parts of sentences in the text in question, may be suitable for conveying to the reader the originality of a publication such as a newspaper article, by communicating to that reader an element which is, in itself, the expression of the intellectual creation of the author of that article. Such sentences or parts of sentences are, therefore, liable to come within the scope of the protection provided for in Article 2(a) of that directive.*

II. BSA: Graphic User Interface as protected subject matter

30 Indisputably, to be able to say something about when there is reproduction of a 'work' – that is, to elucidate the infringement test to be applied – the Court had to go into the work concept at some level. In the *BSA* case, however, it had to address subject matter head on. The Czech Supreme Court asked whether a computer program's graphic user interface was part of the protected expression of a computer program within the meaning of the Computer Programs Directive. The case originated in a dispute between the Czech business software alliance, which sought permission from the Czech authorities to act as a collective management organization and secure compensation for the showing of GUI-generated images (e.g. as part of a television program).

31 The Court –like the Advocate General– rephrased the question as follows: Is 'the graphic user interface of a computer program ... a form of expression of that program within the meaning of Article 1(2)' of the Computer Programs Directive? The answer to that question is no, because according to the Court, protected software includes only '...the forms of expression of a computer program and the preparatory design work capable of leading, respectively, to the reproduction or the subsequent creation of such a program.' Since the graphic user interface 'does not enable the reproduction of that computer program, but merely constitutes one element of that program by means of which users make use of the features of that program', it is not protected under the Computer Programs Directive. This interpretation of the directive sparked much criticism and further questions.[21]

32 For our purposes, the most interesting element which arguably caused the most consternation is that the Court did not stop at concluding that GUIs are in principle not protected as software. Instead, it went on to say that 'it is appropriate to ascertain whether the graphic user interface of a computer program can be protected by the ordinary law of copyright' by virtue of the Information Society Directive. The Court refers to its *Infopaq* judgment and opines that 'the graphic user interface can, as a work, be protected by copyright if it is its author's own intellectual creation.'

III. Football Association Premier League: Infringement test for reproduction

33 Questions on copyright subsistence at first glance are incidental to what the Football Association Premier League (FAPL) joined cases are about. The central issue was whether the Premier League et al. could enforce its territorial licensing system for broadcasts of football matches, and prevent English pubs from showing matches using a foreign satellite decoder card rather than one from a supplier authorized for the UK. Murphy used Greek decoder cards in her pub and was prosecuted for infringement of the Copyright, Design and Patents Act 1988. This penalizes the reception of unauthorized transmissions. The Football Association and others also brought claims for infringement in the civil courts against Q.C. Leisure and others for supplying pubs in the UK with non-UK decoder cards. The administrative court before which Murphy appealed her conviction and the court seized with the civil action made preliminary references to the CJEU.

34 Much of the dispute turned on the free movement of goods and the freedom to provide services and on EU broadcasting law, specifically the two directives that regulate inter alia television broadcasting services: the Television without Frontiers Directive (revamped as Audiovisual Media Services Directive)[22] and the Conditional Access Directive.[23]

35 The copyright questions that were asked–like those in *Infopaq*– concerned primarily the scope of the reproduction right and the exemption for transient or incidental copying in the Information Society Directive.[24] The communication right also comes into play, but the judgment on this issue is of less relevance from the work perspective I am interested in here. The referring court had to determine under UK

law 'whether copies of a substantial part of any relevant copyright work are made in the decoder boxes or on the television screens' in the process of receiving and showing the broadcast football matches.

36 In a judgment that runs to almost 100 pages,[25] the English civil court gives a detailed analysis of the production of televised football matches and the potential types of protected subject matter involved to which the football association (rather than broadcasters) holds rights. The coverage is produced in a series of stages. The broadcasters film the football match using twenty or more cameras thatalso record ambient sound. These videoand audio streams are edited 'live' into a feed thatis relayed for further production to an off-site company that adds logos, video sequences, on-screen graphics (bars showing player or team names, yellow cards, etc.), music and English commentary. The resulting signal is transmitted by satellite to the foreign broadcaster, who can add its logo and commentary before sending the re-encrypted signals to the audience.

37 Judge Kitchin found that various elements embodied in the Premier League match coverage attracted copyright or related rights.[26] It is worth noting that the distinction between copyright works and related rights subject matter that is commonly made in the laws of most Member States (and the EU directives) is not as clearly present in UK law. Notably, the UK's Copyright Designs and Patents Act 1988 uses the term 'film' to mean audio-visual recording, which in other jurisdictions corresponds to the related right of producers in first fixations of films.[27] The 'cinematographic work' is known in other jurisdictions as a category of works of authorship, but is not a category as such under UK law.[28] In *Norowzian v Arks*, however, the Court of Appeal accepted that in principle a film can be considered a dramatic work under the CDPA.[29]

38 The parties agreed that copyright exists in certain graphics such as logos (as artistic works) and in the Premier League theme music ('anthem', as a musical work). The sound recording of the anthem was protected as such ('a related' right in EU-speak). So were various pieces of film, such as highlights of previous matches as well asthe video streams captured from the 20+ cameras used. As far as I understand it, the 'film copyrights' refer primarily to related rights in the audio-visual*recordings*, not to copyright in films as dramatic *works*.

39 The referring court did not ask what the preconditions are for copyright or related rights to exist in (elements of) the televised football matches under EU intellection property directives. It just wanted to know whether the Information Society Directive allowed it to apply a national infringement test or an EU one. In the UK the reproduction of a work or other protected subject matter is infringing if it involves copying a 'substantial part', either qualitatively or quantitatively. Was this test to be applied, or does the Information Society Directive prescribe a different one? Kitchin J asked, 'If it is a matter of interpretation of Article 2 of Directive 2001/29/EC, should the national court consider all of the fragments of each work as a whole, or only the limited number of fragments which exist at any point in time? If the latter, what test should the national court apply to the question of whether the works have been reproduced in part within the meaning of that Article?'[30]

40 The Court of Justice rephrases the question thus:

> *By this question, the referring court asks, in essence, whether Article 2(a) of the Copyright Directive must be interpreted as meaning that the reproduction right extends to the creation of transient sequential fragments of the works within the memory of a satellite decoder and on a television screen which are immediately effaced and replaced by the next fragments. In this context, the referring court is uncertain, in particular, whether it must conduct its appraisal by reference to all the fragments as a whole or only by reference to those which exist at a given moment.*

41 It then answers it by repeating its finding in *Infopaq*, that the reproduction right must be 'given an autonomous and uniform interpretation'. It also repeats that the reproduction right applies to works – that is,'subject-matter which is its author's own intellectual creation'– and that the reproduction right protects against copying in part, if the copied parts contain elements that are the expression of the intellectual creation of the author of the work.

42 With respect to the sub-question aboutthe test for reproduction in part, the Court opines as follows:

> *This means that the unit composed of the fragments reproduced simultaneously – and therefore existing at a given moment – should be examined in order to determine whether it contains such elements. If it does, it must be classified as partial reproduction... In this regard, it is not relevant whether a work is reproduced by means of linear fragments which may have an ephemeral existence because they are immediately effaced in the course of a technical process.*

43 With its focus on copying elements that reflect originality, the test the Court lays down can only apply to copyright works. This raises the question of the autonomous test(s) the Court will develop for the related rights subject matter covered by Article 2: broadcasts, performances, sound recordings and first fixations of film. The answer it gives in *FAPL* will not be of much use to the English courts, bearing in mind that the referring court's question was about frames of digital video and audio that form part of various types of protected productions.

44 The infringement test for copyright works is not crystal clear either. The first leg of the answer says not to take all the copied fragments together, but

only those that 'exist at a given moment' (which immediately raises the obvious question: what unit of time is relevant- seconds, nanoseconds, attoseconds?). The second leg could be read to imply that all copied fragments must be considered, in which case the Court contradicts itself. Or it just stresses that temporary copies are reproductions, which makes it a superfluous statement. The text of Article 2 Information Society Directive expressly includes all manner of temporary reproductions. In turn, of course, this explains why the exemption for transient copying in Article 5(1) was needed. A third and most plausible reading is that the Court makes clear it embraces a highly technical interpretation of copying, which basically means that any communication that involves digital equipment triggers the reproduction right.

45 In the event, the transient copying exemption brings relief. The Court considered the reception of the broadcast signals and the embedded content as a lawful use and any transient copying going on in the decoder and on the television screen met the relevant criteria for Article 5(1) to apply.

46 It is remarkable nonetheless that the Court of Justice glosses over the variety of protected subject matter involved and treats the question as if it concerned the reproduction of one copyright work of authorship. The Court set itself up on that train of thought earlier in the judgment, where it considered whether the CDPAs provisions which protect right holders against foreign decoder devices is compatible with the freedom to provide services in the internal market (Art. 56 TFEU). The protection of intellectual property rights can after all justify a restriction on the freedom to provide services.

47 In the analysis it simplified the intellectual property question, and in the process shed more light on what it considers to be a copyright work. The Court reasoned that *FAPL* cannot claim copyright in the Premier League matches themselves, as they cannot be classified as works under the *Infopaq* test. It arrives at this conclusion by reasoning that sporting events are not intellectual creations within the meaning of the Information Society Directive: 'That applies in particular to football matches, which are subject to rules of the game, leaving no room for creative freedom for the purposes of copyright.'

48 The implications of this view on copyright works, which seems to conflate an originality standard with the work concept, are discussed in more detail below. What is important to note at this stage is that in *FAPL*, the Court seems to affirm its position in *BSA*, which is that the Information Society Directive operates on the basis of a harmonized concept of the work of authorship.

49 What is also remarkable in *FAPL* is that the Court does not stop at dismissing sports events as copyright works –not a necessary statement to answer the referring court's intellectual property questions– but muses on potential alternative protection under domestic law: 'sporting events, as such, have a unique and, to that extent, original character which can transform them into subject-matter that is worthy of protection comparable to the protection of works, and that protection can be granted, where appropriate, by the various domestic legal orders.' An open invitation to Member States if ever there was one. At the same time, it implies that the harmonization of related rights has resulted in only narrow exclusive competence of the EU legislature. This is quite the oppositefrom the scarce room the Court seems to allocate to domestic copyright laws.

IV. Painer: Reproduction of a photograph

50 As in *Infopaq* and Football Association Premier League, the referring court –Austrian this time– sought elucidation on the scope of the reproduction right of Article 2 Information Society Directive in relation to exempt uses under Article 5. This time the dispute was over the adaptation and use of portrait photos. In the case at hand, a freelance photographer from Austria had made a series of portrait photos of a six-year-old girl at a nursery school. The girl was later abducted. The Austrian authorities released some of the photos that the photographer had given to the parents and police. At some point the father commissioned a graphic designer to make a Photofit (a facial composite) of one of the portraits, showing what his daughter would look like now. After eight horrific years in captivity the girl managed to escape. It was a major news item across Europe. Lacking current photos, the defendant newspapers published the old ones. The photographer had neither been asked for permission nor credited.

51 The photographer brought various actions in Austrian courts against newspapers and the graphic designer. In these disputes it was hotly debated to what extent the photos were protected under German and Austrian copyright law. The proceedings that led to a preliminary reference were against five newspapers established in Austria and Germany.[31] The referring court did not ask about standards for subsistence of copyright. Rather, its principal copyright questions concerned the interpretation of the limitations for quotations and for use in the interest of public security (Art. 5(3)(d) and (e) Information Society Directive). It further asked if '...Article 1(1) of Directive 2001/29 in conjunction with Article 5(5) thereof and Article 12 of the Berne Convention, particularly [in the light of the fundamental right to respect for property] to be interpreted as meaning

that photographic works and/or photographs, particularly portrait photos, are afforded 'weaker' copyright protection or no copyright protection at all *against adaptations* [my italics] because, in view of their 'realistic image', the degree of formative freedom is too minor?

52 What is important to note is that with this last question, the Austrian court is second-guessing the Austrian Supreme Court's earlier findings about the Photofit, in a separate action for injunctive relief against the graphic designer. The Supreme Court held that the Photofit was not an adaptation of the source photo but a new, independent work ('*Freiebenützung*'). The end result was too far removed from the portrait photo. The source portrait does meet the modest originality criterion required for copyright protection under Austrian law. But considering the limited creative possibilities when making a portrait photo, the resulting protection is narrow: 'the stronger the individuality of the source work, the more removed must be the creation it inspired for it not to be regarded as an unauthorized adaptation, and vice versa' (case 4Ob170/07i).

53 For the sake of argument, let us assume that all adaptations are a species of reproduction and therefore come within the exclusive reproduction right of Article 2 Information Society Directive. What the Austrian Supreme Court says then seems to be consistent with the CJEU's reasoning in *Infopaq* on reproduction in part: only if the part reproduced expresses the author's own intellectual creation does the reproduction right come into play. Unauthorized copying is about copying what is original.

54 But in the proceedings on the merits, the parties disagreed fiercely on the OGH's reading, so much that the Landgericht Wien thought it wise to make the preliminary reference. Its question may not be the most aptly phrased. Arguably, the fact that the question is not phrased in terms of Article 2 signals that the court does not consider the right to authorize adaptations to be subsumed in the right to authorize reproduction. Why else would it have opted to ask only about Article 1 Information Society Directive and Article 12 Berne Convention? The latter provides for a right to authorize adaptions, albeit only for foreign authors and works from other Berne states. Article 1 Information Society Directive merely indicates the general scope of the directive and contains no substantive norms as such. Article 5(5) mirrors the three-step test for limitations laid down in Articles 9 Berne Convention, 10 WCT and 16 WPPT.

55 On any reading, and especially considering the preceding questions on the exemptions for quotations and public security uses, the Austrian court seems squarely focussed on the scope of protection. The Court of Justice, however, follows the Advocate General (who may have been taking his cue from the submissions made by the Commission and the Austrian government) and rephrases the question completely by turning to the Term Directive 93/98. As we have seen above, Article 6 of the latter harmonizes the standard for protection of photographs as copyright works. The CJEU posits that the Austrian court

> *must be understood as asking, in essence, whether Article 6 of Directive 93/98 must be interpreted as meaning that a portrait photograph can, under that provision, be protected by copyright and, if so, whether, because of the allegedly too minor degree of creative freedom such photographs can offer, that protection, particularly as regards the regime governing reproduction of works provided for in Article 2(a) of Directive 2001/29, is inferior to that enjoyed by other works, particularly photographic works.*

56 Not surprisingly, the CJEU concludes with reference to *Infopaq* and *Football Association* that in principle, portrait photographs can be copyrighted. The'author's own intellectual creation'of *Infopaq* is invoked alongside recital 17 of the Term Directive on Article 6; thus' an intellectual creation is an author's own if it reflects the author's personality'. That can be achieved if ' the author was able to express his creative abilities in the production of the work by making free and creative choices'. For example, these choices can relate to pose, framing, angle, lighting and atmosphere, but also the use of developing techniques and 'post production' (Photoshop). 'By making those various choices, the author of a portrait photograph can stamp the work created with his "personal touch"'. The Court concludes that 'consequently, as regards a portrait photograph, the freedom available to the author to exercise his creative abilities will not necessarily be minor or even non-existent.'

57 Is it significant that the Court refers to *Infopaq* and *Football Association* but not *BSA*? In other words, does *Painer* confirm the existence of a common originality standard for all types of works, or are software (and databases) still to be regarded separately? The latter does not seem likely, since as we have seen the *Infopaq* standard is borrowed from the Computer Programs Directive, Database Directive as well as from the Term Directive on photographs. In *Football Dataco* the Court keeps its analysis strictly to Article 3 Database Directive and not to other 'work' provisions, but it does refer to all the above judgments in elaborating the criterion of originality of the Database Directive. This again suggests a common standard. The more elaborate standard for all works would then be an intellectual creation of the author 'reflecting his personality and expressing his free and creative choices in its production'. Presumably, the shorthand for this is: 'personal touch stamp'.

58 On the scope of protection, the Court goes on to say that'nothing in Directive 2001/29 or in any other directive applicable in this field supports the view that the extent of such protection should depend on pos-

sible differences in the degree of creative freedom in the production of various categories of works'. Therefore, as regards a portrait photograph, the protection conferred by Article 2(a) of Directive 2001/29 cannot be inferior to that enjoyed by other works, including other photographic works.

59 Like the English court before it in *Football Association*, the referring Austrian court will probably not have much use for this answer in deciding whether the reproduction right was actually infringed. Analogous application of the *Infopaq* infringement standard for reproduction in part –only the taking of elements that contribute towards the original character of the copied work is relevant for a finding of reproduction- will get it further. And arguably, in the same place as its Supreme Court.

E. Readings

60 With the exception of the *BSA* case, in none of the preliminary references procedures treated here do the primary questions directly concern constitutive requirements of the copyright work. The Court's apparent construction of an EU-wide work standard is arguably the most controversial outcome of the cases, however. In this section, the focus is on how the 'work' judgments have been received in copyright doctrine in various jurisdictions. The predominant types of readings can be grouped in two broadcategories. The first are positivist-comparative: they attempt to establish and clarify what *is* now the positive European law, and to what extent particular domestic copyright laws comply with post-*Infopaq* standards. The second are methodological-critical: they zoom in on the methods the Court uses to forge European copyright law in relation to its role as the ultimate authority on the interpretation of EU law.

I. Positivist-comparative readings

61 The initial reactions to a court's judgment predictably ask two questions: Does the court say anything new? Do domestic courts need to revisit their normal approach? Especially *Infopaq* and *BSA* have elicited comments which in essence revolve around these two questions. Three readings stand out, treated here in ascending order of magnitude in terms of ramifications for domestic copyright laws. The first is that the Court of Justice recognizes that copyright may exist in very short works. The second is that the Court has interpreted EU law as containing an autonomous standard of originality for copyright works. The third is that the Court of Justice has not just set an originality standard, but has established that the subject matter of copyright is equally harmonized as a domain through 'intellectual creation' as an open-ended concept covering all conceivable types of authored matter.

1. Short works

62 In *Infopaq*, the Court holds (consideration 47) that 'the possibility may not be ruled out that certain isolated sentences, or even certain parts of sentences in the text in question, may be suitable for conveying to the reader the originality of a publication such as a newspaper article, by communicating to that reader an element which is, in itself, the expression of the intellectual creation of the author of that article....'According to a number of commentators, this consideration means that under EU law, very short works can attract copyright.[33]

63 An alternative – and I think a more convincing reading – is that the Court, engaged as it is in infringement analysis, merely expresses the generally accepted view that the taking of unprotected elements of a text does not count towards a finding of infringement of the reproduction right.[34] In other words,there is a threshold: no quantitative amount of copying constitutes a partial reproduction;what matters is the quality of what is copied. I would equally argue that the Court's careful phrasing 'that the possibility may not be ruled out' that reproduction of isolated sentences constitutes a reproduction in part (in a qualitative sense) indicated that this will not readily be the case, especially in informational texts as opposed to fiction.

64 That we should view the *Infopaq* considerations on parts of sentences reflecting originality – that is, counting as elements protected against reproduction – is also in keeping with the later *Football Association* judgment. This also is much focused on what the right infringement test is for Article 2 Information Society Directive, and not at all on the protectability of audio-visual and sound fragments as independent works, a key issue in the national proceedings.

65 Hobson observed that the wording used in *Infopaq*' does not permit the distinction between subsistence (and therefore qualification for protection) and infringement.'[35] But this is only true on the view that the Court equates a part of a text which is capable of conveying the original character of the text as a whole, as a part that for that reason constitutes an original intellectual creation – that is,a copyright work in its own right. To be sure, there is no point in having a right against 'partial'reproduction if the test is whether the something that is copied independently qualifies as a work of authorship.[36] After all, there would then be a full reproduction of the latter and not a partial one.

66 I am not convinced that the ECJ in *Infopaq* must be understood as saying that as a matter of EU law, co-

pyright exists in short texts if they are original. But even if it would say that, I agree with the commentators that nothing much would change at the domestic level. The possibility that a short text –especially a slogan or title – qualifies as a copyright work is generally not ruled out under domestic copyright laws, or even explicitly recognized in the Copyright Act (e.g. France). But the finding that a slogan, for example,is protected as a work of course involves originality closely linked as a constitutive requirement for copyright. On this matter, there seems to be widespread agreement that the Court has harmonized originality, although opinions are divided about what this standard is.

2. Type of harmonized originality standard

67 The literature on *Infopaq* and *BSA* queries what sort of harmonizing standard the Court has set: Is it a fully harmonized standard or rather a minimum one that leaves Member States room, notably to maintain stricter tests for some types of works? This issue is related to the question to which categories of works the originality test applies to begin with: only some, or across the board to all conceivable types of works, or to most but with some exceptions (like applied arts)? A number of commentators have also enquired into the nature of the standard as compared to those known in domestic copyright law, notably whether the 'author's own intellectual creation' is to be viewed as an 'objective' or 'subjective'test.

68 In German literature, it has been argued that *Infopaq*-sets only a minimum standard, the common lowest denominator, a threshold all works have to meet, but Member States can still apply higher standards for specific work categories.[37] While it is true that application of the standard is left to courts of Member States – i.e. they will have to determine whether the requisite level of creativity shows in the case at hand – this does not make it a *minimum* standard.[38] Of course, when applying the criterion, national courts will continue to consider that some information products are more determined by functional demands than others, and to the extent that functionality limits creative choices, it may be that certain types of work jump the hurdle less easily. The Court recognizes this in *Infopaq*, *BSA* and again in *Painer*, though in the latter case it also makes clear that no ex ante distinction must be made between genres as such (such as portrait photographs). In light especially of the *Painer* judgment, a reading of the originality test as a minimum norm no longer seems tenable.

69 The more common opinion indeed is that in *Infopaq* and *BSA* the Court has made the 'author's own intellectual creation' a uniform standard that displaces local deviating ones.[39] What is more, it also seems generally accepted –though grudgingly by many commentators – that the standard applies to all categories of works. The one possible exception could be for applied arts, since as was noted above the Design Directive and Design Regulation explicitly recognize that originality standards are a domestic affair. Article 9 of the Information Society Directive itself states it is without prejudice to provisions on design rights.

70 But here the Court's judgment in *Flos*[40] casts doubt on how much discretion actually remains for individual Member States to set the preconditions of copyright protection for design (usually categorized as applied arts). The question put before the Court concerned the interpretation of Article 17 Design Directive, on the accumulation of copyright protection and design protection for registered designs. The Court holds inter alia that accumulation is mandatory for registered designs, so a registered design must be copyright-protected if it meets the relevant local criteria. Although the Design Directive does not apply to unregistered designs, the Court says 'it is conceivable that copyright protection for works which may be unregistered designs could arise under other directives concerning copyright, in particular Directive 2001/29, if the conditions for that directive's application are met, a matter which falls to be determined by the national court.' This implies that the own intellectual creation standard articulated in *Infopaq* and *BSA* applies to national unregistered designs.

71 That in turn begs the question whether Member States could still maintain a higher local originality requirement for copyright in designs that are registered under domestic design law. After all, the Designs Directive expressly leaves the subsistence of copyright in design to Member States. If so, in theory that could lead to the existence of two different copyright standards for one and the same work of applied art. In practice the problem would be limited to the UK since–as far as I am aware– that is the only Member State with a national unregistered design right.[41]But with respect to the (un)registered Community Design, where cumulative protection under copyright is also mandatory, a similar problem looms.

72 On the reading that the *Infopaq*, *BSA*, *Football Association* and *Painer* all point towards one harmonized originality standard, what do commentators think the consequences for domestic law are? In France, Belgium and the Netherlands, the prevailing view seems to be that in practice not all that much will change.[42] In the UK, Austria[43] and Germany,[44] the application of the 'author's own intellectual creation' is more problematic, at least for some categories of works. Derclaye sees problems primarily for 'sub creative' literary works, the *Infopaq* standard being higher than what is normally required under UK law. For works of applied art ('works of artistic craftsmanship' under section 4(1) of the UK's Copyright, Designs and Patents Act 1988), it implies that the standard must be lowered. Some doubt is also

reported about whether the skill and labour standard as normally applied (for works other than databases and software) is lower than the 'intellectual creation' standard.[45] Whether in practice the protection it offers is less depends largely on the infringement test applied, which until *Infopaq* at least was that reproduction is only infringing if a substantial part was copied.

73 Benabou also sees a danger in the *Infopaq* standard, where the Court concludes that even if the parts (individual words) are unprotected, their selection, arrangement and combination can be. This exporting of the criterion of the Database Directive (and Art. 2(5) BC) to other genres could in her view signify an unwelcome 'reductionist' view of the work, which in turn leads to less protection against the copying of parts than is currently available under French law.[46]

74 In German doctrine, opinion remains divided on whether the 'own intellectual creation' standard of the Computer Programs Directive and Database Directive is the same as the personal creation standard of 2(2) German Copyright as applied to '*kleine Münze*'.[47] Also, various authors have drawn attention to the potential impact on the higher standards applied in Germany for functional texts, for example. All comments predate *Painer*, however, and it is conceivable that commentators would reach a different conclusion about the level of creativity required considering the Court's choice of words in *Painer* ('personal touch').

75 Some authors analyse the originality standard of *Infopaq* in terms of the objective or subjective nature of the test. The difference between an objective and subjective test of originality is essentially presented as the requirement that a work should originate from the author – i.e. not be copied – versus a requirement that the work shows the imprint or personal stamp of the maker. The Court's judgments are viewed through this lens by Belgian scholars, with mixed conclusions. Michaux argues that the *Infopaq* criterion of 'author's own intellectual creation' can be read as an objective criterion, especially in light of the legislative history of the Computer Programs Directive and the Database Directive, but also as a subjective one that maps better with the more common standard in Belgium.[48] Brison estimates that the Court seems to have abandoned an objective approach in favour of a subjective one by making the expression of creativity a central element.

76 The distinction seems inspired by a fairly schematic view of Anglo-Saxon versus continental European notions of originality. In the UK, of course, the relevant criterion is that not only must the work originate from the author (not be copied), it must also involve some labour, skill or independent judgment. In the Netherlands, the Supreme Court articulated a test that also contains 'objective' and 'subjective' elements: a work must originate from the author ('*eigen, oorspronkelijkwerk*') and bear the personal stamp of the author. The latter requirement is very modest and does not seem to differ much from similarly worded requirements in French and Belgian case law, and also appears to be close to the German *kleine Münze* notion that to be a personal intellectual creation, there must be a minimum degree of '*Gestaltungshöhe*'.

3. Generalized concept of work of authorship

77 Commentators are in broad agreement that the Court holds it a matter of European law that there is such a thing as a generalized work concept ('the author's own intellectual creation'). After *Infopaq*, the notion could still be entertained that at most the Court had set a standard for literary works. But when the Court held in *BSA* that a graphic user interface can be a work 'under the ordinary law of copyright' (as opposed to under the Computer Programs Directive), the conclusion seemed inescapable:no freedom remains for Member States to condition which subject matter warrants copyright protection. The *Football Association* judgment confirms this reading.

78 Three lines of criticism predominate. One is that the European legislature never intended to harmonize the work of authorship across the board. The Court should therefore have left it to Member States to determine the preconditions of copyright protection, in compliance with the relevant international and European norms. It was, in other words, not proper for the Court to generalize the standards set for software, databases and original photographs by giving the term 'works' of Articles 2 and 3 Information Society Directive an autonomous interpretation. More is said on this point below.

79 A second criticism is that the 'author's own intellectual creation' as used by the Court is not actually a complete work standard. The Court fails to distinguish between originality as a constitutive standard and other requirements.[49] At most, what the Court really does in *Infopaq* is elaborate that originality means a certain level of creativity is evident in the work. This does not tell us what – if any – other preconditions need to be met for subject matter to be copyrighted. In *BSA* and *Football Association*, the conflation of originality and work is even more apparent.

80 In *BSA* the Court ponders whether a graphic user interface is protected by 'ordinary' copyright. It makes a blanket reference to the criterion of *Infopaq* but sheds no light at all on where to draw the domain boundaries of these 'intellectual creations', artistic, literary, or otherwise. Worse still is the argument in *BSA*. There the Court basically reasons that a foot-

ball match is not a work because the rules of a football game leave no room for creative freedom. But even if that were so (a statement even those with no interest in football will probably disagree with), the constraining effect of rules is hardly the point here. The Court's reason seems analogous to the conclusion that a particular poem is not an original work because it has the formal properties of the Italian sonnet (for example) as a poetic genre. It is beyond dispute that a chosen form or an intended functionality of a text or design can limit creative freedom available to the author and impact how 'thick' the copyright in the object is.[50] In the *BSA* judgment, the Court says as much: expression that is dictated by technical function does not count towards finding originality.[51]

81 Originality understood as the result of creative activity is only one factor in the work equation. The creative form must bear on the right kind of production, a domain which in the Berne Convention is broadly described as 'every production in the literary, scientific and artistic domain'. In addition, we only call something a work if it is either expressed in a manner perceptible to the senses (continental copyright laws) or fixed in some form (Anglo-Saxon tradition). If the Court is on a road to a truly harmonized concept of a work of authorship, it will have to address these criteria as well. The differences among Member States with respect to the (often controversial) copyright status of food design, perfumes, conversations, fashion shows, and conceptual art suggest it will be difficult to construct a work notion on the basis of the existing directives. But the Court will also have to elaborate, for example, to what extent government information is copyrighted, or whether quasi-copyright such as the Dutch non-original writings protection (*geschriftenbescherming*) is consistent European copyright law. References to the Berne Convention, TRIPs, and WIPO Copyright Treaty cannot truly help settle such questions, a matter elaborated upon below.

82 A third criticism is that if the Court indeed means to say that as a matter of European law, there is such a thing as a generalized work concept, it causes an acute problem for those jurisdictions that have a closed list system. The Irish and British copyright clearly operate with a limited number of work categories,[52] and if a particular creation does not fit within the definition of any of them, there is no copyright in it. Not surprisingly, we find the fiercest criticism of *Infopaq* and *BSA* in the UK.[53] Either the existing work categories must be opened up to different types of creation, or the notion of a closed list must be abandoned altogether.

II. Methodological-critical readings

83 It is perhaps striking how much of the literature is highly critical of the Court's approach to harmonizing subjectmatter; then again, if the judgments were uncontroversial, few would be inclined to write about them. It is possible to map the types of arguments voiced to the role of the Court as the ultimate authority on European law and the function of the preliminary reference procedure as an instrument of interpretation. Three lines of critique stand out. Critics take issue with how the Court rephrases the questions referred to it in order to draw in matters on which the referring court sought no clarification. Another objection made is that the Court is too liberal in its use of the tool of autonomous interpretation. Yet another strand of criticism attacks the use and interpretation of international sources in the construction of European copyright law.

1. Rephrasing questions

84 The preliminary reference procedure of Article 267 TFEU is the primary mechanism through which uniform interpretation of EU copyright law is achieved. The initiative lies with the courts of Member States, for they decide to refer questions to the CJEU. Under Article 267 TFEU, an obligation exists for the domestic court of final resort (with an option for lower courts) to refer to the CJEU when a decision on a question of EU law is necessary to enable it to passjudgment in the case before it. Such an obligation does not exist when the question of EU law has already been answered by the Court of Justice, or is 'acteclair'. But the standard for acteclair is high: the domestic court must establish'that the correct application of Community law is so obvious as to leave no scope for any reasonable doubt'.[54]

85 The Court in principle has to answer to every request for a preliminary ruling, and will rarely find that a request is inadmissible.[55] In *Padawan/SGAE* it clarified that the alleged inapplicability of the Information Society Directive on the ground that it provides for only minimum harmonization is not a matter of admissibility but of substance. Where it concerns admissibility, 'there is a presumption of relevance in favour of questions on the interpretation of Community law referred by a national court, and it is a matter for the national court to define, and not for the Court to verify, in which factual and legislative context they operate'.[56] That is not to say that the Court will answer the questions as posed. As we have seen clearly in *Painer* and *BSA*, it is not uncommon for the Court to rephrase them.

86 In the context of the preliminary reference procedure, the court cannot itself apply Community law or judge a provision of national law by reference to

EU law. Its task is to 'provide the national court with an interpretation of Community law which may be useful to it in assessing the effects of that [national] provision'.[57] To be able to do that, it has the liberty to rephrase questions if they have been 'improperly' formulated, or to go beyond the scope of the powers conferred on the Court of Justice under its preliminary reference jurisdiction. In those cases, 'the Court is free to extract from all the factors provided by the national court and in particular from the statement of grounds contained in the reference, the elements of Community law requiring an interpretation ...having regard to the subject-matter of the dispute'.[58]

87 Were questions improperly formulated in the copyright cases discussed here? Vousden argues that in *BSA*, the Court preloaded the key question – 'Is a graphic user interface part of the expression of a computer program?'– (to which the answer might possibly have been yes), by turning it into 'Is a graphic user a form of expression of a computer program?' (to which the answer is more obviously no).[59] In the *Painer* case, the questions of the referring court were squarely on the scope of protection for photographs under the Information Society Directive in light of international copyright norms. The Court, however, rephrased them into a question on constitutive requirements: When is a photograph an original work under the Term Directive?

88 In neither case did the referring court obviously formulate its questions improperly, or ask the Court for the interpretation of international norms beyond its powers (more on these below). So from the perspective of the 'cooperation' mechanism between national courts and the EU court that Article 267 TFEU regulates, it is indeed hard to see why the Court did not stick with the original questions. From the outside looking into the Court's kitchen, it is difficult to ascertain why it rephrases questions that are not formulated properly enough to answer. One likely explanation is that it enables the Court to arrive at an interpretation of directives that creates a more 'coherent' system of European copyright law.

89 Here we enter the realm of methods used by the Court to construct Community law. It is far beyond the scope of this article to query all the various methods of interpretation (legal-historical, textual/grammatical, teleological/purpose-oriented, etc.) the Court applies or could apply in intellectual property cases. But the principle of autonomous interpretation deserves some scrutiny. Much of the criticism levelled against the Court concerns its expansionist attitude, which shows first and foremost in how it opts for autonomous interpretation of terms and concepts in the directives.

2. Autonomous interpretation

90 As was discussed above, a common reading and criticism of *Infopaq* and *BSA* is that in these cases the Court generalized a very specific standard of originality and made it a Community standard for all work categories, even going beyond that to also Europeanize the work of authorship. The Court did so by deciding that protected subject matter ('works') requires autonomous interpretation.

91 The principle of autonomous interpretation is an important tool for the Court to ensure uniform application of Community law. In its earlier case law, the ECJ seemed to accept more readily that instruments could contain both explicit and implicit references to domestic law,[60] but in subsequent cases, room for the latter diminished.[61] Today it appears that autonomous interpretation is the default, and that if the legislature means for a provision or term to refer back to national law, it must make this explicit. And indeed, in recent years the Court has reiterated this principle in *SENA*, *SGAE*[62] and *Infopaq*. In the latter case, the Court stressed that autonomous interpretation is 'of particular importance with respect to Directive 2001/29, in the light of the wording of recitals 6 [averting further fragmentation of national laws] and 21 [need for a broad definition of exclusive rights] in the preamble to that directive'. So far, of course, copyright directives seldom contain explicit references to national copyright law.[63]

92 Logically one would think that autonomous interpretation can only be used to give a Community-wide meaning to legal concepts that are within the scope of a directive. It is here that many commentators take issue with the Court.[64] Some argue that is was wrong to take the lower standard of Database and Computer Programs Directives as informing the 'work' in the Information Society Directive. Others point out that if the Court had left Member States more room to interpret the reproduction right, it would not have needed to interpret what the object of protection exactly is.[65] But most (also) argue, simply put, that the legislature did not intend to harmonize the work concept, so the Court has no business labelling it as a Community-wide notion. By seizing on the occurrence of the word 'works' in Article 2 Information Society Directive, mingling it with work definitions for specific categories in earlier directives and tying it up with notions of subject matter in the Berne Convention and other treaties, the Court has of course done just that.

93 This brings out the complex relationship between the level and kind of harmonization pursued at the legislative stages of each instrument on the one hand, and the methods used by the Court to attach a uniform meaning to legal concepts once instruments have become law. The Court's mantra is that 'in interpreting a provision of European Union law it

is necessary to consider not only its wording but also the context in which it occurs and the objectives pursued by the rules of which it is part.'[66] Here is surely a recognition of different interpretative methods: textual, purposive/teleological, and systematic.

94 But in reality, the Court seems to focus primarily on recitals to construct objectives and underlying principles, so it still engages in a textual interpretation more than anything else. It also does not consider the wider preparatory materials for purposive interpretation, nor is it prone to engage in legal-historical analysis.[67] Unilateral statements made by Member States in the Council, for example, cannot be used to interpret a directive.[68] Nor do Commission Green Papers or Staff Working Papers seem to matter.

95 On the other hand, to arrive at an interpretation the Court does look to other directives in the field. From a viewpoint of systematic interpretation and coherence of Community law, this is a necessary thing to do. But it can also suggest links where no relevant ones exist. For example, take the consideration in *Painer*, where the Court says that 'nothing in Directive 2001/29 or in any other directive applicable in this field supports the view that the extent of such protection [for photographs against reproduction] should depend on possible differences in the degree of creative freedom in the production of various categories of works.' What are the other applicable directives, one might ask? The term is about just that: duration. It is silent on the scope of exclusive rights and limitations. No general reproduction right existed for authors before the Information Society Directive. The scope of rights in the Computer Programs Directive and the Database Directive necessarily concerns only those categories of works. So why consider all these earlier directives?

96 It is fair to say that the Court has a very strong focus on textual interpretation of the acts themselves. As a result, a key feature of the harmonization process may get lost in translation: the piecemeal approximation of laws as a direct consequence of the principles of subsidiarity and proportionality, which necessarily results in a mix and match of varying harmonization standards. Harmonization measures can be full or partial (excluding certain issues), lay down minimum or maximum norms (level of protection), and concern mandatory or optional rules (e.g. with respect to limitations). If autonomous interpretation is the norm, and the sacrosanct high level of protection (recital 9 Information Society Directive) becomes a regular fixture in the Court's assessment, it should come as no surprise if full, minimum and mandatory readings win out.

97 There is also the danger that what a majority of Member States held to be self-evident (e.g. that the Computer Programs Directive contains no uniform criteria for establishing when a production other than software is a copyright work) does not show in the instrument and therefore has no bearing on the interpretation of the Court. If the Court would answer the call for more consideration of the historical background of provisions of Community law, it might conclude with respect to the work of authorship that it is a matter for Member States to specify preconditions for protection on the basis of the following narrative:

98 The obvious explanation for why the directives – with the exception, of course, of the Computer Programs and Database Directives and the Term Directive on photographs– do not concern themselves with specifying what copyright-protected subject matter is, is that this was not an area where differences among Member States were considered pressing problems from an internal market perspective. Hard cases were not something the EC needed to deal with unless they involved significant industries. The computer industry and the budding database industries of the 1980s were a case in point.

99 Equally important, the introduction and approximation of economic rights in the other directives (rental right, lending right, right of communication to the public via cable or satellite broadcasting) took place in the context of protecting classic mainstream media against new forms of exploitation. In other words, there was no reason to debate differences in criteria for the existence of copyright, because the focus was on firmly established work categories such as books, journals, musical compositions, photography and film. A similar argument can be made with respect to the Resale Right Directive, which applies to visual art works existing as a single artefact or made in a limited edition.

100 Another clue that harmonization of subject matter was generally not on the agenda can be found in the Green Paper of 1995.[69] It led directly to the Information Society Directive but does not identify a problem with diverging standards in work. It unequivocally states that originality is not and need not be a harmonized standard. It does discuss multimedia works as new genre, but it does not expect it will be a problem to protect them under existing laws as they are essentially a mixture of old recognized protected genres.

101 With respect to the issue of fixation, it is also fair to assume that this was just not an issue. Software, databases or photographs are 'genres' of works that are hard to imagine as not fixed in some material form (as opposed to music, poetry, choreography, or lectures, for example, which can be created 'live'). So the European Commission, as the initiator of legislative proposals, may simply not have flagged it as relevant.

102 Granted, where the (wider) preparatory materials are silent or unclear, it makes sense for the Court to limit itself to a textual analysis of a directive's provisions. And indeed, the Court has in the past said that 'in the absence of preparatory materials that clearly express the purpose of a provision, the Court can only base its interpretation on the purpose of the text as it has been is established and give it the meaning which flows from a literal and logical interpretation'.[70]

103 It should be noted that although many commentators–including me–think that the Court should not have turned the work into a (incomplete) Community-wide notion, some are more sympathetic.[71] It is undoubtedly true that now that so many aspects of copyright are explicitly harmonized, it makes no apparent sense to leave pivotal questions on subsistence and initial ownership largely a matter of Member States. From that perspective, the Court's activist attitude is understandable. It also creates its own uncertainties, however, dependent as the process is on the limits of the preliminary reference procedure. It also has the potential to change the dynamics of legislative action. Increasingly, whatever freedom Member States want to maintain to tailor their domestic copyright will have to be made very explicit in further acts, which can greatly complicate negotiations in what already is a volatile policy area.

3. Interpretation of international sources

104 The final strand of criticism I would like to discuss concerns how the Court deals with international law in its construction of harmonized criteria for the protection of copyright works. To put this in perspective, it may be useful to give a short reminder of the competence of the Court to interpret international norms in the context of a preliminary reference procedure.

105 International agreements concluded by the European Union form an integral part of the EU legal order, and can therefore be the subject of a request for a preliminary ruling. TRIPs, WCT and WPPT are directly binding on the EU, so the Court can give interpretations that bind the Member States (though not the other parties to these treaties, of course). It determines the boundaries between obligations that remain the sole responsibility of Member States and those of the EU.[72] The Court can also interpret the norms of the Berne Convention, at least those laid down in Articles 2-21 BC and appendices, because of the EU's obligation to comply with them under Article 9 TRIPs and Article 1(4) WCT. Even if an international convention is not binding on the EU (e.g. the Rome Convention of 1961 on related rights), the Court's role under Article 267 TFEU means it is competent to interpret a convention's provisions insofar as the European Union has assumed the powers previously exercised by the Member States in the field to which the convention applies.

106 It is also settled case law that in relations between EU Member States, conventions concluded by Member States with non-member countries cannot be applied to the detriment of the objectives of European Union law.[73] On the other hand, considering the primacy of international instruments to which the EU is a party, EU law must be interpreted in accordance with such international norms whenever possible.[74] If it is evident from the objectives of a directive that compliance with an international treaty was a concern, the Court can bring in the relevant norms to arrive at a purposive reading.[75]

107 In sum, the Court has several avenues through which it can take copyright treaties into account, and its interpretation of them is binding upon Member States. So what are the objections against the approach it takes in its copyright judgments? Not surprisingly, the issue critics take with the Court is not so much that it interprets provisions of the international conventions, but the way it does it and the results it arrives at.

108 *Infopaq* draws the most criticism, which can be explained by the fact that although in the other three judgments the Court makes some references to international treaties with respect to protected subject matter, it attaches no independent meaning to them. *BSA* contains no more than a token reference to Article 10(1) TRIPs Agreement. It obliges the EU and its Member States to protect software whether expressed in source code or in object code as a literary work within the meaning of the BC. The TRIPs Article mirrors the obligation that the EU imposes on its Member States to protect software as literary works (Art. 1(1) Computer Programs Directive). In *Football Association*, the relevant references to international law are to Article 9(1) TRIPs (obligation to respect Art. 1-21 Berne Convention except for moral rights), and the similar obligation of Article 1(4) WCT. It is only with respect to the scope of the communication to the public right (Art. 3 Information Society Directive) that the Court considers the treaties more closely. Otherwise, the references are to *Infopaq*. In *Painer* the Court refers to TRIPs and Article 1(4) of the WIPO Copyright Treaty as a way into the articles of the Berne Convention it deems relevant: the inclusion of photographs in the work list of Article 1, the adaptation right of Article 12, and the right to quote of Article 10(1). With respect to the requirements for protection, it refers to its judgments in *Infopaq* and *Football Association*, and it does not elaborate on the Berne Convention's significance.

109 *Infopaq* then is the cornerstone judgment. In it, the Court focuses on Article 2 Berne Convention. It cites the exclusive reproduction right of Article 9 and parts of Article 2, which defines the scope of protec-

ted subject matter covered by the BC: the examples list of Article2(1); the provision that extends the scope to include collections of literary or artistic works which, by reason of the selection and arrangement of their contents, constitute intellectual creations (Art. 2(5)); and the exclusion of news of the day or miscellaneous facts having the character of mere items of press information (Art. 2(8) BC).

110 On the basis of these provisions, the Court concludes 'that the protection of certain subject-matters as artistic or literary works presupposes that they are intellectual creations.' Since the Computer Programs Directive, Database Directive and Article 6 Term Directive uses similar terminology ('original in the sense that they are their author's own intellectual creation'), and the Information Society Directive builds upon previous directives, the works referred to in its Article 2(a) can only be' subject-matter which is original in the sense that it is its author's own intellectual creation'.

111 A first observation is that though the EU is obliged to comply with the Berne Convention, this does not mean its concept of protected works must be integrated one on one in internal Community copyright law. After all, the Berne Convention concerns itself only with the protection of foreign authors and works (on the basis of national treatment), but the minimum substantive norms on protection do not apply in internal situations. In practice, of course, these norms have a certain unifying effect on domestic copyright laws because contracting states generally will not put foreign authors in a better position than their own citizens. That may be so, but it is not clear to me how that would create a direct *obligation* for the EU to adopt the Berne Convention's concept of protected works in Community law.[76]

112 The Court can (and does) take into account the stated intention of the Community legislator to integrate specific international norms in directives. But of course, not every reference to the Berne Convention, TRIPs, WCT or WPPT in the directives necessarily reflects such an intention. For example, the legislative history of the harmonization of the term of protection for photographs suggests that the reference in Article 6 Term Directive to a photograph as a work within the meaning of the Berne Convention merely helps distinguish photographic works protected under normal copyright (of the kind central to the Berne Convention) from photographs protected by related rights.

113 In *Infopaq*, the Court suggests that the Berne Convention actually provides a uniform work concept. But the BC's elaboration of protected literary and artistic works ('every production in the literary, scientific and artistic domain') is commonly understood as not establishing a particular originality criterion. Also, because the convention elaborates minimum standards, the EU and its Member States are free to extend copyright protection to types of works not within the scope of international conventions.[77]

114 The Court is also criticized for lifting out the 'original intellectual creation' criterion of Article 2(5) BC and treating it as the leading concept. Article 2(5) only deals with collections of works (such as anthologies) and not with all databases.[78] The Court makes no reference in *Infopaq* to Article 10(2) TRIPs, which, unlike Article 2(5) BC, is not limited to collections of works.[79] In the recent *Football Dataco* judgment, which is all about protection of football fixtures lists as databases by copyright,[80] the Court on the other hand refers to Article 10 TRIPs and Article 5 WCT, but not at all to the Berne Convention. Whatever the explicit international sources the Court uses, it is not clear to me why the standards for databases as agreed in TRIPs and the WCT should be generalized to all types of works. It is also noted that although the exclusion of news of the day is listed among the relevant provisions of international law, the Court actually pays no further attention to it when it elaborates the standard for protection.[81]

115 Finally, Vousden is of the opinion that on closer inspection the Court does not actually apply provisions from the international treaties, even though that is what it says it does, but rather takes its inspiration from French and German copyright doctrine.[82] Heinze, on the other hand, wonders whether *BSA* shows signs of incorporating the merger doctrine known from US law.[83] All in all then, commentators are not particularly impressed with the way the Court looks to international norms to construct a Europeanized notion of the copyright work. But perhaps the Court will be asked to revisit the line of reasoning it took in *Infopaq* in one of the undoubtedly many more requests for preliminary references to come.

F. Further down the road

116 Little has been written about the characteristics and role of the preliminary reference procedure in shaping European copyright law. After twenty years of harmonization, it seems odd to say that the interpretation of the copyright directives through preliminary references is only now coming up to steam. Yet this is what a short survey on the growth of preliminary reference procedures shows.

I. Growing numbers of preliminary references

117 If we take a closer look at the number of preliminary references brought before the Court, we can distinguish two periods: the decade from the implemen-

tation date of the first directive, the Computer Programs Directive (1993-2002), and the near decade since the implementation date of the Information Society Directive (2003-2011).

118 A quick and dirty check of the number of copyright cases[84] before the Court of Justice indicates that prior to 2003 roughly twenty cases had been lodged and resulted in judgments. Of these, about half were not concerned with the interpretation of provisions in directives but were about copyright in relation to the free flow of goods and services or abuse of a dominant position in the internal market (EC Treaty, then Arts. 30, 36, 85, 86). In the other half, cases about rental and lending were overrepresented, while none of the preliminary references concerned the Computer Programs Directive.

119 It was not until late 2009 that the first software case was lodged that made it to judgment (*BSA)*. In the second 'post-*Infosoc*' period of 2003-2011, twice as many cases were lodged as in the first period. In half of these, national courts asked questions about the Information Society Directive. A quarter of these cases were about the Rental and Lending Directive, including a handful of proceedings brought by the Commission against Member States for failures to properly implement the public lending right provisions.[85] Still, the Rental and Lending Right Directive comes in a comfortable second place in the ranking of most preliminary reference-prone copyright directives, trailing the Information Society Directive but leading before the Satellite and Cable Directive.

120 The Information Society Directive is so broad in terms of rights and limitations covered that it is predictable that it generates the most preliminary references, and one would also expect that the Information Society Directive would be drawn into cases where the primary questions asked are about earlier directives. And indeed, where before cases lodged typically concerned the interpretation of only one directive, there now is a trend toward cases where preliminary questions are asked about various directives. The Court of Justice's practice to draw in various copyright directives in its discussion of questions asked about a single one may well further stimulate national courts to do the same in their references.

II. A new stage in copyright harmonization?

121 One could say that the Council and Parliament's failure to engage with the question 'what is a work' beyond the specific genres of software, databases and photographs has forced the Court to start answering it. Many questions still go unanswered about the boundaries of the domain of copyright, exclusions of protection (for news of the day, official texts), requirements of fixation, the possibility to maintain national systems with closed lists of work categories, and on and on. Inevitably, I would think, once national courts are taken further down the road to an all-inclusive Community-wide notion of what constitutes a work, there will be no escape from a Community-wide notion of authorship (and initial ownership). And eventually also of moral rights, which has been kept out of the discussion in EU institutions so far with the convenient 'excuse' that it has no particular internal market relevance. As Benabou observed, the Information Society Directive has opened a Pandora's box, enabling the Court of Justice to interpret key concepts of copyright.86

122 Unless, of course, the legislator were to step in. Copyright law becomes more and more politicized, however, to the point where one-issue parties with an anti-copyright agenda are now represented in several national parliaments and the EP. And with nearly double the number of Member States that were involved in drafting previous instruments, one can expect that decision making in the Council and Parliament will not speed up. What is more, much energy these days goes into the enforcement of IP; the much-maligned Anti-Counterfeiting Trade Agreement (ACTA) is a case in point. So perhaps on issues of work, authorship, ownership and the like, the legislator will not do anything for years to come. At most, a few years down the line and many judgments further, it might initiate a 'recast' round of existing directives, in which the judgments of the courts are codified.

123 The preliminary reference tool takes on a new meaning. The numbers of copyright cases brought before the Court of Justice are rising, and the Court shows itself rather activist and willing to construct pan-European notions of copyright that are not clearly in (or even squarely out of) the directives. It is therefore high time for scholars to start studying more profoundly the intricacies and dynamics of the preliminary reference procedure as a mechanism for the unification of European copyright law. It will drive changes in domestic laws for years to come, and I think understanding how national courts and the ECJ through the preliminary reference procedure shape the development of copyright norms is crucial for ensuring the quality of any instruments of intellectual property law to come.There are many questions. Some that come to mind concern the fact that the process is of necessity locally driven. The initiative is with national courts, for in the end they decide to take a matter to Luxembourg. Do some Member States drive the process more than others? How come? Does this push the law in a certain direction? Then there are questions that have to do with the type of disputes that are litigated in copyright. Are some types of disputes more likely to result in preliminary references– e.g. involving certain industriesor focussed on the scope of exclusive rights –

rather than disputes over ownership, for example? If so, does this set the Court on a certain path, which in turn may invite more preliminary references? If there is such a circular effect, is there a danger that it promotes lopsided development of the law, especially considering the enormously broad and diverse areas of cultural production that copyright law impacts? Are national courts the drivers in name, but is the Court of Justice in the seat? Surely such questions deserve greater scrutiny from intellectual property scholars.

124 With some judgments fresh off the press and major ones in the pipeline, there will also be plenty of positivist-comparative work to do. To end with Posner: 'The messy work product of the judges and legislators requires a good deal of tidying up, of synthesis, analysis, restatement, and critique.'[87]And indeed, the tidying up that the Court of Justice itself engages in while attempting to forge common copyright and related rights concepts 'given the requirements of unity of the European Union legal order and its coherence ...'is blowing up plenty of dust for now.

■

1 Mireille van Eechoud, Bernt Hugenholtz et al., *Harmonizing European Copyright Law: The Challenges of Better Lawmaking*, Information Law Series 19, Alphen aan den Rijn: Kluwer Law International 2009.

2 In the Football Dataco judgment of March 1, 2012 (Case C-604/10), the ECJ interprets Art. 3 Database Directive (requirements for copyright protection). This case is not discussed in as much detail as the 2009-2011 cases here, as it was handed down after the manuscript for this article was submitted, and has not yet generated in-depth commentary.

3 Cases on the limitations to the free movement of goods allowed in the interest of copyright and related rights (Art.28/30 TEC, now: 34/36 and TFEU) started with *Deutsche Grammophon v Metro* SB, ECJ 8 June 1971, Case 78/70, ECR [1971] 487. On the principle of non-discrimination, the first copyright case was *Phil Collins v Imtrat*, ECJ 20 October 1993, joined cases C-92/92 and C-326/92, ECR [1993] I-5145. The application of EU competition law was at the heart of *Magill* (*Radio TelefisEireann (RTE) and Independent Television Publications Ltd (ITP) v Commission*, ECJ 6 April 1995, joined cases C-241/91 and C-242/91, ECR [1995] I-743) and *IMS Health* (*NDC Health Corporation and NDC Health v IMS Health Inc. and Commission*, ECJ 29 April 2004, Case C-418/01, ECR [2004] 5039).

4 European Commission, COM (88) 172 final, Brussels, 07.06.1988.

5 European Commission, COM (95) 382 final, Brussels, 19.07.1995.

6 See i.a. recital 16 Database Directive: 'Whereas no criterion other than originality in the sense of the author's intellectual creation should be applied to determine the eligibility of the database for copyright protection, *and in particular no aesthetic or qualitative criteria should be applied'*[italics added].

7 Green Paper on Copyright and the Challenge of Technology 1988, p. 197.

8 The definition of the Database Directive (and Art. 5 WCT) differ from Art. 2(5) BC because the wording of the latter implies that only collections of literary or artistic *works* (as opposed to other materials) come within its scope, and that originality must show in both selection *and* arrangement (as opposed to selection or arrangement, i.e. alternative rather than cumulative elements of the test).

9 For an analysis of the current situation in Germany, see T. Büchner, Schutz von Computerbildern als Lichtbild(werk) ZUM 2011, 549.

10 Initially for 25 years, but subsequent changes have led to a term of life plus 50 years. The term of protection for photographic works is life plus 70 years.

11 Proposal for a Council Directive harmonizing the term of protection for copyright and related rights. COM (92) 33 final, March 1992, p. 36.

12 At the time the European Parliament only had advisory powers. The Maastricht Treaty, which introduced the co-decision procedure between Parliament and Council as the default procedure for legislative instruments, only entered into force in November 1993.

13 Proposal for a Council Directive harmonizing the term of protection for copyright and related rights, COM(92) 602 final - SYN 395.

14 M. Walter, *EuropäischesUrheberrecht*, Michel M. Walter, Silke von Lewinski et al., p. 597; A. Nordemann& L. Mielke, *Zum-Schutz von Fotografiennach der Reform durch das dritteUrheberrechts-Anderungsgesetz*, ZUM 1996, 214-218 at 216.

15 Art. 1, recitals 18-19 Directive 2011/77/EU of 11.09.2011.

16 Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, recital 32 'leaving Member States free to establish the extent of copyright protection and the conditions under which such protection is conferred'; Art. 96(2): 'A design protected by a Community design shall also be eligible for protection under the law of copyright of Member States as from the date on which the design was created or fixed in any form. The extent to which, and the conditions under which, such a protection is conferred, including the level of originality required, shall be determined by each Member State'; see also Directive 98/71/EC of the European Parliament and of the Council 13 October 1998.

17 ECJ 21 January 2011, Case C168/09, *Flos*.

18 Joined Cases C-403/08 and C-429/08 Football Association Premier League and Others.

19 ECJ 1 March 2012, Case C-604/10, on whether English and Scottish football league fixture lists are copyright protected works (collections) under Art. 3 Database Directive. The Court ruled inter alia that copyright in a collection of data exists 'provided that the selection or arrangement of the data which it contains amounts to an original expression of the creative freedom of its author, which is a matter for the national court to determine'. The author must express 'his creative ability in an original manner by making free and creative choices' where the selection and arrangement is concerned. That criterion is not satisfied when the setting up of the database is dictated by technical considerations, rules or constraints which leave no room for creative freedom. Significant skill or labour do not justify copyright under the Database Directive unless they express originality (cons. 38-46).

20 ECJ 16 July 2009, Case C-5/08, *Infopaq*, [2009] ECR I-06569.

21 Thomas Büchner, *Schutz von ComputerbildernalsLichtbild(werk)*, ZUM 2011, 549; S. Dürager, *Die Schutzfähigkeit der Benutzeroberflächeimmaterialgüterrecht*, ÖsterreichischeBlätterfürg ewerblichenRechtsschutz und Urheberrecht 2011, 100-106; C. Heinze,*Software alsSchutzgegenstand des EuropäischenUrheberrechts*, JIPITEC 2011, Vol. 2.; P. B. Hugenholtz, comment on Hof van Justitie EU 16 juli 2009 (*Infopaq*) and 22 december 2010 (*BSA*), NJ 2011, 288 and 289; JochenMarly, *Der Urheberrechtsschutzgrafischer Benutzeroberflächen von Computerprogrammen. ZugleichBesprechung der EuGH-Entscheidung'BSA/Kulturministerium'*, GRUR 2011, 204; Hermann Lindhorst, *AnmerkungbeiEuGH: GrafischeBenutzeroberflächegenießtkeinenUrheberrechtsschutzals-Computerprogramm*, GRUR-Prax 2011, 61; A. van Rooijen, Case comment in AMI 2011, 99-101; Leigh J. Smith, *Whether copyright protects the graphic user interface of a computer programme*,

C.T.L.R. 2011, 17(3), 70-72; Stephen Vousden, *Protecting GUIs in EU law: Bezpec˘nostnı´ Softwarova´ Asociace'*, Journal of Intellectual Property Law & Practice, 2011.

22 The original Council Directive 89/552/EEC 'on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities' (known as 'Television without Frontiers' or 'TWF' Directive), was amended by Directive 97/36/EC, and again amended and renamed by the Audiovisual Media Services Directive of 2007 (since consolidated in Directive 2010/13/EU).

23 Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access.

24 Peculiarly, the Court refers to the directives as the 'Copyright Directive' rather than the Information Society Directive, to the 'Related Rights Directive' rather than the more usual Rental and Lending Right Directive, and to the Satellite and Cable Directive as the 'Satellite Broadcasting Directive'. I stick to the more commonly used terminology here.

25 25 [2008] EWHC 1411 (Ch).

26 Subjectmatter that in other jurisdictions (and various directives) is known as the object of related or neighbouring rights (performance, sound recording/phonogram, first fixation of film) is not so named in the UK's Copyright Designs and Patents Act 1988, but is generally also called 'copyright'.

27 Initially the related rights for audio-visual recordings were harmonized in the Rental and Lending Right Directive (Art. 2 Rental and Lending Right, Distribution Right Art. 9, Art. 7 Reproduction Right - repealed, now Art. 2 Information Society Directive), now also through the Information Society Directive.

28 See P. Kamina for an in-depth analysis of differences in the law of Member States, esp. as viewed from a UK and French perspective, *Film Copyright in the European Union*, Cambridge University Press 2002.

29 *Norowzian v Arks Ltd &Anor* (No. 2), [1999] EWCA Civ 3014.

30 J. Kitchin summarized the issue thus in para. 222 [2008] EWHC 1411 (Ch): 'It is clear that fragments of the various film works, the musical work and the sound recording are stored sequentially in the decoder. The question is whether such fragments individually amount to a substantial part of the copyright work and, if not, whether they should be considered collectively.'

31 For a discussion of another important aspect of this case– namely, do the Austrian courts have jurisdiction to hear a joint claim against the Austrian newspapers and German newspaper under the Brussels I regulation – see my case comment Multiple defendants and territorial intellectual property rights:*Painer* revisits Roche through Freeport on the Conflict of Laws net blog.

32 Whether the reproduction right includes the right to authorize adaptations is a contentious issue; see Mireille van Eechoud et al., *Harmonizing European Copyright Law*, Kluwer 2009, p., 73-76, 83-84 (arguing there is no harmonized adaptation right).

33 Inter alia: FabienneBrison, *'Originality' in Copyright: A Community-wide Notion*, Winter 2010 <http://ipintelligence.howrey.com/originality-in-copyright-a-community-wide-notion/>; LexBruinhof, *Elf woordenkunnengenoegzijnvooreenverveelvoudiging. KortcommentaarbijHvJ EG, 16 juli 2009, zaak C-5/08, B9 8070, Infopaq /DanskeDagbladesForening*, at Wieringa Advocaten; Frey,*LeistungsschutzrechtfürPresseverleger* - ÜberlegungenzurStruktur *und zu den Auswirkungen auf die Kommunikationim Internet*, MMR 2010, 291; B. Michaux, *L'originalitéen droitd'auteur, une notion davantagecommuna utaireaprésl'arrêtInfopaq*, Auteurs & Media 2009 (5), 473-488; Artur-Axel Wandtke, NJW 2010, 3144 (book review).

34 Cf. also focussing on reproduction, P. Petersen, *Reproduction of 11 word snippets of copyright work, case comment on Infopaq*, Cri 5/2009, 146-147; Andrew Hobson, *Newspaper Licensing Agency Ltd v Meltwater Holdings BV*, Entertainment Law Review 2011, 22(3), 101-104.

35 Andrew Hobson, *Newspaper Licensing Agency Ltd v Meltwater Holdings BV*, Entertainment Law Review 2011, 22(3), 101-104.

36 Under UK law, the relevant test (prior to *Infopaq*) was whether a 'substantial part' was copied. On that test, Lord Hoffman opined in Designers Guild ([2000] 1 WLR 2416):'So it may sometimes be a convenient short cut to ask whether the part taken could by itself be the subject of copyright. But, in my view, that is only a short cut, and the more correct approach is first to determine whether the plaintiffs' work as a whole is "original" and protected by copyright, and then to inquire whether the part taken by the defendant is substantial.'

37 In this vein: M. Leistner et al.,*ALAI report Germany*<http://www.alaidublin2011.org/wp-content/uploads/2011/04/Germany.pdf>; v. Ungern-Sternberg, *Die Rechtsprechung des BundesgerichtshofszumUrheberrecht und zu den verwandten-Schutzrechten in den Jahren 2008 und 2009 (Teil I)*, GRUR 2010, 273; W. Erdmann, *Die Relativität des Werkbegriffs*, in: Festschrift für Michael Loschelderzum 65. Geburtstag, Köln: Schmidt 2010, 61-73; S. Von Lewinski, *Recent Developments of German Authors' Rights Law*, Auteurs & Media, 2011, 162;JochenMarly, *Der UrheberrechtsschutzgrafischerBenutzeroberflächen von Computerprogrammen. ZugleichBesprechung der EuGH-Entscheidung'BSA/Kulturministerium'*, GRUR 2011, 204 (different criteria for software as work and graphic user interface as work).

38 If I understand correctly, this is what some writers referred to in M. Leistner et al. 2011 ALAI report Germany.

39 Among others: P. Sirinelli, RIDA;D.J.G. Visser, 'Endstraingehaald door *Infopaq*', B9 8122; V. Benabou, Note d'observations, C.J.C.E. (4e ch.), 16 juillet 2009, RDTI 2009, no. 39, 61 ff.; Jonathan Griffiths, ECJ decision in Czech GUI case could pose questions for UK copyright law, <http://ipandit.practicallaw.com/6-504-8145>; C. Handig, *The copyright term 'work' - European harmonisation at an unknown level*, 40 IIC 665-685 (2009).

40 CJEU 27 January 2011, Case C-168/09, *Flos*.

41 For an in-depth comparative analysis of design protection in the UK, France and Italy, see E. Derclaye, *Are Fashion Designers Better Protected in Continental Europe than in the United Kingdom?*, The Journal of World Intellectual Property Vol. 13, no. 3, 315-365 (2010).

42 P.B. Hugenholtz, NJ 2011, 288, 289; D.J.G. Visser, *KroniekIntellectueleEigendom*, NJB 2010, 779; K. Koelman, *NootbijHvJEG 16 juli 2009, zaak C-5/08 (Infopaq)*, AMI 2009, p. 198-205; B. Michaux, *L'originalitéen droitd'auteur, une notion davantagec ommunautaireaprésl'arrêtInfopaq*, Auteurs & Media 2009 (5), 473-488; V. Benabou, states that the 'intellectual creation' will eclipse the 'empreintepersonel' standard of French law, but it is unclear whether she sees this as a substantive change; see V. Benabou, *Note d'observations, C.J.C.E. (4e ch.), 16 juillet 2009*, RDTI 2009, no. 39, 61 ff. At any rate, in *Painer* the CJ uses the 'personal stamp' criterion.

43 See C. Handig, *WievielOriginalitätbrauchteinurheberrechtliches-Werk?*, RdW 1/2010, Artikel-Nr. 16.

44 P. Petersen, *Reproduction of 11 word snippets of copyright work, case comment on Infopaq*, Cri 5/2009, 146-147; C. Heinze, S*oftware alsSchutzgegenstand des EuropäischenUrheberrechts*. JIPITEC (2011)Vol. 2; Christian Handig, *The Copyright Term 'Work' – European Harmonisation at an Unknown Level*, 40 IIC 665 (2009).

45 Isabella Alexander, *The concept of reproduction and the 'temporary and transient' exception*,C.L.J. 2009, 68(3), 520-523; E. Derclaye, *Infopaq International A/S v DanskeDagbladesForening (C-5/08): Wonderful or worrisome? The impact of*

the ECJ ruling in Infopaq on UK copyright law', 32(5) EIPR 247-251(2010), arguing that the skill and labour is a lower standard than originality under *Infopaq*.

46 V. Benabou, *Note d'observations, C.J.C.E. (4e ch.), 16 juillet 2009*, RDTI 2009, no. 39, 61 ff.

47 C. Heinze, *Software alsSchutzgegenstand des EuropäischenUrheberrechts*. JIPITEC (2011)Vol. 2.

48 B. Michaux, *L'originalitéen droitd'auteur, une notion davantage communautaireaprésl'arrêtInfopaq*, Auteurs & Media 2009 (5), 473-488.

49 V. Benabou, *Note d'observations, C.J.C.E. (4e ch.), 16 juillet 2009*, RDTI 2009, no. 39, 61 ff; E. Declayre, *Wonderful or worrisome? The impact of the ECJ ruling in the Infopaq on UK copyright law,* 32(5) EIPR 247 (2010); Jonathan Griffiths, *ECJ decision in Czech GUI case could pose questions for UK copyright law*, <http://ipandit.practicallaw.com/6-504-8145>.

50 See, however, Jonathan Griffiths, *ECJ decision in Czech GUI case could pose questions for UK copyright law*, <http://ipandit.practicallaw.com/6-504-8145> on the protection by copyright in musical scores of baroque music.

51 Cons. 48: 'When making that assessment, the national court must take account, inter alia, of the specific arrangement or configuration of all the components which form part of the graphic user interface in order to determine which meet the criterion of originality. In that regard, that criterion cannot be met by components of the graphic user interface which are differentiated only by their technical function.'

52 Handig notes that in Austria it is disputed whether a work must fit one of the categories of the Copyright Act: C. Handig, *The copyright term 'work'- European harmonisation at an unknown level*, 40 IIC 665-685 (2009).

53 Jonathan Griffiths, ECJ decision in Czech GUI case could pose questions for UK copyright law, <http://ipandit.practicallaw.com/6-504-8145>; E. Derclaye, 'Wonderful or worrisome? The impact of the ECJ ruling in the *Infopaq* on UK copyright law', 32(5) EIPR 247-251 (2010); 'The Lionel, the Bezpečnostnísoftwarováasociace and the Wandering Court of Justice', Tuesday, 11 January 2011, posted at<http://ipkitten.blogspot.com/2011/01/lionel-bezpecnostni-softwarova-asociace.html>; Leigh Smith, Whether copyright protects the graphic user interface of a computer programme, C.T.L.R. 2011, 17(3), 70-72.

54 ECJ 6 October 1982, Case 283/81 (CILFIT), ECR 1982, 3415.

55 If it is manifest that the 'interpretation of Community law that is sought bears no relation to the actual facts of the main action or to its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it'. See ECJ 20 May 2010, Case C-138/09 (Todaro-Nunziatina), ECR 2010, I-4561 and cases cited there.

56 ECJ 21 October 2010, Case C-467/08 (Padawan).

57 Case 20/87 *Gauchard* [1987] ECR 4879, and later cases

58 See inter alia ECJ 29 November 1978, Case 83/78 *Pigs Marketing Board v Redmond* [1978] ECR 2347.

59 Stephen Vousden, 'Protecting GUIs in EU law: Bezpecˇnostnı´ Softwarova´ Asociace', Journal of Intellectual Property Law & Practice, 2011.

60 Hagen OHG, ECJ 1 February 1972, Case 49-71, [1971] ECR 23.

61 See e.g. ECJ in *Ekro* (18 January 1984, Case 327/82, [1982] ECR107) where implicit reference to national customs is accepted; *Schwedler/Parlement* (8 March 1990, Case T-41/89, [1990] ECR II-79) where explicit reference is required;*DíazGarcía/Parlement*(18 December 1992, Case T-43/90, [1992] ECR II-2619) where implicit reference is accepted becausethe Court cannot establish autonomous meaning using elements of EU law and principles.

62 Case C 245/00 SENA [2003] ECR I 1251, paragraph 23, and Case C-306/05 SGAE [2006] ECR I 11519.

63 Examples are Art. 2 Computer Programs Directive (authorship of collective works), Art. 2(2) Rental Right Directive, Art. 2(1) Term Directive (co-authorship of audio-visual works), recital 27 Resale Right Directive. On the latter,in Dali the Court held that with respect to royalties of resale due to 'those entitled under' the deceased author (Art. 6), national law determines who is entitled. But here,of course, it is relevant that typically the law of succession (not copyright law) governs the issue (ECJ 15 April 2010, Case C518/08 (Dali)).

64 Inter alia V. Benabou, Note d'observations, C.J.C.E. (4e ch.), 16 juillet 2009, RDTI 2009, no. 39, 61 ff; Gernot Schulze, 'Schleichende Harmonisierung des urheberrechtlichen Werkbegriffs? - Anmerkung zu EuGH', *Infopaq*/DDF, GRUR 2009/11, p. 1019; P.B. Hugenholtz, NJ 2011, 288, 289; Isabella Alexander, 'The concept of reproduction and the 'temporary and transient' exception'C.L.J. 2009, 68(3), 520-523; F.W. Grosheide, Comment on *InfopaqvDanskeDagbladesForening*, Intellectue leEigendom&Reclamerecht 2009 nr. 6, 318-32.

65 Another angle, not explored here, is that the Court does not consider the wider social and economic effects of its interpretation. Axel Metzger, for example, argues that the Court's textual (literal) interpretation in *Infopaq* results in an overly restrictive standard thatcauses social costs and seems to have little positive effect for the supposed beneficiaries. Axel Metzger, 'Licensing and collecting in the 21st century: What's in sight and who's ahead?', GRUR Int 2010, 687.

66 See Case C-301/98 KVS International [2000] ECR I-3583, paragraph 21; Case C 298/07 Bundesverband der Verbraucherzentralen und Verbraucherverbände [2008] ECR I-7841, paragraph 15; and Case C-403/09 PPU Detiček[2009] ECR I 0000, paragraph 33.

67 C. Handig, The copyright term 'work' - European harmonisation at an unknown level, 40 IIC 665-685 (2009).

68 ECJ 30 January 1985, Case 143/83 (Commission/Denmark), [1985] ECR 427.

69 European Commission, Green Paper on Copyright and Related Rights in the Information SocietyCOM (95) 382 final, Brussels, 19.07.1995. p. 27.

70 ECJ 1 June 1961, Case 15-60, (Simon) ECR 1961, 225 [translated from the French version].

71 H.M.H. Speyart, Comment on *Infopaq*, NTER 2009/10, p. 335; C. Handig, The copyright term 'work' - European harmonisation at an unknown level, 40 IIC 665-685 (2009).

72 See e.g. ECJ 8 March 2011 Case C-240/09 (Lesoochranárskezoskupenie).

73 Case 286/86 Deserbais [1988] ECR 4907.

74 ECJ 10 September 1996, Case C-61/94 (*Commission / Germany)*, [1996] ECR I-3989.

75 See in this vein the Advocate General's opinion of 29 June 2011 in Case C-135/10 (SCF ConsorzioFonografici), on the application of the Rome Convention 1961.

76 In practice, of course, it is the fact that individual Member States are obliged to provide authors from other (EU) Member States the minimum substantive rights that makes it necessary for the EU to ensure that its harmonized copyright standards comply with the Berne minimum.

77 Isabella Alexander, *The concept of reproduction and the 'temporary and transient' exception* C.L.J. 2009, 68(3), 520-523; E. Derclaye, Infopaq International A/S v DanskeDagbladesForening (C-5/08): wonderful or worrisome? The impact of the ECJ ruling in Infopaq on UK copyright law, 32(5) EIPR 247-251 (2010); G. Schulze, *SchleichendeHarmonisierung des urheberrechtlichenWerkbegriffs? - AnmerkungzuEuGH „Infopaq/DDF'*,GRUR 2009, 1019; C. Handig, *The copyright term 'work'- European harmonisation at an unknown level*, 40 IIC

665-685 (2009); V. Benabou, *Note d'observations, C.J.C.E. (4e ch.), 16 juillet 2009*, RDTI 2009, no. 39, 61 ff.

78 Stephen Vousden, *Infopaq and the Europeanisation of copyright law*, W.I.P.O.J. 2010, p. 197-210; V. Benabou, *Note d'observations, C.J.C.E. (4e ch.), 16 juillet 2009*, RDTI 2009, no. 39, 61 ff.;

79 E. Declayre, *Wonderful or worrisome? The impact of the ECJ ruling in the Infopaq on UK copyright law*, 32(5) EIPR 247-251(2010).

80 See note 19 above for a short description.

81 B. Michaux, *L'originalité en droit d'auteur, une notion davantage communautaire aprés l'arrêt Infopaq*, Auteurs & Media (2009) no. 5, 473-488.

82 Stephen Vousden, *Infopaq and the Europeanisation of copyright law*, W.I.P.O.J. 2010, p. 197-210, and *Protecting GUIs in EU law: Bezpec˘nostnı´ Softwarova´ Asociace*, Journal of Intellectual Property Law & Practice, 2011.

83 C. Heinze, *Software alsSchutzgegenstand des EuropäischenUrhebe rrechts,*JIPITEC (2011)Vol. 2.

84 I looked at cases reported in the CJE's case law digest at <http://curia.europa.eu>, counting on the basis of the year in which a case was lodged. This does not include cases withdrawn.

85 The Commission brought five such cases before the Court between 2002-2005 (excluding infringement proceedings which did not result in judgment), which testifies to the controversial nature of the Rental and Lending Right Directive, esp. its provisions on compensation for public lending.

86 V. Benabou, *Note d'observations, C.J.C.E. (4e ch.), 16 juillet 2009*, RDTI 2009, no. 39, 85.

87 Richard Posner, *How Judges Think*, Cambridge (Mass), Harvard University Press (2010), 210.

The Digital Economy Act in the dock: a proportionate ruling?

The High Court of Justice, Queen's Bench division, Administrative Court, 23-28 March 2011, British Telecommunications plc (BT) and TalkTalk Telecom plc v the Secretary of State for Business, Innovation and Skills (BIS) and others Case No: CO/7354/2010. The case was heard by Mr Justice Kenneth Parker.

by **Monica Horten**, PhD. London.

Abstract: The UK's Digital Economy Act 2010 contains measures to enforce copyright on the Internet, specifically a two-tiered form of a graduated response. The Act was challenged in the High Court by two of the UK's biggest Internet Service Providers (ISP), who obtained a Judicial Review of the copyright enforcement provisions. This paper is an overview of the case, based on the hearing of March 2011 and the ensuing judgement. It focuses on the two most hotly contested grounds for the challenge, namely an alleged failure to notify the European Commission under the Technical Standards Directive, and the proportionality or otherwise of the contested provisions. It observes how the judgement accepted the defence argumentation of the government and the copyright owners as interested parties, and how the ISPs appeared to be put on the back foot.

Keywords: Digital Economy Act, Judicial Review, copyright enforcement, copyright infringement, BT, Talk Talk,

Recommended citation: Monica Horten, The Digital Economy Act in the dock: A proportionate Ruling, 3 (2012) JIPITEC, 1 para

A. Introduction

1 This case concerns a Judicial Review of a British law and as such it is unusual, if not the first of its kind. The interest in the case is that it addresses the controversial Digital Economy Act 2010, sections 3-18 (the contested provisions). These sections provide for copyright enforcement measures applied to the Internet. In a nutshell, two British providers of Internet access services – BT and TalkTalk were challenging the decision of the government to impose obligations on them for the benefit of third parties in another industry, namely those organisations with an interest in protecting their copyright. The nature of those obligations was that they were asked to send notifications to their subscribers, based on allegations of copyright infringement supplied by the copyright owners, to hold data on repeat notices and ultimately to impose sanctions using traffic management techniques. The obligation regarding technical sanctions created a form of graduated response or '3-strikes' measures. BT and TalkTalk obtained permission to proceed with the Judicial Review in November 2010[1], and the hearing was on 23-28 March 2011.

2 BT and Talk Talk set out five grounds on which they challenged the Act[2]. These were:

3 *Ground one* – failure to notify the European Commission. It was argued that the copyright enforcement provisions in Sections 3-18 of the Digital Economy Act constitute a technical regulation, and should

have been notified to the European Commission as required by the Technical Standards Directive [3]. On that basis, the copyright enforcement provisions would be unenforceable.

4 *Ground two* – incompatibility with the E-Commerce directive[4], Article 12 'mere conduit', and Article 15 'No general obligation to monitor'.

5 *Ground three* – they were being asked to retain, process and disclose personal data and traffic data incompatibility in a manner incompatible with the E-privacy directive[5]

6 *Ground four* – the contested provisions were disproportionate in their impact on Internet service providers and their subscribers.

7 *Ground five* – incompatibility with the Authorisation directive[6], in respect of the costs which they were being asked to contribute for the implementation of the contested provisions.

8 BT and TalkTalk sought a quashing order for the contested provisions, or declaratory relief that the provisions were unlawful.[7] They were unsuccessful on all grounds, except for the removal of a liability for administrative costs incurred by Ofcom[8], under Ground Five.[9]

9 This review of the case will concentrate on Grounds One and Four, which were the most hotly disputed and most heavily argued. They were also the issues on which BT and TalkTalk should have had the strongest case. However, they did not succeed and the review will outline the arguments put forward for the claimant and the defendants, and in the judgement.

10 One slightly odd aspect of the case is that the defendant 'Secretary of State' was of a different party and government from the one that brought in the Act. The defendant was the current Conservative-Liberal Democrat coalition government. The Act had been passed through the legislature by the previous Labour government, and received Royal Assent on 10 April 2010. The manner of its passing through the Westminster Parliament, in particular through the House of Commons, is the subject of controversy, although that is outside the scope of this case review.

11 The 'others' in the case, were 10 organisations representing the music and film industries. They were led by the BPI (British Recorded Music Industry) and the Motion Picture Association, with legal representation provided by the law firm Wiggin LLP. In addition, there were the British Video Association, Film Distributors' Association, Football Association Premier League, and the Producers Alliance for Cinema and Television (PACT) . These organisations were joined by four trade unions - Broadcasting Entertainment Cinematograph and Theatre Union (BECTU), the Musicians' Union, Equity and Unite.

12 Although they were technically there just as 'interested parties', it was observable[10] that their argumentation influenced the outcome of the case. Their submission to the court was a defence of Act and the copyright enforcement measures, and it arguably functioned to support the government's position. It may be relevant to note that the BPI and the Motion Picture Association had actively lobbied for the Act under the previous government.

B. Background

13 Sections 3-16 of the Digital Economy Act 2010 amend the Communications Act 2003, Section 124. They therefore amend telecommunications law for the purpose of enforcing copyright[11].

14 Importantly for the Judicial Review, the Digital Economy Act copyright enforcement provisions actually set up a two-part structure. The first part provides for the notice-sending and the compilation of the list of subscribers to whom repeat notices have been sent. This is the Copyright Infringement List (CIL) also sometimes referred to as the repeat infringers list, and it would be a form of blacklist of subscribers alleged to have infringed copyright via the Internet connection more than once. The rights-holders would be entitled to see names from the list, for the purpose of taking those individuals to court on ground of copyright infringement. These were the 'Initial Obligations' under the Act.[12]

15 The second part creates a by-pass of the court process. The Internet service providers would be asked to impose sanctions directly against their own subscribers, on the basis of the copyright infringement list. The rights-holders would determine which individuals on the list were to be sanctioned. The proposed measures include throttling or reducing the speed of access to a point where downloading or file-sharing becomes impossible, and cutting off the access for a 'temporary' period which is undefined in the Act. These were the Obligations to Limit Internet Access,[13] frequently referred to as 'technical measures'.

16 An appeals process was to be set up to handle subscribers who disputed the allegations against them. This process was to be set up and overseen by Ofcom.

17 Another important feature of the contested provisions for the Judicial Review is that they fall short of some critical specifications. For example, they do not say how many notices are required in order for a subscriber to be placed on the blacklist. They do not specify exactly which technical measures are to be applied under particular circumstances. Those ele-

ments and others would be specified by two Codes of Practice, which would be drawn up under the auspices of the regulator, Ofcom. The Codes of Practice would go before Parliament as Secondary legislation, and in particular, the code implementing technical measures could be subject to further consultation and Parliamentary scrutiny.

18 Regarding costs, the proposal was that the rights-holders should pay 75 per cent, and the ISPs 25 per cent, of all costs. The judgement on Ground five relieves the ISPs of paying any costs towards Ofcom's expenses, including its own costs for administering the measures, and the costs of setting up and running the appeals process.

I. Ground 1 – technical regulations

19 At issue with Ground 1 was whether or not the contested provisions should have been notified to the European Commission, and more specifically, at what point they should have been notified. Should they be notified before implementing secondary legislation is in place or not? The government had not done so before the Act was put before Parliament, nor had it done so by the time of the hearing, which was almost one year on from the passing of the law. Given the structure of the Digital Economy Act, which was reliant on the Codes of Practice to implement the provisions, the point turned on whether or not the Act had to be notified before the Initial Obligations Code was in place.

20 The core of the argument put forward by the claimants, BT and TalkTalk, was that the Digital Economy Act 2010 established a number of obligations on Internet Service Providers, which would affect the technical operation of their business. As such, there was a requirement to notify them to the European Commission. As the contested provisions had not been notified, the law would be unenforceable.

21 The claimants argued that the contested provisions were prescriptive. This is reflected in the language of the text which says that ISPs 'must', for example, take specified actions upon receipt of the allegations from copyright owners[14] (called copyright infringement reports in the Act). The copyright owners are under no such obligation – they 'may' make the reports to the ISPs.

22 The claimants argued that the prescribed obligations were clear in their effect and that they were capable of being applied by the regulator, Ofcom, with immediate effect and subject to financial penalties.[15] There is no room for the specification to be withdrawn, unless the Act were to be repealed, and therefore it is irreversible. [16] In other words, if it were shown that less restrictive measures could be effective, there is no possibility under the Act for such measures to be introduced.[17]

23 The claimants further argued that the Act must be viewed as a consolidated two-tier approach, since the Obligations to limit Internet access build on the specification that is set out in the Initial Obligations. The second tier cannot operate without the first tier being in place.[18]

24 The government, as the defendant, put forward the argument that the provisions were empty, not prescriptive and merely enabling.[19] At the hearing, the government Counsel, Mr Eadie, described the contested provisions as "a series of highly flexible provisions identifying subject matter areas that need to be covered. They simply do not descend into any sort of detailed regulation". Mr Eadie argued that it followed that the contested provisions had, at the time of the hearing, no legal effect. They would not have legal effect until the Codes of Practice were in place, because one would not know the specifics until the Codes had been finally agreed. As such, the defendant suggested, the law did not yet need to be notified to the European Commission.

25 The interested parties submitted in support of the government's argument, that the "correct test " is not whether the contested provisions contain an obligation, but one of "current legal effect." [20]

26 During the hearing, the judge, Mr Justice Parker, probed the notion of prescriptive versus enabling provisions. Speaking to Antony White QC, counsel for BT and TalkTalk, he explored a view that the contested provisions were "somewhere in the middle".

> *"You can see conceptually, I would have thought, that in a pure enabling law, principles are just laid down and then, let's say, by secondary legislation the actual regime was brought into force, and there would be no dispute, then, that that was anything other than a pure enabling law. Then, at the other extreme, you would have a case where, let's say, legislation is not to be brought into effect until a statutory instrument sets the date, and then you in a case like that, could argue strongly. That is such a formal step that it must be regarded as notifiable Here I think it's common ground you are somewhere in the middle".*[21]

27 The claimants highlighted that whilst, for example, the Act did not set the threshold which would define a 'repeat infringer', it did indicate that there would be a threshold, and there were indications in the pre-legislative documents that it could be set at 'three' copyright infringement reports.

28 The defendant argued that the government intended to notify the Act when the Codes of Practice were in place, and that the Codes were necessary for the European Commission and other Member States to understand correctly what the Act would do[22].

29 The judgement concluded that the Initial Obligations were not merely enabling legislation and that they did constitute a technical regulation. The issue was whether or not they were sufficiently precise as to be enforceable and to have legal effect[23]. On this point, the judgement came down in favour of the government and against the claimants. It stated that the contested provisions were not legally enforceable unless and until a Code of Practice was in place. The ISPs were under no liability, and not required to take any actions under the Act, until the Codes were in place. The Codes of Practice would determine the substantive content of the obligations.

30 The purpose of the notification to the European Commission was to "prevent technical regulations from being enacted and being enforceable against individuals before the Commission and other Member States have had an opportunity to comment upon the proposed regulation."[24] Hence, the judge came to the final conclusion that this purpose was 'not impeded' by the decision to wait until the Code of Practice is in place and he dismissed the claimant's case on Ground.

31 In effect, BT and TalkTalk had been forced into a corner at this early stage. If the Initial Obligations Code did not have legal effect, then it followed that the Code to Limit Internet Access, that brought in technical sanctions against the ISPs' subscribers, also did not have legal effect. This line of argument enabled the discussion of technical measures – which created the greater controversy - to be kept to a minimum. The argumentation at the hearing focussed on the Initial Obligations Code, on the basis that it was necessary to persuade the judge on this point, before one could move on to the second Code to Limit Internet Access. One could extrapolate that this was unhelpful to the claimant's case, since a stronger argument could have been made against the Act with the technical measures included.

II. Ground 4 – proportionality

32 In arguing their case for ground 4, that the Digital Economy Act would have a disproportionate effect on ISPs and on consumers, the claimants presented a case based on a balancing of the freedom to provide services versus copyright, as a property right. They chiefly relied on an economic analysis in expert reports submitted as written evidence.[25]

33 The claimants were trying to show that the government had been unrealistic in its targets for the public benefits to be created by the Digital Economy Act, and that those targets were 'fundamentally flawed'.[26] Moreover, it was claimed that the government had failed to correctly calculate the implementation costs, for example failing to include costs for the appeals process[27]. The objectives were set too high, and a significant cost burden would be placed on the ISP industry for measures which had a high chance of failure.

34 In particular, the claimants were critical of the government's Impact Assessment, which accompanied the Digital Economy Act 2010. The government's target was a 70 per cent reduction in copyright infringement due to peer-to-peer file-sharing. This was based on survey data provided to the government by the rights-holders, stating that 7 out of 10 file-sharers would stop downloading copyrighted material if they were sent a notice by their ISP. It was pointed out by Mr White, for the claimants, that this was the sole source of the data supporting the government's objective.[28] One of the expert reports stated:

> *"even without knowledge of the subsequent edition of the Digital Entertainment Survey, the claim that 70 per cent of those who engage in illegal downloading would stop completely and forever as a result of receiving a notification from their ISP is straining credulity. I would like to think that such an assumption – which is crucial for the entire analysis – should have been considered very carefully, and should have been subject to some sense checks."*[29]

35 In fact, the government's own evidence to the hearing stated that no checks of the methodology behind the survey had been carried out, nor had the government commissioned its own evidence to cross-check it. However, this evidence was not directly challenged by the claimants.

36 The claimants went into more detail of the government's figures, including an assumption that 70 per cent of people ceasing to file-share equated to a 55 per cent overall reduction in file-sharing, and a figure of £400 million per annum for music sales currently displaced by peer-to-peer file-sharing. This was the government's assessment of the scale of the problem and the intended benefit of the legislation was to 'recover' those displaced sales for the music industry.

37 The claimants put up an argument that it was incorrect to assume that all copyright infringement was occurring via peer-to-peer file-sharing networks, since these reflected less than 40 per cent of all traffic on the ISP networks. The displacement of sales could not be attributed to peer-to-peer alone, and it was therefore fallacious to assume such a benefit would be achieved solely by targeting peer-to-peer.[30] On that basis, the contested provisions were a disproportionate response to the problem and a disproportionate burden on the ISPs.

38 The claimants' final argument was that the contested provisions would create a chilling effect, which would have negative economic consequences.[31] However, this argument was rebutted, and eventually turned around into one that supported the government and the interested parties, on the basis that any

economic negatives for 'infringers' were not worthy of consideration.

39 Overall, the judge was not happy at being presented with such a large volume of complex economic analysis[32] and it proved to be less helpful to the claimants than it might have been. He rejected the notion that the proportionality assessment should be judged on economic criteria alone and dismissed the claimants' extensive analysis as "a general utilitarian calculus"[33]. He also rejected the balancing proposition which the claimants presented, namely the right to free trade versus copyright as a property right.

40 The defendant (the government) and the interested parties put forward an alternative line of argument which the judge preferred. The defendant proposed that the two relevant questions in determining proportionality were "is it a legitimate aim?" and "is this type of legislation an appropriate response?" It was argued that the Digital Economy Act measures were more proportionate than the current system which relies on a preliminary action to obtain the contact data for Internet users whose IP addresses have been identified on file-sharing networks, in order to take court action against those users. It was suggested that the contested measures, which would draw a distinction between repeat infringers and one-offs, and would send warning notices to Internet subscribers, were a fair response[34] to the problem of peer-to-peer file-sharing .

The government's points were reprised and expanded by the counsel for the interested parties, Mr Saini. In summary, the interested parties - the copyright owners - submitted after both claimants and defendant had completed their submissions. They demolished a number of the points raised by the claimants over the course of the hearing. They began with the balance proposed by the claimants – freedom to provide services versus copyright as a property right, and the judge confirmed that this was 'a case of conflicting rights'.[35] Then they took the judge through the rationale supporting the contested measures, rebutting the claimant's criticisms of the 70 per cent figure, and explaining the government's justification for relying on it[36]. Finally, they invited the judge to consider the balance between the rights of copyright owners to protect their property versus the rights of the alleged infringers to enjoy 'the fruits of their unlawful behaviour[37]':

"That is effectively a shorthand for the point which was debated between my Lord and Mr White, which is that there is a cost here, because consumers who are already infringing copyright are going to suffer a disbenefit because they're going to have to stop infringing copyright."

41 Mr Justice Parker responded that "the government would be holding itself up to ridicule if it took into account the consumer welfare of infringers".[38]

42 The judgement dismissed all of the claimants' economic criticisms. In summary, the judgement did not agree with the claimants' assertion that the government should provide substantiated figures in its impact assessment. Instead, the judgement stated that legislation could go ahead on the basis that it would in general terms, make an impact.

43 The judgement stated that it was not sufficient to show that there were errors in the impact assessment. It determined that the correct approach in a case where it is inherently difficult to quantify the costs, benefits and outcomes would be for the legislator to "identify and take account of the important benefits and their broad measure".

44 The judgement declared that "Parliament" was entitled to decide on the basis that there would be a 'significant reduction' in file-sharing, citing the case of Sinclair Collis Limited v Secretary of State for Health[39] :

"a decision to legislate may be proportionate even though cost/benefit analysis produces a negative money balance; or a variant of that, that a decision to legislate may be proportionate provided that the legislator identifies and takes account of the important detriments and their broad measure."

On this basis, the claimants' case for a proportionality challenge was dismissed:

"in the context of a proportionality challenge, the relevant issue is not whether the figure of 70 per cent in the impact assessment was robust, but whether Parliament was entitled to proceed on the basis that a carefully worded letter from the subscriber's ISP, drawing the subscriber's attention to the fact that the unlawful file sharing had been detected, and that persistent infringement could lead to unpleasant legal sanctions, would have a strong and immediate impact on unlawful P2P file sharing."[40]

C. Observations

45 It should have been the government (Secretary of State) who shouldered the burden of proof in this case, and who put forward the evidence to justify the contested measures.[41] However, as a general observation, it seemed that it was the claimants who had to justify their challenge, and who were on the back foot.

46 It does seem that if the claimants had been able to establish that the case concerned the contested provisions as a whole, incorporating the two-tier process in its entirety, then they would have been able to mount a stronger challenge to the contested provisions. Notably, they could have presented the judge with a different balance, namely balancing the right to protect copyright against the interference with the individual's right to due process. This is a politically more potent argument[42]. However, as they were pressed to stick just to the Initial Obligations Code, making that argument would have been more difficult.

47 The judgement accepted the arguments of the government and the interested parties on both of the grounds considered here. However, it would seem that a way was found to fit the judgement to the case.

48 On Ground one, there appears to be a fairly thin line between what should be notified and what may wait until secondary legislation is in place. If one compares the Digital Economy Act with the French Creation and Internet law, or the Spanish *Ley Sinde*, it would seem that there is little difference in the level of specification in any of these three laws. Yet, two were remitted to the European Commission prior to any secondary or implementing legislation, and one was not.

49 On Ground four, it could be observed that a piece of case law had been found to get the government off the hook. The economic figures in the government's Impact Assessment do merit investigation. It is correct that the 70 per cent figure used to set the targets for the contested provisions was sourced from one market research survey, supplied by the copyright owners[43], which was contradicted by a follow-up survey[44] a year later. The methodology for both surveys was not examined nor made public, and it is somewhat concerning that the government did not have access to methodological information, as stated in the written evidence to the review.[45] It would seem to invalidate the concept of an Impact Assessment, if the quality of the data used to determine the assessment is subsequently irrelevant. The notion of an Impact Assessment is further invalidated if the legislator is entitled to make decisions based on a general assumption supplied by the industry, which has the greatest interest in having the legislation on the Statute – which is the implication of this judgement.

50 Addendum: The judgment was upheld on appeal, with one small additional concession to the appellants relating to costs.[46] The appeal ruling agreed that BT and TalkTalk should not have to contribute to the case fees for subscriber appeals, since case fees would be 'administrative charges' within the context of the Authorisation directive, and therefore unlawful.

1 Administrative Court , 2010b. The High Court of Justice, Queen's Bench division, Administrative Court, Case No: CO/7354/2010, Notification of the judge's decision with attached reasons, 11.11.2010.

2 Administrative Court , 2010a. *Claimants' Statement of Facts and Grounds. Prepared by Antony White QC and Keiron Beal, 5 July 2010,S.10.* In the High Court of Justice, Administrative Court, Claim number CO7354/2010. British Telecommunications plc (BT) and TalkTalk Telecom plc v the Secretary of State for Business, Innovation and Skills (BIS).

3 1998/34/EC of 22 June 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, and as amended by Directive 1998/48/EC of 20 July 1998.

4 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

5 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Amended by 2009/136/EC

6 2002/20/EC, of 7 March 2002, on the authorisation of electronic communications networks and services. Amended by 2009/140/EC .

7 Administrative Court, 2010a, as above, S.11.

8 Ofcom is the UK regulator for telecommunications. In respect of the Digital Economy Act, it has been given responsibility for facilitating and overseeing the copyright enforcement measures. However, in this context, it is important to note that Ofcom will not be a 'Hadopi'. It will not have any active role in forwarding notices or applying sanctions.

9 Administrative Court , 2011. *.Approved Judgement*, S.265. The High Court of Justice, Queen's Bench division, Administrative Court, 23-28 March 2011, British Telecommunications plc (BT) and TalkTalk Telecom plc v the Secretary of State for Business, Innovation and Skills (BIS) and others, Case No: CO/7354/2010,

10 The author attended the court hearing on Days 1,2 and 3 and was able to personally observe the dynamics of the various parties. This case review is based on notes from the case, and transcripts of the hearing to which the author has had access, as well as the documents cited.

11 For more detail on the Digital Economy Act and how it amends telecoms law, see Monica Horten, 2011a, Copyright At A Policy Cross-Roads – Online Enforcement, The Telecoms Package And The Digital Economy Act in 'Net Neutrality and other challenges for the future of the Internet, Proceedings of the 7th International conference on Internet, law and politics, Universitat Oberta de Catalunya, Barcelona, 11-12 July 2011.

12 Digital Economy Act, 2010, Articles 3-7 Initial Obligations

13 Digital Economy Act, 2010, Articles 8-12 *Obligations to Limit Internet Access*

14 Digital Economy Act, 2010, Article 3, Obligation to notify subscribers of reported infringements.

15 Administrative Court, 2010a, as above, S.93

16 Administrative Court, 2010a, as above, S.103.

17 Administrative Court, 2010a, as above, S.96.

18 Administrative Court, 2010a, as above, S.77.

19 Author's notes from the hearing, day 3, Mr Eadie making the submission for the Secretary of State.

20 Author's reading of court transcript, Day 4.

21 Author's notes from the hearing, day 1, Mr Justice Parker, hearing Mr Antony White QC for BT and TalkTalk

22 Author's notes from the hearing, day 2, Mr Eadie making the submission for the Secretary of State

23 Administrative Court, 2011, S.80.

24 Administrative Court, 2011, S.88.

25 Expert report prepared by Professors Mansell and Steinmueller: Administrative Court , 2011, S.232 and Administrative Court, 2010a, S.4; and expert report by Dr Koboldt: Administrative Court , 2011, S.248-261.

26 Administrative Court, 2010a, as above, S.207

27 Author's note taken at the hearing, Day 2, checked against transcript. Mr White, discussing costs which had been left out of the government's account, cited subscriber appeals.

28 Author's note taken at the hearing. Mr White's point is substantiated by the Digital Economy Act 2010 Impact Assessment,

page 70, which states that: "Results from the Digital Entertainment Survey (2008) indicate that 70% of copyright infringers would stop downloading digital products if they received a call or letter from their ISP. The policy objective is to achieve this reduction within 2 years."

29 Administrative Court, 2011, S.255. Citation is from the report by Dr Koboldt.

30 Administrative Court, 2011, S.251 and author's notes from the hearing.

31 Based in part on an intervention by Consumer Focus and Article 19.

32 Administrative Court, 2011, S.242. He complained that the claimants had submitted four expert reports running to 220 pages, whereas the interested parties had submitted a modest 50 pages of expert evidence.

33 Author's notes from the hearing, Day 2, the claimants' submissions and Day 4, the interested parties' submission.

34 Author's notes from the hearing, Day 3.

35 Author's reading of court transcript, Day 4.

36 This is in spite of it having been contradicted by a figure in the subsequent 2009 survey Administrative Court , 2011, S.254.

37 Administrative Court, 2011, S.249

38 Author's reading of court transcript, Day 4.

39 Administrative Court, 2011, S.244. Sinclair Collis Limited v Secretary of State for Health [2010] EWHC 3112 (Admin)

40 Administrative Court, 2011, S.256

41 Author's notes from the hearing, Day 1.

42 Monica Horten, 2011b, The Copyright Enforcement Enigma – Internet Politics and the Telecoms Package – see chapter 12.

43 The figure was sourced from the Digital Entertainment Survey 2008, which is sponsored by Wiggin LLP (Administrative Court , 2011, S.29 and S.254).

44 The follow-up survey was the Digital Entertainment Survey 2009.

45 Rachel Clark, of BIS, in written evidence, as cited in Administrative Court , 2011, S.252.

46 In the Court of Appeal from the High Court of Justice, Queen's Bench Division, Administrative Court, Case No: C1/2011/1437, 6 March 2012. Appeal heard by Lady Justice Arden, Lord Justice Richards and Lord Justice Patten/.

Derecho Privado de Internet, Cuarta Edición

Pedro Alberto de Miguel Asensio

Book Review

by **Gerald Spindler**, Göttingen, Prof. Dr., Department of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law, University of Göttingen

Recommended citation: Gerald Spindler, Book Review: Derecho Privado de Internet, cuarta edición by Pedro Alberto de Miguel

1 This book is appearing in its 4th edition, which gives a clear hint of its outstanding importance in the Spanish (and international) discussion. The author deals with nearly all conceivable issues in terms of 'Internetl aw' or electronic commerce.

2 Whereas the first chapter is dedicated to the foundations of the Internet –in particular the 'governance' of the net such as ICANN or domain names and IP numbers–the second chapter turns to the fundamental services and their providers with regard to their liability. The steadily intensifying discussion surrounding data protection (which recently reached its zenith with the publication of the proposal of the new EC regulation on data protection) is dealt with in the third chapter, followed by a somewhat smaller part on unfair competition law. In contrast, De Miguel focuses on intellectual property rights such as trademark law (fifth chapter) with special regard to domain name litigations or copyright (sixth chapter); here the author applies abstract findings on the most salient phenomena on the Internet, including p2pnetworks, search engines and the retro-digitization by Google Books. The last chapter of the book is dedicated to contract law with an emphasis on the formation of the contract, electronic payment services and digital signatures and their like.

3 Given the global character of the Internet, it is quite obvious that conflict of laws plays an essential role in its regulation. Hence, every chapter (each legal area) is concluded with a reflection on international private law and the criteria that should be used to assess the location of an act or a damage. In this context and with regard to the principle of country of origin enshrined in Art. 3 of the E-commerceDirective, the author recommends– in line with the recent decision of the European Court of Justice – that this article not be read as a principle of private international law rather than limiting the applicable law (No 127 s.). However, although the ECJ has now clarified the interpretation of Art. 3 of the E-commerce Directive, the details of its application still remain unclear, such as the test of which law is more provider-friendly (including how far the test should reach).

4 For such an encyclopedic review of nearly all aspects of Internet law, it is quite difficult for a reviewer to select specific parts on which to concentrate. I will focus on abstract issues, such as regulation of the Internet, as well as on some more specific issues, including liability and intellectual property rights.

5 In his first chapter, De Miguel elaborates the well-known tension that was intensively discussed in the 1990s between the anarchical and global structure of the Internet on one hand and the regulatory approaches of states to somehow regain control of the Internet. The author omits neither self-regulatory phenomena nor software as a means to steer the behavior of participants, taking into account most of the internationally relevant literature from both sides of the Atlantic (No. 71 –89). He discards the idea of a virtual space free of regulation and points to a multifactor and multilevel approach that pragmatically uses those means that promise to render an efficient result in each case.

6 Regarding liability issues, Miguel intensively discusses the role of contractual disclaimers (No. 138 -140) that are frequently also part of standard contract terms. However, the author does not further analyze whether these standard contract terms could be deemed unfair, for instance with regard to the control of virus infections of data stored by a host provider. After reviewing potential liability issues such as defamation, product liability, and wrongful information, De Miguel also debates the role of Internet intermediaries.He takes the developments in the US into account, in particular the DMCA, and compares

these with the harmonization in Europe (and the implementation of the E-Commerce Directive in Spain – No. 196 ss.). The Spanish jurisdiction plays an interesting role in the EU as some important cases have already reached the ECJ, somehow puzzling by the narrow interpretation of the E-Commerce Directive. This is the background for Miguels commentaries (and criticism), for instance, on the ruling of the Court of Barcelona concerning Google with regard to Art. 13 of the E-CommerceDirective (by applying the caching privilege, No. 207).

7 Regarding host providers, De Miguel highlights the developments in Spain, especially the decisions concerning the Google AdWords case (No. 208 ss.). However, the difficult distinction between 'neutral' host providers and 'actively' engaged providers offering additional services to customers, thus losing their liability privilege according to the decision of the ECJ in the L'Oreal v. eBay case, is obviously still not being discussed in depth in Spain. A well-known deficit of the Spanish implementation of the E-Commerce Directive consists in the definition of knowledge of the provider, which is apparently restricted to official notices by 'competent authorities' (No. 217). Miguel criticizes this stance with good grounds as 'confusing'.

8 Of utmost interest for other member states such as Germany are the vigorous rules in Spain regarding liability exemptions of hyperlinks and search engines (No. 229 ss.). Art. 17 of the Spanish act applies the liability regime of host providers to search engines and hyperlinks without any distinction.

9 Thus, De Miguel gives a broad overview of the recent developments of liability at the Spanish, European, and international levels. However, given the recent cases of the European Court of Justice, it would be commendable to extend this profound analysis to injunctions. Obviously, actors are increasingly sticking to injunctions to safeguard their interests, in particular in cases of Internet marketplaces (trademark infringements) or access providers (copyright cases like the SABAM case decided by the European Court of Justice). In particular, in a huge number of cases the German courts have developed new criteria for assessing the liability of intermediaries that go far beyond the traditional landmarks laid down in the E-Commerce Directive, including obligations to collaborate between Internet marketplace and trademark owners or some kind of notice-and-takedown procedure for host providers of blog forums.

10 With respect to data protection, the author outlines in detail the fundamental directives on the European level as well as their Spanish counterparts. Miguel extensively analyzes the scope of the famous Lindqvist decision of the European Court of Justice concerning personal data made public by a website (No. 268 ss.). Moreover, the author realizes the ever-growing importance of social networks by reporting the corresponding recommendations of the Art. 29 Data Protection Group. However, De Miguel obviously restricts himself to the modest role of commentator (cf. for instance No 260 ss. concerning the concept of consent); the severe problems of consent assumed just by means of registration–for instance, in the case of Facebook–are partly omitted. In general, the concept of consent is at the center of debates surrounding the new EU proposal of a regulation on data protection; this needs to be elaboratedmore, given the fact that people often are not aware of the dangers that are involved concerning the use of their data. Moreover, the specific problems of minors who represent a large part of the social communities should be on the agenda more than before.

11 With regard to cookies and behavioral targeting/advertising (No 283 ss.), De Miguel points to the (debated) Art. 5 (3) of the E-PrivacyDirective 2009/136/EU. Unfortunately, however, he does not take a firm stance on the highly disputed issue of how these provisions should be implemented, given the fact that the same directive obviously allows for the use of a browser to express in general (!) a consent for setting a cookie. Moreover, the conflict between freedom of speech and data protection is becoming more and more important because any communication contains personal data. This conflict, however, is seldom addressed by regulations, nor is it addressed by Spanish data protection rules as Miguel does not refer to this fundamental conflict. Finally, the application of EU data protection law with regard to US-based corporations entangles problems of interpretation of location of data processing. The author here follows the approach of the Art. 29 Data Protection Group, which will now be codified in the new EU proposal on Data Protection. Thus, the market principle will govern the application of data protection norms, in particular whether the website has directed its services and offers to clients in the EU. The existing bulk of data protection norms already can be read in that manner, a view shared by Miguel (No. 296 ss.).

12 Finally, it is interesting how the discussion on intellectual property rights is reflected in De Miguel's oeuvre. With regard to Web 2.0 content, in particular 'mash ups', the author details the protection of newly generated content as well as the limits for users to modify protected content of third parties (No. 599 ss.). Of utmost interest are De Miguel's reflections upon issues of responsibility of services such as Facebook or YouTube that claim to benefit from the liability privileges of host providers while at the same time imposing strong licenses on their users to make use of the content (No. 603 s.).The author points to the ongoing discussions about monitoring obligations of these services as well as deals with regard to collecting levies.

13 In contrast to other works on Internet law, it has to be emphasized in this context that De Miguel also discusses licenses such as creative commons at length (No. 605 ss.). As the author shows, Spanish courts (as well as other courts in the EU) accept creative commons licenses as applicable and enforceable (No 609). According to the importance of Spanish cases on cache copies related to Google services, De Miguel pays much attention to the interpretation of the corresponding limits of the right of reproduction (No. 616 ss.). However, from the perspective of an outsider, the highly debated issue of streaming and its impact on cache reproduction should be taken up in future editions to come.

14 Regarding limits to copyrights, Miguel concentrates on the copy for private purposes. This is closely related to the famous Padawan case in Spain concerning levies for

copying without any distinction between private and business purposes (No. 640 ss.). He also discusses the concept of (tacit) consent to make use of content uploaded to the Internet, at least for services that are quite common such as search engines (No. 648 ss.). De Miguel seems to favor this as a back door to the closed list of limits to copyright enshrined in the Information Society Directive, coming close to the fair use doctrine in the US. However, we should realize that these figures and constructions undermine traditional legal thinking and freedom of consent, thus opening the Pandora's box of every 'unwritten' limit to copyright. The list of interesting topics seems to be endless – and Miguel copes with almost all of them, be it the Google Books project, the *loi Hadopi* in France or other legislative initiatives.

15 In sum, there are scarcely any topics of Internet law missing. Only a few issues are not touched upon, and it might enrich the book to include chapters on antitrust law, media law (such as regulation of convergence, which De Miguel already discusses) or contracts with providers, including access provider contracts, social network contracts, or 'apps' contracts concerning specific platforms for software and digital content. However, this should not be regarded as a fundamental critique of the oeuvre as, in sum, De Miguels book is indeed an encyclopedia of Internet law, with special regard to its implementation in Spain. The effort to undertake such a comparative legal work is huge, and it is the only way to cope with the global phenomenon of the Internet. The book is highly recommendable for everyone engaged in electronic commerce and Internet law as a rich source of information that spans all kinds of legal areas,thus making it indispensable for European lawyers in these fields.

JIPITEC

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law

www.jipitec.eu