Community wireless networks, intermediary liability and the McFadden CJEU case

Federica Giovanella, Melanie Dulong de Rosnay

Community wireless networks, intermediary liability and the McFadden CJEU case

Federica Giovanella and Mélanie Dulong de Rosnay

1. Introduction

This article focuses on the possible implications of the McFadden decision[1] by the Court of Justice of the European Union (CJEU) on the development and sustainability of community networks (CNs). CNs provide internet connectivity through open wi-fi, normally based on distributed infrastructure and wireless technologies, that enable users to create an open, community owned and run, network.

CNs constitute a grassroots alternative to commercial internet service providers (ISPs): as infrastructure commons, they have the potential to be participatory, democratic, and more respectful of communications privacy.

The possibility of offering open wi-fi is one of the main issues at stake in the McFadden case. This article explains how the CJEU decision is likely to affect the fate and the design of CNs. Particular attention is paid to the effect of the decision on the organisational shaping of CNs in Europe and structural changes CNs may have to consider implementing:

- the donation policy, the fee or absence thereof, as the decision refers to the commercial status of providers;
- the legal status (network operator, intermediary, internet service provider) and the existence of a legal representative, or the absence thereof in the case of very decentralised CNs;
- possible warranties and disclaimers contained in the service Terms of Use;
- the technological decentralised architecture, impacting and impacted by possible password, data retention and registration obligations.

After describing what are CNs and how they work (part 2), the article presents the liability challenges for CNs and in particular the hurdles to assign liability (part 3 3) and the specific situation of the 'Störerhaftung', the legal doctrine that provides that a wi-fi operator is responsible for users' wrongdoings in Germany, the jurisdiction of origin of the McFadden case.

The article then analyses in detail the McFadden decision (part 4) and its implications for the organisational shaping of CNs according to selected design features (part 5). It finally draws some conclusions on future scenarios (part 6).

2. The structure of community networks

A CN is a distributed network organised with a bottom-up approach. Network devices are placed in people's houses and interconnected to one another with an unplanned topology. The interconnection is normally wireless over unlicensed bands, but in some cases the community is also able to include wired interconnections. Most CNs are mesh networks and require routing: distributed routing protocols take care of identifying the correct path from the sender to the destination and every node participates in routing the other's messages. CNs do not need careful planning and/or a predefined number of nodes: when a core of nodes is active, the network can be enlarged simply by adding more nodes, which, in turn, will be the entry points for future participants that want to join. The only technical requirement is to be in the wireless communication range (up to several kilometres with directive antennas) of an existing node.

CNs may also offer some internal local services, as for instance social networks, telephony and messaging; these services are managed by the people of the community and are independent from the mainstream internet access services, which can be either simple ADSL connections shared by the users (so called 'gateway nodes'), or high speed connections sponsored by the community itself. In the latter case, the CN is also considered a bottom-up ISP.

CNs rely on ethical values of participation, sustainability[2], universal access, net neutrality and privacy. They are built, owned, managed and used by the community as a commons[3].

The distributed infrastructure of the network reflects (and is reflected in) a peer-to-peer organisation where there is no hierarchical structure either in technical or in social terms. A technopolitical utopia, 'the desire of mesh network developers is to give the Net a technical structure which makes it difficult to impose any

top-down control structure.'[4] For Benkler, 'The main challenge to leveraging this fact into a decentralization of power over wireless networks is to design technical and contractual systems that can permit unrelated individuals to share access to their diversely owned wireless spots'.[5]

As for their internal governance, most CNs do not have written norms regulating relations between users. Communities normally adopt soft regulatory tools as terms of use for their services, manifestos with general egalitarian principles, such as the 'Picopeering Agreement'[6]. Other CNs implement different, more structured instruments, as for instance the 'Compact for a Free, Open & Neutral Network' (FONN Compact)[7] of the Catalan network 'Guifi.net'. The FONN is basically a licence binding both the network and the users.

Finally, CNs often rely also on anonymity. Even though the majority of CNs provide static IP public addresses to their members/subscribers, some of them – such as the Italian network Ninux.org – do not assign IP addresses. In fact, although each node has an 'internet protocol' (IP) address, users choose their own IP address and can change it at any time, which makes it irrelevant to search for and allocate liability based on IP addresses. Some networks keep track of the modification in IP addresses while some would not be able to do so because of their underlying technical design choices. This means that they cannot be considered highly reliable; in turn, this means that even if the IP address is known, it would be almost impossible to identify the person who was using that number at a given moment. The scenario is further complicated by the simultaneous application of anonymisation software or encryption techniques.

All these features may affect the way law applies to these networks. This paper focuses mainly on intermediary liability aspects, which are those touched upon by the CJEU's decision in McFadden.

3. Liability issues in community networks

The distributed architecture of CNs creates several legal challenges.

Distribution causes the fragmentation of data and conduct, so that it becomes difficult, or even impossible, to understand who committed a specific action, or even to determine if an action was caused by a single identifiable person[8]. In fact, since the possibly illicit action might be assigned to a high number of different users' machines, it is not only technically but also legally very problematic to understand who contributed to the violation of a right[9].

In the realm of tort law, the above described features of CNs allow the consideration of at least three different scenarios, involving the three main actors of CNs: the end user, the internet service provider, and the CN itself[10].

3.1 End user

A single user can either be held liable for her own conduct or, if routing another user's data, for taking part in the action of the other user or facilitating it. In such cases, givien the lack of harmonisation in the general civil liability sector, ordinary rules of civil liability of each Member State wall apply.

In both circumstances, the first step to be taken to enforce the infringed right would be to identify the person behind the screen. However, this goal might be difficult to achieve due to the high level of anonymity and fragmentation that characterises CNs. The structure of CNs poses new obstacles to traditional laws, where acting against the actual wrongdoer would be the most direct approach.

3.2 Community networks as entities

Another possibility is that the CN itself – as an entity - could be accountable for what happens inside the network. However, CNs are often neither incorporated as companies, nor even have a clear structure, with a person in charge of the community who could be considered liable in case of wrongful actions. In the Italy cases, Ninux does not have legal personality and it would not be possible to sue a legal person. A partially different case is where CNs organise themselves as (or are run by) foundations or associations, as Guifi.net. Foundations and associations will normally have a legal representative, in the form of a committee or a president, who could be accountable for the actions of the members. Even though this depends again on national law, normally foundations and association (must) also have financial assets on which the whole activity is based, and from which fines and other legal fees could be extracted.

It should be noted, however, taking Guifi.net as an example, that its FONN Compact explicitly includes a section devoted to 'Security and Responsibility'. This section states that the 'open network is not responsible for any damage a user may suffer during its use' and that 'each user is responsible for his use of the network, the contents he contributes and his act'. The same sections also clarify that private networks connected to Guifi.net are excluded from the application of the FONN itself. These provisions aim at shielding Guifi.net (and the foundation) from liability in case of wrongful actions, in a way akin to what a commercial ISP would do. This means that, despite the existence of a foundation which could theoretically be held liable for users' wrongful conducts, the FONN shifts risks to the users accepting its conditions.

3.3 Internet service providers

When the wrongdoing is committed through a gateway node, another subject comes into play: the ISP. ISPs' liability is regulated by national transpositions of Directive 2000/31 on Electronic Commerce[11]. The Directive allows providers to be shielded from liability if they meet specific requirements[12]. If they do not comply with the requirement of the Directive – and its implementation – providers can be held liable for a third party's conduct. On the contrary, if the requirements introduced by Directive 2000/31 are met, the provider will be exempt from liability, meaning that it will not be obliged to pay damages even if its conduct did somehow cause the damage. However, such exemptions do not prevent national courts from requiring the ISP to terminate or to prevent an infringement, exactly as in the case of injunctions (art 12.3).

The Directive introduces three different kinds of providers - access providers, caching providers and hosting providers – but only access providers might be affected by the McFadden decision analysed here.

3.3.1 Access providers

The situation applicable to CNs is the one involving the access provider (or 'mere-conduit' provider), whose liability limitation is introduced by article 12 of the Directive. Mere-conduit providers – that is those affected by the McFadden decision analysed

here– are described by the Directive as those whose service consists in 'transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network'. Such intermediaries are not liable for user's conduct provided they do not (a) initiate the transmission; (b) select the receiver of the transmission; and (c) select or modify the information contained in the transmission.

Access providers normally rely on contractual clauses through which they forbid their customers to share the connection; in so doing they limit their responsibility. If the user/node opens his/her connection to the network he/she breaches the contract. He/she could therefore be considered liable for breach of contract and be asked to pay for the loss suffered by the provider in case an illicit action took place through the gateway and caused damage to someone[13].

As for the gateway node, since it has a public IP address assigned by its access provider, the owner of the node would be identifiable and could be sued for damages directly by the victim of the wrongdoing. However, it should not be taken for granted that a user could be considered liable for another person's conduct. Indeed, national laws would apply: for instance the Italian framework for tort law would not allow liability to be placed on the gateway node for the activity of another user, since no general clauses exist on third-party liability[14].

Nonetheless, making the hypothesis that the gateway could be liable for another user's illicit action, once it had obtained an IP number, the plaintiff could ask a judge for a motion to obtain the identity of the subscriber. If a court grants this kind of motion, the gateway user's access provider matches the access data with the identification data of its customer, obtaining the real identity of the gateway subject, who can in turn be sued or contacted for a settlement by the plaintiff[15]. This possibility has already been tested at both national and European level, for cases of copyright infringement. In Europe, the conflict between the need for enforcement and users' personal data protection has very often been solved by judges in favour of the latter[16]. This would be yet another obstacle to the enforcement of rights.

3.3.2 Open wi-fi: duty of care versus negligent conduct

A different case might be one where the law considers leaving a wi-fi connection open to anyone to be tantamount to negligent conduct. In other words, when law imposes on users a specific duty of care for their internet connection, the fact of not protecting the connection could make them liable. A few European countries adopt this rule. A clear example is the French one: the so called 'HADOPI' law requires internet subscribers to make sure that their wi-fi connections are not used to infringe copyright. However, it is currently not clear how one should comply with this obligation[17]. Some hold that subscribers should secure their network by means of passwords, in order to avoid incurring liability for third parties' infringement of copyrighted works[18].

Germany represents an even more interesting case worth detailed analysis in particular because it also related to the system from which the McFadden case emerged.

3.3.3 The German doctrine of 'Störerhaftung' applied to open wireless networks

Although there is no specific provision that introduces liability for third party's conduct for the case of unsecured wi-fi, the *Bundesgerichthof* (BGH – the German Supreme Court) has applied analogically § 1004 of the German Civil Code (BGB) which offers injunctive relief against infringement of property to infringement of IPR[19]. The concept is the one of 'Störerhaftung', meaning 'liability of the interferer'[20]. This liability is a form of strict liability, but limited to injunctions[21], that is: limited to measures that aim at stopping the infringing activity or at preventing it for the future. These injunctions can be granted only when three conditions are satisfied:

- first, there must be an adequate causal contribution to the activity of the infringing party;
- second, there must have been a legal and factual possibility to avoid the third party's infringement;
- third, the subject must violate a reasonable duty of care or monitoring duty aimed at preventing infringements[22].

In spite of this doctrine, as a consequence of the implementation of Directive 2000/31, intermediaries (theoretically) enjoyed anyway the limitation of liability briefly described above, laid down in articles 7-10 of the German Tele-Media Act (*Telemediengesetz*)[23]. However, the applicability of these provisions to wi-fi operators is not entirely definite; it is not the case that the German legislator recently introduced a specific provision that extends these liability limitations to wi-fi ISPs.

As mentioned, the BGH has sanctioned the liability of a person for unsecure wi-fi, both in private networks and in commercial networks.

In the 2010 case '*Sommer unseres Lebens*'[24] the BGH considered a private owner of an unprotected wi-fi network to be liable for copyright infringement committed by an unidentified person. The owner of the network should have protected it with safety measures to prevent the misuse of third parties[25]. The suitability of the measures should have been assessed considering the technical standards applicable when the modem was installed. The fact that the owner had not replaced the password set by the producer of the router was enough for the court to hold the owner liable for the violation of a specific duty of care[26]. Other courts took a different approach and held that the password set by the producer was a sufficient protection[27]. In the *Sommer unseres Lebens* the BGH did not even consider the application of the liability exemption introduced by Directive 2000/31[28].

3.3.3.1 The case of commercial open wireless networks

A partially different approach is adopted by the courts with regards to commercially used open wireless networks. It seems that differences exist between the case of networks accessible only by users known by name (as in hotels) and networks accessible by unknown users.

For instance, the Court of Frankfurt am Mein held that a hotel owner is not responsible for copyright infringement committed by an unidentified individual, when the network was protected with industry standard encryption technology[29]. In a case involving the owner of a holiday apartment, the same court considered the owner not liable as he had instructed his guests not to use the wi-fi network for illicit actions[30].

In another case, the district court of Hamburg applied the liability limitation of the Tele Media Act to the wireless network operated by the owner of a hotel[31].

Hence, basically when a provider of a commercial network can know the users by name, password protection or instructions to users are enough to shield her from liability[32].

3.3.3.2 The case of unknown users

In cases where users are unknown, courts have adopted fluctuating decisions. In a case involving an internet café, the Regional Court of Hamburg held that the owner was liable since he had not blocked the ports that were used by unknown clients to share copyrighted files[33].

In 2014 the district court of Berlin-Charlottenburg decided on a lawsuit involving Freifunk, the main German CN. The court ruled out the liability of the operator of the Freifunk wi-fi hotspot under the doctrine of Störerhaftung. Interestingly, the court discussed whether the network operator had violated a duty of care and it stressed the importance of not impairing the business of 'free radio'. More precisely, the court stated that imposing upon the owner an obligation to block certain ports or DNS or to instruct all the users would place an excessive burden on the owner[34].

This was the legal framework for open wi-fi when the Munich Regional Court asked for a preliminary ruling in the McFadden case.

4. The 2016 European Court of Justice's decision in *McFadden*

4.1 Background of the case: an open wireless local area network (WLAN)

On 15 September 2016 the Court of Justice of the European Union adopted a decision in a case that could potentially affect any CN in Europe[35].

The request for a preliminary ruling was made by the Munich Regional Court in Germany in a process pending between Tobias McFadden and Sony Music Entertainment Germany GmBH.

Tobias McFadden owns a shop where he sells and leases lighting and sound systems. Within his shop, Mr McFadden runs a wireless local area network (WLAN) free of charge; access to the network was intentionally open to anyone and not protected by a password, to allow customers to use it and to draw passers-by's attention.

In September 2010, by means of this WLAN a musical work was made available to the public on the internet free of charge, without the consent of the right holders. Sony Music, the producer and the right holder of that work, sent a formal notice to Mr McFadden to obtain protection of its rights on the musical work. As a response, Mr McFadden brought an action to obtain a negative declaration (so called 'negative Feststellungsklage') before the Munich Regional Court.

Sony counterclaimed asking for damages compensation on the ground of direct liability for copyright infringement. The company also asked an injunction, meaning: an order from the judge to stop McFadden's allegedly infringing activities.

In January 2014, the Munich court dismissed Mr McFadden's action and upheld Sony's counterclaims. Tobias McFadden appealed the decision, arguing that he is exempted from liability thanks to article 12.1 of Directive 2000/31 (§ 8 of the *Telemediengesetz*). As referred to above, Directive 2000/31 introduced internet service providers' liability exemptions; in particular, article 12 deals with mere-conduit (or access) providers.

Consequently, Sony argued that in the event that the Munich court would not find Mr McFadden directly liable, it should apply the *Störerhaftung* doctrine as McFadden had not secured his wireless network, so allowing third parties to infringe Sony's copyright.

Paragraph 97 of the German Law on Copyright (*Gesetz über Urheberrecht und verwandte Schutzrechte – Urheberrechtsgesetz*)[36] introduces the right for the copyright holder to ask for an injunction and for damages compensation in case of copyright infringement. This paragraph has been interpreted as applicable to both direct (*Täterhaftung*) and indirect infringements (*Störerhaftung*). As already explained, a person that contributed to the infringement committed by another person, either voluntary or with a sufficient degree of causation, can be considered a *Störer*, meaning: an indirect infringer[37].

4.2 The questions asked by the Munich court to the ECJ

The Munich court considered it to be plausible that the violation of Sony's rights was not committed by Mr McFadden, but by another party. At the same time, the German court was also inclined to consider Tobias McFadden liable under the Störerhaftung doctrine. However, the court was not sure whether the exemption provided by article 12, Directive 2000/31 was or was not applicable to Mr McFadden; as if it was, he could not be considered liable at all.

In such a situation, the German court referred the case to the CJEU asking for an interpretation of some European Directives and asked ten different questions, that for the purposes of this article can be essentially traced back to two main issues:

1 Can a free WLAN operator be qualified as 'provider of information society services' and enjoy the liability limitations introduced by article 12, Directive 2000/31 applicable to a WLAN operator?

2 What measures should a provider adopt to avoid liability for third party's intellectual property rights infringement?

4.2.1 What is a provider of information society services?

The first question can be answered only by interpreting the definition of 'information society service' included in Directive 98/34 and recalled by Directive 2000/31. An information society service is meant as any service normally provided for remuneration, by electronic means and at the individual request of a recipient of services (art 1(2) Directive 98/34)[38]. Hence, services have to be considered as 'services normally provided for remuneration' in exactly the same vein as in article 57 TFUE.

In fact, recital 18 of Directive 2000/31 specifies that information society services must be an economic activity. However, this does not mean that the 'remuneration' has to come from clients or customers; it would be enough that the service is provided with the aim of advertising goods or services sold by the same service provider[39].

Hence, Mr McFadden's service can be considered as an 'information society service' and enjoy the liability exemptions provided by article 12, Directive 2000/31[40].

Upon the request of the referring court, the CJEU also clarified that article 12 of Directive 2000/31, on mere-conduit providers, refers to services that involve the transmission in a communication network of information. Such activity must be of mere technical and passive nature, as described by recital 42 of the same Directive. To enjoy the limitation of liability provided by article 12, a provider's activity should not go beyond this technical nature. The Directive requires no other conditions to allow a provider to enjoy the liability limitation[41].

4.2.2 What measures should a provider implement to avoid liability for infringement?

The most interesting point of the judgment, and probably the one that will probably have more effect onthe future of open wi-fi networks, is what kind of measure should a provider of open wi-fi adopt to avoid infringements and subsequent liability. This question entails another one: is a provider enjoying the liability exemptions of article 12 shielded only from damages or is it also shielded from injunctions?

The Munich court asked whether Directives 2001/29[42] and 2004/48[43] – that relate to copyright in the information society and to intellectual property rights enforcement – read in conjunction with article 12 of Directive 2000/31 preclude the grant of an injunction against an intermediary when it has already been ascertained that the only technical measures that the provider may adopt are in practice :

- to terminate the account,
- or to password-protect the access to the network,
- or to examine all communications passing through the network.

The CJEU held that different rights should be taken into account in deciding these issues. First, copyright deserves protection, as article 17.2 of the Charter of Fundamental Rights of the European Union states. At the same time, however, it is necessary to consider access provider's freedom to conduct a business (art 16 of the Charter), that could be compromised by the injunction requested, as well as users' freedom of information protected by article 11 of the Charter.

As the Court of Justice declared in the 2008 *Promusicae* case, when numerous rights are at stake, it is for the Member States' authorities to ensure a fair balance amongst these rights[44]. In addition, as stated in the *UPC Telekabel Wien* case, when it is the access provider that can determine which measure to adopt to achieve the result sought by the copyright holder, this measure should be a way to strike a fair balance[45].

4.2.3 Monitoring, termination, and password protection as possible measures and how they clash with fundamental rights

The Court of Justice did not consider any possible solution to the problem of copyright infringement by open wi-fi networks. The judges only analysed the three measures that according to the referring court can be adopted in the case in question, namely:

- the examination of all communications passing through the network. The CJUE stated that such a measure would be in contrast with article 15 of Directive 2000/31, that excludes the imposition on service providers of a general obligation to monitor:
- The termination of the account: this solution would cause serious impediment to the freedom to conduct a business, although in the case at issue this is only a secondary activity for Mr McFadden; hence it would not allow the striking of a fair balance amongst the various rights.
- The password protection of the internet connection: such measure could instead strike a fair balance, given that, although it would affect both freedom to conduct a business and users' freedom of information, it would limit both rights only marginally. In particular, it would not deeply affect the freedom of information of the recipient, as such a connection would be only one of the many ways to access the internet. However, as we will discuss in the part of this article on the implications of the decision, there could be two ways to interpret the position on the password: either password protection satisfies the balance of rights, or, on the contrary, password protection is acceptable if it satisfies the balance of rights, which it arguably does not.

Moreover in general, when a provider adopts an injunction, it must ensure that the measure prevents unauthorised access to the copyrighted material, or at least makes it very discouraging for internet users[46].

The Court of Justice therefore held that password protecting a connection can be a deterrent to copyright infringing activities, as long as users are required to identify themselves to obtain the password and do not act anonymously.

In conclusion, given that the other two measures do not allow the striking of a fair balance, the CJEU found that another measure should be adopted to ensure effective copyright protection and it is debatable whether password protection achieves the required balance of rights.

5. The possible impact of *McFadden* for community networks as providers

Many of the answers given by the CJEU deal with providers' liability and will not affect CNs and their development. However, at least two main issues should be analysed more thoroughly to understand what kind of consequences they might have on CNs.

The issues are those arising from the questions/answers numbers 1, 5, 9, 10.

5.1 Applicability of the liability limitation: how to distinguish ancillary and commercial activity in the absence of a payment

Question 1 concerned the applicability to Mr McFadden's network of the liability limitations introduced by Directive 2000/31 for providers. The court considered the Directive applicable to McFadden's offer of an internet connection. The same conclusion was also reached by Advocate General Szpunar[47]. The key point was that even though Mr McFadden offered the connection for free, such offer was made in the context of his main economic activity. It was a way to advertise his business, to make passers-by aware of the existence of the shop. Although it was a merely ancillary activity, this has to be considered as an information society service, because it is strictly related to another economic activity. Hence, it is considered to be 'made for remuneration', despite the fact that there is no direct remuneration from clients/users.

The implication for CNs of such an interpretation is that unless there is a form of remuneration, they would be outside the eCommerce Directive. Only in the case that a CNs offered other services, being paid in one way or another by users, could it be considered as a service provider and enjoy the corresponding limitations on liability for a third party's conduct[48].

At the same time, if one of the gateway nodes is run by a shop owner or by a company, the person owning the node would probably enjoy the limitations provided by Directive 2000/31. Indeed, in such instances, providing an internet connection would be an ancillary activity to the main economic one, exactly as in the case of Mr McFadden.

It is interesting to note that while the case was pending before the Court of Justice the German legislator amended the law on media and communications and extended the liability exemptions for access providers to providers that offer wi-fi connection[49].

5.2 Risks and drawbacks of injunctions requiring the application of password protection as identified by Advocate General Szpunar

Questions 5, 9, and 10, concerned the possibility of granting an injunction against a provider in order to protect copyright and requiring alternatively the implementation of one of the three measures which have been identified and analysed with regards to possible clashes with fundamental rights:

1 control the information passing through the connection;

2 terminate the connection;

3 put a password to protect the connection.

The Court of Justice found that only the measure of password-protecting the connection would allow to reach a fair balance to be reached amongst the different rights at stake: it would not restrict too much either the freedom to conduct a business or the freedom of information. The court also specified that such a measure would be appropriate provided that users are required to identify themselves in order to obtain the password.

Advocate General Szpunar had however reached a different solution[50]. Contrary to what the Court of Justice held, he considered that the obligation to make wi-fi secure would actually undermine the business model of those offering internet connection as an additional service to the main ones offered. Some people running these businesses might decide not to make investments to secure the network or just to understand the regulatory constraints. At the same time, consumers might stop using the service of a shop or restaurant because the use of the wi-fi would need identification and entering a password. The Advocate refers to the example of outlets for fast-foods[51].

The Advocate also observed that imposing password protection for the connection and to identify users would also entail retaining users' data. Only if users' personal data is stored, together with the IP numbers and the external ports through which the users have established the connection, would it be possible to trace the infringement back to that specific user.

These obligations are normally imposed only by commercial ISPs. Such obligations would, in the words of Advocate Szpunar, be disproportionate to people that offer an internet connection as an extra activity to their principal one. In addition, it might not be effective against copyright infringement, especially in the case of peer-to-peer traffic[52]. Advocate Szpunar finally claimed that putting a password on free wi-fi would mean a disadvantage for society as a whole, as free wi-fi offers great potential for innovation[53].

Reading McFadden again, the validity of password-protecting the internet connection to strike a fair balance between the rights at stake can be questioned: requiring users to identify themselves to obtain the password and not acting anonymously does not allow a fair balance of rights. Indeed, in the case of CNs, home access to the internet would be mostly achieved through that connection, unlike browsing from a shop. Examining the balance of rights from the side of the CN could reveal a similar imbalance.

In addition, it can be noted that there are numerous ways to implement password protection, some requiring no effort and no control from the provider, where the end user can enter any information without verification, with others requiring verification and data retention (as suggested by the CJEU), a huge burden on the CNs.

5.3 The applicability of the decision will depend of the scope of national definitions of intermediaries and economic operators

The effect on CNs might or might not be significant , depending on the applicable national legal framework.

What was declared by the Court of Justice concerns injunctions introduced by article 8.3 of Directive 2001/29 and article 11 of Directive 2004/48 that are addressed only to 'intermediaries'. As there is no definition of 'intermediary' in these Directives, the interpretation of the CJUE should be considered. The court has always dealt with 'intermediaries' that were economic operators, such as access providers[54]. The court stated in the Tommy Hilfiger decision that:

> *[f]or an economic operator to fall within the classification of 'intermediary' within the meaning of those provisions, it must be established that it provides a service capable of being used by one or more other persons in order to infringe one or more intellectual property rights, but it is not necessary that it maintain a specific relationship with that or those persons*[55].

CJEU's case law had also already clarified that for an economic operator to be classified as an 'intermediary' within the meaning of articles 8.3, Directive 2001/29 and 11, Directive 2004/48, 'it must be established that it provides a service capable of being used by one or more other persons in order to infringe one or more intellectual property rights, but it is not necessary that it maintain a specific relationship with that or those persons'[56]. In addition, there is no need for the intermediary to propose services other than the one used by the third party to infringe property rights: it is enough that the provider offers services capable of being used by a third party to commit the wrongdoing[57].

As the CJEU's decisions refer to 'economic operators', the McFadden judgment applies surely to those who provide an internet connection as a main activity, as well as to those providing it as an ancillary activity to their main economic one (exactly as Mr McFadden).

The question arises: would it be better for a CN – or for a gateway node - to qualify as a provider, and to be protected by the liability exemption and also its counterparts, including a possible

injunction? Or on the contrary, would CNs be better off, and would it be an option at all, if they do not qualify as intermediaries and economic operators?

The qualification is indeed uncertain due to the specific nature of their activities, first due to the non-profit but at the same time non-ancillary nature of their activity, and second due to the architectural settings of mesh networks, making each individual node an intermediary in the technical sense, but not in the economic sense, if the spirit in which the Directive was written was to target businesses rather than private individuals. This depends on national law.

5.4 Interpretation according to German, French and Italian laws

According to the McFadden judgment, if a CNs' gateway node is run by an economic operator, this node could be ordered to password protect its wi-fi connection. In such cases, the owner of the node will undergo both a positive and a negative effect derived from the McFadden decision. The positive effect is the liability exemption under article 12, Directive 2000/31. The negative effect is that the owner could be the target of an injunction.

However, when the node owner is a private individual, it is not certain whether injunctions ordering the individual to password-protect a connection could or not be granted against a private person. Since the CJEU's case law does not clarify such an issue, national legislation must be considered.

It would first be helpful to consider how the Directives were implemented and interpreted, to understand whether the notion of 'intermediary' has been construed to encompass also private persons. If this was the case, then private individuals could be subject to injunctions to stop third party's infringement.

Going back to the German case law above illustrated, there should be no doubts about the applicability of injunctions in the German context to private people. This interpretation is an analogy taken from the infringer of physical property and it does not depend on the EU Directive.

The same can be said with regard to the French law. In these cases, the gateway owner can enjoy the liability exemption, if he/she is a private person. However, he/she could be the target of injunctions. This would mean that there would be negative effects on the same subject.

In the case of Italy, for instance, a person can be held liable for a third party's conduct only when a specific provision exists. This means that a single individual cannot be held liable for someone else's conduct and cannot be the target of injunctions. The McFadden case does not affect this situation. Hence, CNs – and their gateway nodes – would be in a better position if they did not qualify as intermediaries under the meaning of the CJEU's decision.

Some of them are already ISPs (in France in particular). But for those wanting to promote open wi-fi, an option to circumvent the effect of a 'McFadden injunction imposing passwords' could be to create a separate entity (association) subscribing to a CN ISP and sharing wi-fi. If they receive an injunction, the operation could be transferred to a new legal entity (which would not be subject to the password restriction).

The interpretation given by the Court of Justice in McFadden could undermine CNs' development. With regard to the sustainability of the network, if the gateway user has to bear the damages caused by someone else and/or the costs of an injunction, this could clearly be a deterrent for the opening of the network to the internet. Indeed, ISPs were chosen as accountable subjects in the internet environment in part due to their 'deep-pockets' and their organisation as business companies. They do have the funding to face damages and injunctions and they also have the structure to analyse, prevent and bear the risks connected to their activity. This is clearly not the case for CNs.

5.5 The impact of *McFadden* on the structural design of community networks

A question worth asking is: what could CNs modify in their features in order to avoid the negative consequences of the Mc-Fadden judgment? In other words, can the decision affect the shaping and the sustainability of ecology of CNs as alternative, peer-to-peer, commons-based solution to provide a service? Which dimensions would be likely to be affected? Should CNs take pre-emptive measures to avoid negative consequences, or would a modification of the design be so disruptive that it would signify the end of open CNs?

We analyse selected features of CNs and their possible relation with the ECJ decision based on a previous categorisation of peer production platforms according to their level of (de)centralisation applied to five dimensions: ownership of means of production; technical architectural design; socio-economic organisation and governance of work patterns; rights and responsibility of the peer-produced resource; and value of the output[58].

The ownership of the means of production can be understood as the existence of a legal person with a status. The absence of a legal representative poses additional constraints to the difficulties which had been identified by the Advocate General.

The economic structure of the arrangement to benefit from wi-fi can be variable and is a matter of importance since the existence of a payment is mentioned in the decision as a criteria to determine whether the eCommerce Directive applies. Policies will oscillate from the absence of a fee to subscriptions at different levels for different categories of members, depending also on their involvement in the CN. It would be difficult to assess whether voluntary in-kind contributions (as manager of a node, as rooftop caretaker, as community officer reaching out to new audiences, as drafter of user documentation) would be assimilated to a professional role.

The governance decisions on possible changes to bring to selected features of a CN can be taken by a board, by nodes, or in the case of a decentralised organisation, be impossible as they should be implemented by all nodes which will not necessarily agree and cannot technically be forced to.

They include possible modifications to the other dimensions of the CN: the fee policy, the legal structuration, the technical design, or terms of use, when they exist, and whether CNs could or should amend their promises or exclusion of service. As for liability disclaimers for possible wrongdoings by users, would they be sufficient to relieve the other members from liability? Or, to draw a parallel with hotels, we wonder whether asking users to not commit copyright infringement before they sign up would be considered a sufficient measure.

Finally, the most crucial aspect of the decision likely to affect CNs

is the reflection on the implementation of the three measures identified: password instead of keeping the network open, registration of user information, and data retention obligation. CNs will have to evaluate the cost of implementing such measures, should they become compulsory to avoid liability. They may be too expensive or too difficult to implement, and compliance may signify the death of the CNs, if too many individual nodes choose to close, jeopardising the technical viability of the local network.

Probably, a recommendation could be to make or to maintain a network as distributed as possible, and even more than they currently are. Indeed, previous research on some CNs demonstrates that they might not be as decentralised as they would like to be[59]. In some cases, many nodes are actually owned by a single person, who also manages and keeps the network running. These are called 'critical nodes' and reflect a more general trend on the re-centralisation of the web. If a node opened to the internet is also a critical node for the functioning of the entire CN, the imposition of an injunction or a claim for damages against the owner might hamper not only the functioning of the node, but the functioning of the entire CN.

This means that not only should the technical structure of the CN be highly distributed, but also the ownership of the nodes should be distributed, in order to distribute the governance and the risks.

6. Conclusions

While community wireless networks structural design and features vary, the McFadden decision targeting open wi-fi could have implications for their future. In this article, after describing the specific nature of CNs in terms of architecture and liability, we presented the ECJ McFadden decision and the possible impact of it on CNs. If considered as providers, they could have to implement technical measures, such as password-protection, in order to avoid liability for infringement. The applicability of the liability limitation to activities which can be ancillary and non-commercial is not clear-cut, and requiring password protection could be disproportionate and threaten the sustainability of CNs. The applicability of the decision will also depend on the scope of national definitions of intermediaries and economic operators.

Since there is no harmonisation of tort law in Europe, the only relevant framework at the European level is human rights. This opens up a discussion on the structural tensions between Parliament and the courts in the field of human rights online, and on how these tensions affect the room for manoeuvre of those trying to shift the design of the internet and hence its politics. An empirical field is community networks, and it would be interesting to determine whether similar observations could be drawn from other fields, such as open source cryptography projects.

Federica Giovanella
University of Trento
federica.giovanella@unitn.it

Mélanie Dulong de Rosnay
CNRS-Sorbonne Institute for Communications Sciences
melanie.dulong@cnrs.fr

Acknowledgments

The research presented in this paper was conducted with funding provided by the EU Horizon 2020 project netCommons: Network Infrastructure as Commons, (grant agreement number: 688768, http://netcommons.eu/).

The authors would also like to thank for their useful comments on a draft of this paper Félix Tréguer and the participants of the Information Law and Policy Centre research *workshop* 'Restricted and Redacted: Where now for human rights and digital information control?', Institute of Advanced Legal Studies (IALS), London, 9 November 2016.

References

Christina Angelopoulos, 'CJEU AG suggests that free Wi-Fi providers may not be ordered to password protect their networks', (2016) Kluwer Copyright Blog, at: http://kluwercopyrightblog.com/2016/04/14/6540/

Roger Baig, Ramon Roca, Felix Freitag and Leandro Navarro, 'guifi.net, a crowdsourced network infrastructure held in common' (2015) *Computer Networks*, vol 90, pp 150–65.

Pablo Baistrocchi, 'Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce' (2002) Santa Clara Computer & High Tech LJ, vol 19, no n 1, 111-30.

Yochai Benkler, 2016. 'Degrees of Freedom, Dimensions of Power'. *Daedalus*, 145(1), 18–32. http://doi.org/10.1162/DAED_a_00362

Christoph Busch, 'Secondary Liability for Open Wireless Networks in Germany: Balancing Regulation and Innovation in the Digital Economy' (2015) ssrn.com, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728350

Stefano Crabu, Federica Giovanella, Leonardo Maccari, Paolo Magaudda, Hackivism, Infrastructures and Legal Frameworks in Community Networks: the Italian Case of Ninux.org' (2016) JoPP, Special Issue #9 'Alternative Internets', at: http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/ninux-org

Primavera De Filippi, Danièle Bourcier, '"Three-Strikes" Response to Copyright Infringement: The Case of HADOPI,' in F Musiani, DL Cogburn, L DeNardis, NS Levison (eds), *The Turn to Infrastructure in Internet Governance*(London, Palgrave-Macmillan, 2016) 125-52.

De Filippi, Primavera, and Félix Tréguer, 'Expanding the Internet Commons: The Subversive Potent of Wireless Community Networks' (2015) JoPP, Special Issue #6 'Disruption and the Law', at: http://peerproduction.net/issues/issue-6-disruption-and-the-law/peer-reviewed-articles/expanding-the-internet-commons-the-subversive-potential-of-wireless-community-networks/.

Melanie Dulong de Rosnay, 'Peer-to-peer as a Design Principle for Law: Distribute the Law,' (2015) JoPP, Special Issue #6 'Disruption and the Law', at: http://peerproduction.net/issues/issue-6-disruption-and-the-law/peer-reviewed-articles/peer-to-peer-as-a-design-principle-for-law-distribute-the-law/.

Mélanie Dulong de Rosnay, Francesca Musiani, 'Towards a (De) centralization-Based Typology of Peer Production,' (2016) *TripleC: communication, capitalism & critique*, vol. 14, no 1, 189-207, available at: http://www.triple-c.at/index.php/tripleC/article/view/728.

Christian Fuchs, 'Sustainability and community networks,' (2016) *Telematics and Informatics*, 34(2), 628–39. http://doi.org/10.1016/j.tele.2016.10.003.

Giorgio Giannone Codiglione, 'Indirizzo IP, Reti Wi-Fi e responsabilità per illeciti commessi da terzi,' (2016) Dir Informatica, vol 29, no 1, 107-43.

Federica Giovanella, 'Liability Issues in Wireless Community Networks,' (2015) JETL, vol 6, no 1, 49-68.

Robert VII Hale, 'Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet,' (2005) Santa Clara Computer & High Tech LJ, vol 21, no 3, 543-59.

Jordan S Hatcher, 'Mesh Networks: A Look at the Legal Future,' (2007) J of Internet Law, vol 11(1), 1-16, available at http://ssrn.com/abstract=814984.

Thomas Hören, Silviya Yankova, 'The liability of internet intermediaries – the German perspective,' (2012) IIC, 501-31.

Martin Husovec, 'Holey Cap! CJEU Drills (Yet) Another Hole in the E-Commerce Directive's Safe Harbors,' (2016) JIPLP (forthcoming), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843816.

Benjamin D Kern, 'Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law,' (2004) Santa Clara Computer & High Tech LJ, vol 21, no 1, 101-62.

Annette Kur A, 'Secondary Liability for Trademark Infringement on the Internet: The Situation in Germany and Throughout the EU,' (2014) Colum J L & Arts, 525-40.

Sylvia Kierkegaard, 'ECJ Rules on ISP Disclosure of Subscribers' Personal Data in Civil Copyright Cases – *Productores de Música de España (Promusicae) v Telefónica de España SAU* (Case C-275/06),' (2008) Computer Law & Security Report, vol 24, no 3, 269-74.

Michal Koščík, 'Privacy Issues In Online Service Users Details Disclosure In The Recent Case-Law. Analysis of Cases *YouTube v* Viacom and Promusicae v. Telefonica,' (2009) Masaryk University Journal of Law & Technology, vol 3, no, Koščík 259-66. https://journeb.muni.cz/mujlt/article/view/2539/2013

Rosa Julià-Barceló, 'On-line Intermediary Liability Issues: Comparing EU and US Legal Frameworks,' (2000) EIPR, vol 22, no 3, 105-19.

Rosa Julià-Barceló, Kamiel J Koelman, 'Intermediary Liability: Intermediary Liability in the E-Commerce Directive: so far so good, but it's not enough,' (2000) Computer Law & Security Review, vol 16, no 4, 231-39.

Daithí Mac Síthigh,. 'Law In The Last Mile: Sharing Internet Access Through Wifi', (2009) *SCRIPTed*, vol 6, no 2, 355-76.

DLA Piper, 'EU Study on the Legal Analysis of a Single Market for the Information Society, New Rules for a New Age?, Liability of Online Intermediaries,' (2009) at http://ec.europa.eu/digitalagenda/en/news/legal-analysis-single-market-information-society-smart-20070037

Leonardo Maccari, 'Decentralized, multi-hop networks: Are They really different from the Internet?,'(2014) Dagstuhl Seminar,16-21 November 2014, at: http://drops.dagstuhl.de/opus/volltexte/2015/4971/pdf/dagrep_v004_i011_p078_s14471.pdf.

Leonardo Maccari, Renato Lo Cigno, 'A Week in the Life of Three Large Wireless Community Networks,' (2015) Ad Hoc Networks, vol 24, pt B, 175-90.

Armin Medosch, *The Rise of the Network Commons* (2015) at http://www.thenextlayer.org/NetworkCommons

Romain Robert, Mark Manulis, Florence De Villenfagne, Damien Leroy, Julien Jost, Francois Koeune, Caroline Ker, Jean-Marc Dinant, Yves Poullet, Olivier Bonaventure and Jean-Jacques Quisquater, 'WiFi Roaming: Legal Implications and Security Constraints,' (2008) International Journal of Law and Information Technology, vol 16, no 3, 205-41.

Thibault Verbiest, Gerald Spindler, Giovanni Maria Riccio, Aurélie Van der Perre, (2007) 'Study on the Liability of Internet Intermediaries,' at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

Notes

1 C-484/14, *Tobias McFadden v Sony Music Entertainment Germany GmbH*; decision delivered on 15 September 2016.
2 Fuchs, 2016.
3 Baig et al, 2015.
4 Medosch, 2015.
5 Benkler, 2016.
6 http://www.picopeer.net/PPA-en.shtml.
7 https://guifi.net/en/FONNC.
8 Hatcher, 2007; Dulong de Rosnay, 2015; Giovanella, 2015.
9 Dulong de Rosnay, 2015.
10 Giovanella, 2015, 52-63.
11 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] Official Journal (OJ) L 178, 17.7.2000, 1–16. Since Directives are not immediately applicable within Member States but must first be implemented within each legal system, there may be discrepancies between Member States' regulation of ISP liability. Nevertheless, in the case of Dir 2000/31, Member States implemented almost verbatim the Directive's wording. Indeed, Italian implementation of Dir 2000/31 is simply a 'copy-paste' of the Directive's text (see *decreto legislativo* 9 April 2003, no 70, specifically arts 14–17). UK implementation (through the Electronic Commerce (EC Directive) Regulations 2002, SI 2013/2002) has almost the same wording as the Directive as well (see specifically sse 17–19). The German enactment is worded in a manner very similar to the original (cf Telemediengesetz vom 26 Februayr 2007 (BGBl I S 179), spec §§ 8-10).
12 Basically, providers are required not to interfere with users' conducts, see para 3.3.1. for access providers' requirements. For an in-depth analysis of ISPs' liability regime consider: Julià-Barceló and Koelman, 2000; Baistrocchi, 2002; Verbiest *et al*, 2007.
13 Kern, 2004; Hale, 2005; Mac Síthigh, 2006; Robert et al, 2008; Giannone Codiglione, 2013.
14 Giannone Codiglione, 2013, 123-35; Giovanella, 2015, 63.
15 Each European country has its own procedural rules, but, for instance, for what concerns intellectual property rights art 8 of Dir 2004/48 (of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, so called 'IPR Enforcement Directive') introduced a specific tool that had to be implemented in each Member State.
16 Reference is to the seminal case decided by the European Court of Justice *Productores de Música de España (Promusicae) v Telefónica de España SAU* (Case C-275/06), on which see: Kierkegaard, 2008; Koš ík, 2009.
17 Cf the model clause to be inserted in contracts ('Modèle de clause à insérer dans une charte informatique, contrat de bail, contrat de location', etc) at: https://

www.hadopi.fr/hadopi-vous/modele-de-charte-ou-clause-pour-les-professionnels

18 French Intellectual Property Code art L 336-3, as amended by art 11, Loi n 2009-669 of 12.06.2009, so called 'HADOPI law'. Cf De Filippi and Bourcier, 2016, 136-37.

19 Busch, 2015, 3; Hören, Yankova, 2012, 504; 510.

20 Hören, Yankova, 2012, 511-518; Kur, 2014, 532.

21 Kur, 2014, 533.

22 Busch, 2015, 3.

23 Busch, 2015, 2-4; Hören, Yankova, 2012, 502.

24 Bundesgerichthof, Judgment of 12.05.2010, Sommer unseres Lebens.

25 However, according to Hören, Yankova, 2012, 516, once the owner has secured the wi-fi, there is no duty to update the safeguards to the latest standards.

26 Busch, 2015, 4.

27 Landgericht Frankfurt am Main, judgment of 14 June 2013, MMR 2013, 605; Amtsgericht Hamburg, judgment of 9 January 2015, BeckRS 2015, 08939 , as reported in Busch, 2015, 5.

28 Busch, 2015, 5. Similar reasoning has been applied by the BGH also in cases where the owner of a wi-fi network had provided access to members of her family, who misused the network and infringed copyright. See again Busch, 2015, 5; Hören, Yankova, 2012, 516-517.

29 Landgericht Frankfurt am Main, judgment of 18 August 2010, MMR 2011, 401.

30 Landgericht Frankfurt am Main, judgment of 28 June 2013, GRUR-RR 2013, 507.

31 Amtsgericht Hamburg, judgment of 10 June 2014, CR 2014, 536.

32 Busch, 2015, 6. See the same paper for many other cases.

33 Landgericht Hamburg, decision of 25 November 2010, MMR 2011, 475.

34 Amtsgericht Charlottenburg, judgment of 17 December 2014, CR 2015, 192 as reported by Busch, 2015, 7.

35 C-484/14, *Tobias McFadden v Sony Music Entertainment Germany GmbH.*

36 Law of 9 September 1965 (BGBl I, p 1273), as amended by the Law of 1 October 2013 (BGBl I, p 3728).

37 Cf Opinion of the Advocate General Szpunar in the case C-484/14, *Tobias McFadden v Sony Music Entertainment Germany GmbH*, para 15-16.

38 Directive 98/34 was repealed by Dir 2015/1535, of which art 1, letter (b) introduces the same definition.

39 C-352/85, *Bond van Adverteerders v The Netherlands State*, April 26 1988, para 16. On this issue see DLA Piper, 2009, 10 ff; Giovanella, 2015, 60-61.

40 A similar conclusion was already reached by the CJEU in a case decided while McFadden was pending: C-291/13, *Sotiris Papasavvas vO Fileleftheros Dimosia Etairia Ltd et al*, 11 September 2014, paras 26-30.

41 According to the text of the CJEU's decision, the issue arose due to a particularity of the German language.

42 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, pp 10–19

43 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157, 30.4.2004, pp 45-86..

44 C275/06, January 29, 2008, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, para 68 e 70.

45 C-314/12, 27 March 27, 2014, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, paras 62 and 63.

46 C-314/12, 27 March 27, 2014, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, para 62.

47 Opinion of the Advocate General Szpunar in case C-484/14, *Tobias McFadden v Sony Music Entertainment Germany GmbH*, paras 34-56.

48 Clearly, in case a Member State, while implementing the Directive, did not include the distinction between commercial/non commercial/free of remuneration services, this interpretation would not apply. Cf Husovec, 2016, 3.

49 Zweites Gesetz zur Änderung des Telemediengesetzes, 21 July 2016, Bundesgesetzblatt, I 2016 Nr 36. The amendment added a new paragraph into s 8 of the Telemedia Act.

50 Opinion of the Advocate General Szpunar in Case C-484/14, *Tobias McFadden v Sony Music Entertainment Germany GmbH*, paras 134-50.

51 Opinion of the Advocate General Szpunar in Case C-484/14, *Tobias McFadden v Sony Music Entertainment Germany GmbH*, paras 138-39.

52 Opinion of the Advocate General Szpunar in Case C-484/14, *Tobias McFadden v Sony Music Entertainment Germany GmbH*, paras 145-46.

53 Opinion of the Advocate General Szpunar in Case C-484/14, *Tobias McFadden v Sony Music Entertainment Germany GmbH*, paras 148-49.

54 C-577/07, 19 February 2009, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH*, paras 43-46.

55 C-494/15,7 July 2016, *Tommy Hilfiger Licensing LLC at al v Delta Center as*, para 23, recalling C-314/12, 27 March 2014, *UPC Telekabel Wien GmbH v Constantin Film Verleinh GmbH and Wega Filmproduk-tionsgesellschaft mbH*, paras 33-36.

56 C-314/12, 27 March 2014, *Telekabel Wien GmbH v Constantin Film Verleih GmbH e Wega Filmproduktionsgesellschaft mbH*, paras, 32 and 35; see also C-494/15, 7 July 2016, *Tommy Hilfiger Licensing LLC, at al v Delta Center as*, para 23.

57 *Tommy Hilfiger Licensing LLC, at al v Delta Center as*, paras 24-25.

58 Dulong de Rosnay, Musiani, 2016, 194-96.

59 L Maccari, 2014; S Crabu, F Giovanella, , P Magaudda, 2016.