



Alternative rules for alternative networks? Tort law meets wireless community networks

by **Federica Giovannella**

Abstract

This paper analyses the existing rules on civil liability in order to test their applicability on wireless community networks (WCNs), with a focus on the European framework. In particular, the paper considers tort liability for three different actors: WCNs users, ISPs (in the case of shared Internet connection), and WCNs themselves; it describes the different situations to which civil liability should be applied in relation to the three mentioned actors. The analysis demonstrates that the structure of WCNs seems irreconcilable with the aims of current legal framework for tort law. The paper attempts to envision possible solutions through a multilayered approach based on social norms and contracts.

Contents

- [1. Introduction: Distributed architectures](#)
- [2. A closer look at wireless community networks](#)
- [3. Civil liability and WCNs](#)
- [4. Tort law failure?](#)
- [5. A possible solution via a multilayered approach](#)
- [6. Conclusions](#)

1. Introduction: Distributed architectures

Distributed architectures have recently attracted a lot of attention from both specialists and the general public. Their diffusion touches upon different spheres of online and off-line activities and brings law and lawmakers to face, yet again, the recurring problem of how to deal with a new technology.

Distributed architectures can assume different shapes. Generally speaking, they rely on autonomous computers, which are part of a network and share the resources of the system. Examples of distributed architectures include the BitTorrent file-sharing system, as well as the increasingly famous Bitcoin payment system; but many other examples exist [1].

These distributed systems rely on a peer-to-peer architecture, where there is no central server managing or coordinating the network; instead, all the machines are considered to be equally important ("peers") and function simultaneously as client and as servers. Peer-to-peer can be considered as a "class of applications that takes advantages of resources [...] available at the edge of the Internet" [2]. Indeed, the idea of a decentralized network was a drive in creating the Internet: a computer network without any central node would have been more resilient to possible attacks. However, the Internet then evolved in a different way, as today it mainly relies on a few operators and on a limited number of central nodes [3].

While the architectures analyzed in this paper are distributed at the level of hardware, peer-to-peer is especially famous for its implementation at the "application level": programs that rely on software which decentralize information and users' participation, but that run on the existing structure of a network with points of centralization, namely: the Internet [4]. Such applications have shaped law and the way courts apply it. A prominent example is Grokster and the "inducement of liability" doctrine [5].

Parallel to the development of decentralized peer-to-peer networks, another way exists, in which users implement a physically decentralized network through the decentralization of the hardware. Wireless community networks (WCNs), on which this paper mainly concentrates, fall into this category. In particular, the aim of this article is to analyze how the current framework for civil liability applies to

WCNs and to hypothesize a new approach to tort law issues in WCNs, which would permit rights enforcement while taking into account the specificity and the potential of these networks.

The [next section](#) describes the main features of wireless community networks. [Section 3](#) is devoted to the analysis of the different situations to which civil liability should be applicable according to current rules within the European context. The paper will then illustrate some possible solutions, taking into account the existing literature on the assessment of liability in WCNs and in decentralized architectures at large ([Section 4](#)). On the base of such literature, the paper also proposes a new solution, based on a multilayered approach attributing a central role to social norms and contract governing the relations among network users ([Section 5](#)). Lastly, the paper draws some conclusions ([Section 6](#)).

2. A closer look at wireless community networks

Community networks (CNs) vary in scope, coverage, aims and management; for the sake of clarity, I will consider the different networks as a single category for the purpose of this paper [[6](#)]. CNs, which in the majority of cases are wireless, are networks organized through a bottom-up approach, whereby people who identify themselves as a community create a self-managed and community-based network. These architectures allow interactions between users (for example via messaging or sharing of data), and can bring Internet connectivity to locations where it is unavailable. Indeed, a WCN can be a valid alternative to obtaining an Internet connection in those areas where Internet service providers (ISPs) do not offer their services, for example in remote regions where it would not be profitable [[7](#)].

Despite their potential, until now, WCNs have been studied almost exclusively by researchers in communication engineering and computer science (for instance: Flickenger, 2002; Akyildiz, *et al.*, 2005; Ishmael, *et al.*, 2008; Maccari and Lo Cigno, 2015) [[8](#)]. Social scientists have demonstrated an increasing attention over the last decade (Powell, 2006); legal scholars have been the last to approach the issue (De Filippi and Tréguer, 2015; Dulong de Rosnay, 2015).

A WCN comprises nodes that both generate data and route the traffic of other nodes. The structure of these networks, made of stand-alone devices, permits the connection of thousands of nodes. In some regions and cities WCNs are a mass phenomenon, for example in Athens and Barcelona [[9](#)]. When a node is connected to the Internet, the entire WCN's community can potentially surf the Internet; this is possible since data travels from one node to another and can reach the "connected node". Through that node, and with the consent of that node's owner, other users can access the Internet. This kind of node is known as a "gateway" (to the Internet).

As mentioned, WCNs are characterized by a bottom-up approach that translates into the absence of a hierarchical organization. The majority of these networks also lack a central administrative body with control or representative powers. However, the Barcelona-based network (Guifi.net) is an exception, since it is represented and supported by a foundation [[10](#)]. Nonetheless, it remains true that each user is responsible for her own node: the network is simply a spontaneous community-based structure [[11](#)].

WCNs are characterized by reliability and ease of implementation. First, WCNs are based on redundant communication paths, meaning that if data try to go through a given route, and a link fails, the network automatically redirects the data through other paths. Second, adding a new node is a simple 'plug and play' operation that, coupled with the low cost of wireless access points, makes WCNs an easy-to-implement technology [[12](#)].

Last but not least among WCNs' features is a high level of anonymity. Even though each node has an "Internet protocol" (IP) address, users choose their own IP address and can change it at any time. Furthermore, in contrast to what happens in the Internet environment, there are no databases in which these IP numbers are registered. Some networks keep track of the modification in IP addresses. This is the case, for instance, of the Italian network "Ninux.org", which includes in its Web site a prospect that each user can update with the modification occurred. This entails that the prospect cannot be considered highly reliable; in turn, this means that even in the case that the IP address is known, it would be almost impossible to identify the person who was using that number at a given moment.

3. Civil liability and WCNs

As previously mentioned, distributed architectures force the application of existing laws to face a number of challenges. Distribution implies the fragmentation of conducts, so that it becomes difficult, when not impossible, to define who committed a specific action. The object of the illicit action might be allocated to a high number of different users' machines, which makes it — not only technically but also legally — extremely problematic to define who contributed to the violation of a right (Dulong de Rosnay, 2015).

The issue becomes even more problematic considering that the IP addresses of the people taking part in these networks are usually undetectable or, at least, very difficult to match with the real identities. In addition, anonymization software or encryption techniques are very often implemented.

Most WCNs communities have not written norms regulating relations amongst users, nor have they imposed a central authority. WCNs usually rely on "manifestos" such as the "Picopeering Agreement" [[13](#)]. Others more structured WCNs, such as Guifi.net, implemented other regulatory tools, such as the "Compact for a Free, Open & Neutral Network" (FONN Compact) [[14](#)], a license binding both the network and the users [[15](#)].

At the base of these "soft regulatory tools" there is the idea that people joining the network are motivated by, and most importantly share, the common principles of community participation and knowledge diffusion.

Generally, if a user who is already part of the community infringes its rules, and the community no longer accepts her behavior, there are some technical ways to exclude her [16]. These latter characteristics seem to demonstrate that internal social norms, meant as informal standards and rules applied within a given group, are in place to govern internal relations amongst WCNs' members. A similar approach is also embedded in the FONN Compact, which includes a specific clause that allows for the cessation of the agreement with a participant to the network "in extreme cases" [17].

While different legal issues could arise from the diffusion and use of CNs, this paper concentrates only on tort law matters. This section, in particular, gives a brief excursus of the possible liability situations that can be envisaged.

Given the structure and functioning of WCNs, these situations include at least three different cases corresponding to three subjects: the final user, the Internet service provider, the network [18].

A user can be held liable for her own conduct but, at the same time, if routing another user's information, she might be considered jointly liable for the action of the other user.

According to the European legal framework [19], ordinary rules of civil liability of each member state would apply, such as article 2043 of the Italian civil code, § 823 I of the German *Bürgerliches Gesetzbuch* (*BGB*), or the general "tort of negligence" or other specific figures of tort law in the English system [20]. In the second situation, general clauses of civil liability will be applicable along with those providing for joint and several liability. For example, article 2055 of the Italian civil code states that "[w]hen the damage can be attributed to more than one person, all of them are jointly liable and obliged to compensate the damage". Other examples are § 830 I of the *BGB*, which considers two or more people liable for damage resulting from an unlawful act they committed jointly; and the English Civil Liability (Contribution) Act of 1978, whose section 1(1) provides that "any person liable in respect of any damage suffered by another person may recover contribution from any other person liable in respect of the same damage (whether jointly with him or otherwise)".

In both situations, in order to enforce the infringed right, the first step taken is the identification of the person behind the screen, *i.e.*, the owner of the node that originated the wrongful content. But this task may be very difficult to accomplish. As mentioned, IP addresses are self-chosen by users and there are no reliable databases where these data are registered or retained, as it happens for public IP numbers.

Therefore, the possibility of identifying the wrongdoer diminishes considerably, with the consequence that there is no legal protection for the victim. The problem persists in the case of a user routing someone else's illicit data; even in this instance no user can be identified and, consequently, considered liable.

These enforcement problems highlight the difficulties that a technological structure such as a WCN poses to the classical view of tort law. Acting directly against the final users would be the most straightforward solution. It would also be the correct one, given the general rule that each person is liable only for her own actions. However, from a technological point of view this solution seems impossible. As a consequence, other defendants could be considered by the subject who undergoes the damage. For instance, in case the wrongful action took place through the gateway, could the ISP be held liable for such behavior?

In this case, the national transposition of the 2000 Directive on Electronic Commerce would apply [21]. According to the Directive, ISPs can be held liable for users' actions only if specific requirements are met (Julià-Barceló and Koelman, 2000; Baistrocchi, 2002; Verbiest, *et al.*, 2007). In other words, if the ISP complies with the specific conduct required of it by the law, it will not be held liable for a third party's wrongful action. Articles 12 to 14 of the Directive subdivide ISPs' activities into three different categories: mere conduit, caching, and hosting. The three activities entail an increasing level of involvement by the intermediary; this implies, for example, that it is generally more difficult for a hosting ISP than for a mere conduit ISP to be exempt from liability in relation to a user's wrongful behavior. In addition, in order to prevent free speech "chilling effect", the Directive also provides that Member States cannot impose on ISPs a general obligation to monitor (art. 15).

Articles 13 and 14 of the Directive provide definitions of "caching" and "hosting" providers. The former implies "the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request". The latter involves "storage of information provided by a recipient of the service". Caching and hosting providers are held liable for the activity of storing information (albeit in different ways) upon the request of a user, and for not removing the information when required. Therefore, the Directive imposes liability on a caching or a hosting ISP irrespective of the source of the information; in other words, in the case of WCNs, it would not matter whether the information that must be removed comes from the user owning the node, or from another user within the WCN.

A partially different reasoning must be made for "mere-conduit" providers; article 12 of the Directive defines them as providers 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".

As these providers do not store information, but simply transmit it, they can be exposed to the action of third-party users (that is, users other than their customers) without the possibility of controlling the source of the information. At the same time, however, a binding contract generally exists between the ISP providing connection and its customer. Therefore, besides the cases in which the Directive's exemptions apply, a provider could limit its responsibility by means of specific contractual provisions,

expressly forbidding the customer to share the connection. Contractual provisions of this kind are already in place in various contracts [22]: in such circumstances, the customer/node-user that opens her node to other peers would thereby breach the contract. In addition to being liable for breach of contract, the customer could also be considered liable for the damages suffered by the provider as a consequence of the illicit conduct committed through the gateway (Kern, 2004; Hale, 2005; Mac Sithigh, 2009; Robert, *et al.*, 2008; Giannone Codiglione, 2013).

In the case that the illicit action is made through the gateway node, a narrow space for action could remain. The gateway node can be identified since it has a public IP address.

Again, national laws should be applied. Taking Italy as an example, the current framework for tort law would not allow liability on the gateway node for the activity of the user, since no general clauses exist on third-party liability [23].

Nonetheless, making the hypothesis that the gateway was liable, once obtained an IP number, the plaintiff should 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 [24]. This possibility has already been tested at both the national and the 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 favor of the latter [25]. This would be yet another obstacle to right enforcement.

A further possibility may exist: leaving a Wi-Fi connection open to strangers might amount to a negligent conduct, in case a specific duty of care on the gateway user exists. This would depend, yet again, on national laws. A few European countries seem to adopt such an interpretation. In the German case "Sommer unseres Lebens" the German Supreme Court (*Bundesgerichtshof*) held that a private person who failed to secure her connection through a password enabling third parties to infringe copyright can be considered as an indirect infringer [26]. In June 2016 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 [27].

Similar discussions have been ongoing in the U.K. with regard to the "Digital Economy Act" [28]. The highly debated "HADOPI" law, in France, already requires Internet subscribers to make their Wi-Fi connections secure by means of passwords, in order to avoid incurring in liability for third parties' infringement of copyrighted works [29].

As for Italy, while in the past professionals running a Wi-Fi connection business had to identify each and every person using the network, these duties do not exist any longer [30], and in 2013, the government adopted a decree that aimed at liberalizing Internet access through Wi-Fi technologies [31].

3.1. The "Mc Fadden" decision and its possible implications

At the European level, on 15 September 2016 the Court of Justice decided on a case involving Wi-Fi sharing [32]. The facts of the case are quite straightforward: Tobias Mc Fadden owns a shop where he also runs a wireless local area network (WLAN) that is open to the public and accessible free of charge. In September 2010, someone made a song available through that network, without the consent of the copyright holder, Sony Music. Sony sued Mc Fadden asking for compensation for indirect infringement for not having secured his WLAN, as decided in the mentioned German Supreme Court's decision "Sommer unseres Lebens". Mc Fadden brought an action to obtain a negative declaration and, as a response, Sony asked for an injunction against Mc Fadden to stop copyright infringement.

The Court of Munich made a request for preliminary ruling to the CJEU, asking numerous questions. The two issues that seem most important for CNs can be summarized as follows: can a network like Mc Fadden's be considered an "information society service" and therefore enjoy the liability limitation of art. 12, Dir. 2000/31? If the answer is positive, such an intermediary could also be the target of an injunction to stop copyright infringement, as art. 8 Dir. 2001/29 [33] and art. 3, Dir. 2004/48 provide. Thus, the second question was: what measure should an intermediary adopt in order to strike a fair balance among rights? In particular, the referring court listed three: termination of the account; examination of the information passing through it; password protection of the WLAN.

Advocate General Maciej Szpunar, in his opinion of March 16, stated that the definition of 'service normally provided for remuneration' that Dir. 2000/31 refers to should be interpreted in a broad sense, including connections offered within the economic context of a bigger business [34]. Therefore, these services can benefit from the exemptions provided by Dir. 2000/31 [35]. As for injunctions, the Advocate General immediately considered the termination of the account as absolutely disproportionate. Second, examination of the information would clash with art. 15, Dir. 2000/31 that prohibits the imposition on providers to monitor information. Finally, Advocate Szpunar specified that the imposition to make Wi-Fi network secure by means of a password does not strike an appropriate balance between the different rights at stake [36]: are freedom to conduct a business, freedom of information, right to protection of intellectual property. In fact, password protecting a network would negatively affect the two mentioned freedoms, without granting certain results against copyright infringement. The necessity to retain users' data in order to allow a subsequent enforcement was considered an excessive burden. Advocate General also maintained that such an imposition could have a negative impact on society as a whole, as open Wi-Fi is important for innovation [37].

The Court of Justice took a partially different stand. The Court agreed with Advocate Szpunar on the issues of the applicability of art 12, Dir. 2000/31 to cases such as Mc Fadden's. However, judges' reasoning was different on the question of password-protection. The Court considered password protecting the network as a valid measure to achieve balance between rights. According to the CJEU, this measure does not harm freedom to conduct a business, as it merely requires to adjust a small

technical feature. It would not damage the core of freedom of information, as users could still obtain the password. Furthermore, the Court also noted that such network would be only one of the possible connections. The European judges specified that password protection could also be an effective defense for intellectual property rights, provided that users reveal their identity to obtain the password so that they do not act anonymously [38].

3.2. What liability for WCNs?

The impact of this decision is yet to be seen, but a few conclusions can already be attempted. In case a CN's gateway node is owned by a business, this gateway could be considered as an intermediary and therefore enjoy liability limitation under Dir. 2000/31. However, it could also be the target of injunctions. Other situations, such as private individuals sharing their connection, are not influenced by this decision and their liability remains (exclusively) a matter of Member States laws. Obviously, the position taken by the CJEU does not seem to favor the situation of CNs.

A situation akin to that of CNs' gateway nodes has often occurred to users running an "exit node" of The Onion Router (Tor) network. It has sometimes happened, in case of criminal wrongdoing, that Tor users owning an exit node have been subject to police search and at times equipment was seized [39].

The question of whether merely running a gateway node is a behavior punishable by current laws may be set aside. However, from the point of view of social welfare, *i.e.*, with regard to the sustainability of the network, if the gateway user has to bear the damages caused by someone else, this could clearly be a deterrent for the opening of the network to the Internet.

Yet a final option shall be evaluated, namely a possible liability of the WCN for the wrongdoings committed inside the network. WCNs originate within communities as self-organized and spontaneous ways of communication. Contrary to what happens with ISPs, wireless community networks are not incorporated as companies. In many cases, they do not even have a clear structure, with a person in charge of the community or network who could be considered liable in case of wrongful actions. In such cases, WCNs do not have legal personality and it would not be possible to sue them. For these reasons, it is quite difficult to ascribe responsibility to a specific person or entity. A partially different case would be the one of those CNs that organize themselves as (or are run by) foundations or associations, as Guifi.net. Foundations and associations shall normally have a legal representative, in the form of a committee or a president, who could be held liable for the actions of the members. Even though this depends again on each country's system of laws, normally foundations and association (must) also have financial assets on which the whole activity is based [40].

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 clarifies that private networks connected to Guifi.net are excluded from the application of the FONN itself [41].

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 hypothetically be held liable for users' wrongful conducts, the FONN shifted risks to the same users accepting its conditions.

For the other cases, considering WCNs as communities of people, one might think of applying joint and several liability to all of those who participate in the network and in its activities [42], as if they had all contributed to the wrongdoing. However, since none of the users can be traced — except for the gateway user — the applicability of such a liability regime remains only hypothetical. The same can be said with reference to the applicability of the already investigated secondary-liability doctrines.



4. Tort law failure?

As emerges from the discussion above, ordinary rules for civil liability fail to fill the existing gap due to the inherent structure of WCNs. WCNs are expanding in many different countries on all continents. For this reason the need for specific regulation should be given consideration. These rules ought to take into account the strategic role that WCNs can play (and are already playing) in improving communications and sharing knowledge. In fact, WCNs can be a very useful tool to improve connections amongst people within a community and also between different communities. These networks can also provide Internet access where it would otherwise not exist, and facilitate participation in public debates, thereby enhancing free speech (also) through anonymity. All in all, WCNs can be a powerful tool for supporting democracy, especially in developing countries [43]. Potential regulation should balance the need to protect the rights of those susceptible to suffer damage with the need to protect the network and its potential in order to avoid unfair restrictions on freedom of expression.

Focusing on the two pillars of WCNs, namely users and the network itself, it might seem easy to hypothesize potential solutions. For instance, one could think about an identification system for community users or a specific liability regime for the networks [44].

However, such solutions would either be not feasible, or highly affecting WCNs and their positive features, or both. In fact, the introduction of a specific liability regime for the networks would need them to be organized as associations or foundations, so that a person or a committee in charge of the legal entity could be held liable. To compel communities to take this path would restrict the scope and reduce the benefits of WCNs.

In addition, if the network was the only subject liable for wrongful conducts, users could literally hide themselves behind their monitors, leaving the WCN to bear the entire responsibility for their illicit action.

Furthermore, WCNs do not normally have the financial capability to pay for possible damages, frustrating the same rationale of damages compensation. This makes the imposition of liability on WCNs even less desirable.

On the other hand, while the introduction of an identification system seems to be the only way to enforce the rights of third parties, it would have chilling effects on anonymity and, in turn, on free speech. Furthermore, this system would not be free from the enforcement problems already encountered in the Internet environment as to the identifiability of people "behind IP addresses" [45].

The outcome of this analysis is that the current state of WCNs does not allow reconciliation of the network's goals, strengths and spirit with the need to ensure effective protection of individuals' rights, both inside and outside the community. Therefore, different solutions should be investigated.



5. A possible solution via a multilayered approach

A first question to be considered with regard to possible solutions is whether the State would in fact be able to regulate these technologies, and whether this intervention is even desirable.

Community networks already regulate themselves to some extent. Users rely on manifestos, informal norms, and general principles to guide their actions. In some instances, users are asked to comply with a specific license. People entering a community adopt its rules and its underlying principles and ideas. Users not complying with these principles can technically be excluded from the network or the contract they agreed on can be ceased.

The existence of these informal norms can represent the starting point for the lawmaker. The law could seek to cement and intensify these informal norms, for example, requesting that each WCN adopts a code of conduct. The law should not dictate the content of the agreements; it should only encourage the adoption of such codes [46].

Users place high value on the network's functions, features and principles. Internal codes of conduct would be in line with such values. It would be possible to impose a monitoring system implemented by users. Through the creation of an internal centralized "authority", users could monitor their peers and signal the presence of suspect conduct. In this way, users select as peers only those who comply with the 'network order'. This could also be coupled with the implementation of internal filtering systems. Each gateway could function as a filter for the data that other users try to send to the Internet [47].

Putting in place such a system would clearly require a careful study of the social norms governing WCNs. This would enable a better understanding of these networks and of the underlying communities. The lawmaker could then understand if and how to intervene in this field, trying to encourage a virtuous circle of social norms in order to reduce illegal actions [48].

This approach would be the least invasive for the structure of WCNs. Its added value would mainly be linked to the self-enforceability connected to the pre-existing social norms. The effectiveness of such an approach would, however, have to be tested. Uncertainty remains: even if this approach was able to reduce the probability of wrongful conduct, the same problems highlighted above would nevertheless occur any time an illicit action is committed within or through a WCN.

A virtuous example is the one of Guifi.net and of its FONN Compact. The license is based on some fundamental principles, including: freedom to use the network, right to share knowledge of mechanisms and principles underlying the CN, the right to offer services and contents and the right to join the network with the duty to extend the same rights and freedom to anyone else [49]. As mentioned, the license also includes specific clauses that shield Guifi.net's liability for users' wrongful actions. In addition, the FONN also provides a specific dedicated means to resolve conflicts concerning the interpretation and application of the FONN itself. Such a conflict resolution system strengthens the FONN and allows its enforceability at an internal level and not only before national courts [50].

The adoption of a license such as the FONN would *de facto* oblige the community to organize as associations or foundations, in order to have legal personality [51]. It would nonetheless prove a useful tool to regulate liability issues for the CN, in order to preserve it without compromising its core, positive features.

All in all, the current state of WCN denotes the presence of a tort law failure or, better, of an enforcement failure. In case a person undergoes a damage coming "from the WCN", it might be impossible to obtain a compensation for this damage. The legal system presents a loophole, due to which the damage "remains on whom it was caused".

Should lawmakers intervene? Is a regulatory framework for these networks necessary and, most important, desirable? State intervention might be desirable in case the public interest in pursuing these wrongdoings is higher than the loss which WCNs would undergo due to the effects of such a regulation. In other words, lawmakers should weigh the importance of the survival and prosperity of WCNs against the importance of single subjects to obtain the enforcement of their rights.




6. Conclusions

The aim of this paper was to illustrate the liability issues arising from the diffusion of WCNs. Once again, technology, which develops more rapidly than law, requires the interpreter to question the feasibility of applying old rules to new problems. Three different situations of liability were considered: liability of the user for her own actions; liability of the ISP supplying the connection to a user who shares her connection with other users; and liability of the network for the actions of users.

Each of these three situations reveals the presence of gaps in current law. Applying old legal schemes to this new technology does not help in predicting the outcomes of possible lawsuits: where a right has been violated through a WCN, it remains unclear whether the enforcement of that right will be effective, or even possible.

This paper advances some ideas which could, nevertheless, have an adverse impact on the role of WCNs and, in particular, on people's freedom to communicate. The most viable solution seems to involve internal systems within the network, coupled with diffuse monitoring of users' conduct by other peers. In addition, the adoption of specific licenses by WCNs might be an efficient regulatory tool for the relationships among users and the relationships between users and "the network".

Whatever the solution to be adopted, the most important challenge will be balancing the protection of the network with the protection of individual rights. This is relevant given that WCNs are recognized as representing a very interesting tool for fostering democracy, especially in developing countries, where these networks are gradually spreading.

The future might, or might not, bring cases involving the liability of WCNs. Indeed, given that WCNs are not "market driven" technologies, they might avoid being the subject of external interests and liability cases [52]. But such cases arise, it will be necessary to understand how best to balance these apparently irreconcilable needs for protection. 

About the author

Federica Giovannella is post-doc fellow in Comparative Private Law at the Department of Information Engineering and Computer Science of the University of Trento.
E-mail: federica [dot] giovannella [at] unitn [dot] it

Acknowledgments

This work was supported partially by the University of Trento under the grant "Wireless Community Networks: A Novel Techno-Legal Approach" — Research Projects 2014, and partially by the European Commission, H2020-ICT-2015 Programme, Grant Number 688768 "netCommons" (Network Infrastructure as Commons).

Notes

1. For instance Wuala, a formerly distributed storage service; Diaspora, a distributed social network based on independently owned nodes; Twister is a free software peer-to-peer microblogging project.

2. See Shirky, 2000.

3. Elkin-Koren, 2006, pp. 20–21.

4. Among these there is the then famous "Napster" peer-to-peer file-sharing program and its successors, including "Grokster".

5. *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005). Reversed the Court of Appeal decision — *MGM Studios, Inc., v. Grokster, Ltd.*, 380 F.3d 1154 (9th Cir. 2004), upholding the District Court one — *MGM Studios, Inc., v. Grokster, Ltd.*, 259 F.Supp. 2d 1029 (C.D. Cal. 2003).

6. I am aware that such an approach might be misleading, but for the purpose of this paper, I prefer a general approach than an excessively specific one.

7. For an explanation of WCNs: Jain and Agrawal, 2003; Poor, 2003.

8. See also the EU FP7 projects "CONFINE" and "CLOMMUNITY": www.confine-project.eu, www.clommunity-project.eu, and the EU H2020 project "netCommons" www.netcommons.eu, all accessed 23 March 2016.

9. See <http://awmn.net> and <http://quifi.net>. See also, for a list of WCNs throughout the world: https://en.wikipedia.org/wiki/List_of_wireless_community_networks_by_region, all accessed 23 March 2016.

10. <http://fundacio.quifi.net/index.php/Foundation>, accessed 23 March 2016.

11. Another feature of WCNs is that many software packages are released and used under open source licenses, applying the way of thinking and entailing the positive effects of this approach. In fact, there seems to be a crossover of open source movement and community networks. See also the Compact for a Free, Open & Neutral Network: <https://quifi.net/en/FONNC>, accessed 23 March 2016.

12. IC2 Institute, Austin's Wireless Future, January 2004, 33
<http://repositories.lib.utexas.edu/handle/2152/14550>, accessed 23 March 2016.
13. <http://www.picopeer.net/PPA-en.shtml>, accessed 23 March 2016.
14. <https://quifi.net/en/FONNC>, accessed 23 March 2016.
15. See "II About this document (FONN)" of the FONN Compact, *cit.*
16. For example, since each node is based on a small antenna that covers a given space, moving the antenna to point in another direction means cutting off some connected nodes, namely the nodes of those who are not accepted by the community. These behaviors recall the functioning of peer-to-peer technologies for file sharing that scholars consider to be governed by social norms. See the contributions of Strahilevitz, 2003; Schultz, 2006.
17. See "X About Conflict Resolution and Jurisdiction", n. 3, of the FONN Compact, *cit.*
18. Giovannella, 2015, pp. 52–63.
19. The main focus of attention will be the EU legislation on electronic communications, although occasional reference will be made to the Italian legal system. Italy represents a good testing case since Italian legislation on electronic communication derives, for the greatest part, from EU law and WCNs are now spreading in the country, in particular Ninux.org: <http://www.ninux.org>, accessed 23 March 2016.
20. In a similar vein see art 1:101 of the Principles of European Tort Law (PETL) and art 1:101 of Chapter VI, Book VI, of the Draft Common Frame of Reference.
21. 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). U.K. implementation (through the Electronic Commerce (EC Directive) Regulations 2002, no 2013/2002) has almost the same wording as the Directive as well (see specifically secs 17–19). The German enactment is worded in a manner very similar to the original (*cf.*, *Telemediengesetz* vom 26. Februar 2007 (BGBl. I S. 179), spec. §§ 8–10).
22. See, for example, the terms and conditions of the UK provider Plusnet, which states: "You may only use the service for your own personal use and enjoyment": clause no 15 of "Plusnet Residential Standard Terms", available at: <http://www.plus.net/info2/legal/index.html>, accessed 23 March 2016. See also Telecom Italia, "General contractual clauses" for ADSL supply: clause n. 7 provides that the access to the Internet through the ADSL cannot be granted to other users in a way that allow the latter to use the services linked to the Internet access (terms available at https://img.tim.it/sdr/documenti/assistenza/fisso/Condizioni_Gen_Contratto_Alice_0.pdf, accessed 23 March 2016). The Electronic Frontiers Foundation provides a list of 'wireless friendly' ISPs in the U.S. so as to foster the diffusion of WCNs: <https://www EFF.org/pages/wireless-friendly-isps>, accessed 23 March 2016.
23. Giannone Codiglione, 2013, pp. 123–135.
24. 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 was then implemented in each member state.
25. 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; Košík, 2009.
26. *Bundesgerichtshof*, Decision of 12.05.2010 — I ZR 121/08, *Sommer unseres Lebens*.
27. *Zweites Gesetz zur Änderung des Telemediengesetzes*, 21 July 2016, *Bundesgesetzblatt*, I. 2016 Nr. 36. The amendment added a new paragraph into Section 8 of the Telemedia Act.
28. Consider the public consultation promoted by Ofcom (Independent regulator and competition authority for the U.K. communications industries), at: <http://stakeholders.ofcom.org.uk/consultations/infringement-implementation/?a=0>, accessed 23 March 2016.
29. 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". De Filippi and Bourcier, 2016, pp. 136–137.
30. These duties had been imposed by *decreto legge* d.l. 27 July 2005, n. 144, which had temporary effects and was not prorogated after the end of 2011.
31. *Decreto legge* 21 June 2013, n. 69. The same decree also clarified that when supplying an Internet connection is not the main activity of the provider many administrative requirements do not apply; *cf.*, for a specific analysis with regard to WCNs: Giovannella, 2015, pp. 960–964.
32. CJEU, C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, decided on 15 September 2016.

- [33.](#) 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.
- [34.](#) Opinion Advocate General Szpunar, C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, 16 March 2016, par. 34–50.
- [35.](#) Opinion Advocate General Szpunar, *cit.*, spec. par. 57.
- [36.](#) Opinion Advocate General Szpunar, *cit.*, par. 147. The necessity that a fair balance is struck between different rights at stake can be found in C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, *cit.*
- [37.](#) Opinion Advocate General Szpunar, *cit.*, par. 148–149.
- [38.](#) CJEU, C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, *cit.*, par. 94–96.
- [39.](#) See P. Howell O’Neill, “The real problem with Tor’s security,” *Daily Dot* (12 July 2015), at: <http://kernelmag.dailydot.com/issue-sections/features-issue-sections/13606/tor-arrest-history/>, accessed 9 September 2016, as well as personal cases described in the TOR Web site: <https://blog.torproject.org/blog/five-years-exit-node-operator>.
- [40.](#) Consider, for instance, the Italian statute regulating the creation of associations with legal personality that requires that associations to have an ‘adequate assets’ for the goals they aim at (*Decreto del Presidente della Repubblica*, 10 February 2000, n. 361, art. 1, comma 4).
- [41.](#) “VII About Security and Responsibility” of the FONN Compact, *cit.*
- [42.](#) In addition to the national laws cited above, an interesting approach could be that of art 3:105 PETL on “Uncertain partial causation”. The articles states: “In the case of multiple activities, when it is certain that none of them has caused the entire damage or any determinable part thereof, those that are likely to have [minimally] contributed to the damage are presumed to have caused equal shares thereof”.
- [43.](#) Cf., OECD, “Development of wireless local area networks in OECD countries,” *OECD digital economy papers*, No. 71, 2003, OECD Publishing, at: <http://dx.doi.org/10.1787/233145088433> accessed 23 March 2016.
- [44.](#) Giovannella, 2015, pp. 63–67.
- [45.](#) 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; Koščik, 2009.
- [46.](#) An example of this kind is European Directive 2000/31 art. 16 that requires Member States to take part in the drafting of codes of conduct and encourage their adoption, “to contribute to the proper implementation of Articles 5 to 15”, among which there are providers’ liability provisions. Stakeholders did in fact create codes of conduct that introduced “notice-and-take-down” regimes to improve both the protection of right and provider’s position towards liability issues. See for instance the “Memorandum of Understanding” signed in Brussels in 2011: http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf.
- [47.](#) Hatcher, 2007, p. 13.
- [48.](#) For an explanation of how law can influence social norms: Ellickson, 1991; McAdams, 1997; Ellickson, 2001; Posner, 2007.
- [49.](#) See “I General Principles and Summary” of the FONN Compact, *cit.*
- [50.](#) See “X About Conflict Resolution and Jurisdiction” of the FONN Compact, *cit.*
- [51.](#) The agreement of a high number of individuals to a license such as the FONN might lead — in some countries — to the creation of a “*de facto*” association or a similar entity.
- [52.](#) Contrary to what happens to peer-to-peer technologies sharing copyrighted contents. Elkin-Koren, 2006, p. 62.

References

- Ian F. Akyildiz, Xudong Wang and Weilin Wang, 2005. “Wireless mesh networks: A survey,” *Computer Networks*, volume 47, number 4, pp. 445–487.
doi: <http://dx.doi.org/10.1016/j.comnet.2004.12.001>, accessed 10 November 2016.
- Pablo Baistrocchi, 2002. “Liability of intermediary service providers in the EU Directive on Electronic Commerce,” *Santa Clara Computer & High Technology Law Journal*, volume 19, number 1, pp. 111–130, and at <http://digitalcommons.law.scu.edu/chtj/vol19/iss1/3>, accessed 10 November 2016.
- Primavera De Filippi and Danièle Bourcier, 2016. “‘Three-strikes’ response to copyright infringement: The case of HADOPI,” In: Francesca Musiani, Derrick L. Cogburn, Laura DeNardis and Nanette S. Levinson (editors). *The turn to infrastructure in Internet governance*. London: Palgrave-Macmillan, pp. 125–152.

- Primavera De Filippi and Félix Tréguer, 2015. "Expanding the Internet commons: The subversive potential of wireless community networks," *Journal of Peer Production*, number 6, 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/>, accessed 10 November 2016.
- Melanie Dulong de Rosnay, 2015. "Peer-to-peer as a design principle for law: Distribute the law," *Journal of Peer Production*, number 6, 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/>, accessed 10 November 2016.
- Niva Elkin-Koren, 2006. "Making technology visible: Liability of Internet service providers for peer-to-peer traffic," *New York University Journal of Legislation and Public Policy*, volume 9, pp. 15–76.
- Robert C. Ellickson, 2001. "The evolution of social norms: A perspective from the legal academy," In: Michael Hechter and Karl-Dieter Opp (editors), *Social norms*. New York: Russell Sage Foundation, pp. 35–75.
- Robert C. Ellickson, 1991. *Order without law: How neighbors settle disputes*. Cambridge, Mass.: Harvard University Press.
- Rob Flickenger, 2002. *Building wireless community networks*. Sebastopol, Calif.: O'Reilly.
- Giorgio Giannone Codiglione, 2013. "Indirizzo IP, Reti Wi-Fi e responsabilità per illeciti commessi da terzi," *Il diritto dell'informazione e dell'informatica*, volume 29, number 1, pp. 107–143.
- Federica Giovanella, 2015. "Liability issues in wireless community networks," *Journal of European Tort Law*, volume 6, number 1, pp. 49–68.
doi: <http://dx.doi.org/10.1515/jetl-2015-0002>, accessed 10 November 2016.
- Robert V. II Hale, 2005. "Wi-Fi liability: Potential legal risks in accessing and operating wireless Internet," *Santa Clara High Technology Law Journal*, volume 21, number 3, pp. 543–559, and at <http://digitalcommons.law.scu.edu/chtlj/vol21/iss3/2>, accessed 10 November 2016.
- Jordan Hatcher, 2007. "Mesh networking: A look at the legal future," *Journal of Internet Law*, volume 11, number 5; version at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=814984, accessed 10 November 2016.
- Jonathan Ishmael, Sara Bury, Dimitrios Pezaros and Nicolas Race, 2008. "Deploying rural community wireless mesh networks," *IEEE Internet Computing*, volume 12, number 4, pp. 22–29.
doi: <http://dx.doi.org/10.1109/MIC.2008.76>, accessed 10 November 2016.
- Saurabh Jain and Dharma P. Agrawal, 2003. "Wireless community networks," *Computer*, volume 36, number 8, pp. 90–92.
doi: <http://dx.doi.org/10.1109/MC.2003.1220588>, accessed 10 November 2016.
- Rosa Julià-Barceló and Kamiel J. Koelman, 2000. "Intermediary liability: Intermediary liability in the e-commerce firefictive: So far so good, but it's not enough," *Computer Law & Security Review*, volume 16, number 4, pp. 231–239.
doi: [http://dx.doi.org/10.1016/S0267-3649\(00\)89129-3](http://dx.doi.org/10.1016/S0267-3649(00)89129-3), accessed 10 November 2016.
- Benjamin D. Kern, 2004. "Whacking, joyriding and war-driving: Roaming use of Wi-Fi and the law," *Santa Clara High Technology Law Journal*, volume 21, number 1, pp. 101–162, and at <http://digitalcommons.law.scu.edu/chtlj/vol21/iss1/3>, accessed 10 November 2016.
- Sylvia Kierkegaard, 2008. "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)," *Computer Law & Security Report*, volume 24, number 3, pp. 269–274.
doi: <http://dx.doi.org/10.1016/j.clsr.2008.03.004>, accessed 10 November 2016.
- Michal Koščík, 2009. "Privacy issues in online service users details disclosure in the recent case-law. Analysis of cases *YouTube v. Viacom* and *Promusicae vs. Telefonica*," *Masaryk University Journal of Law and Technology*, volume 3, number 2, pp. 259–265, and at <https://journals.muni.cz/mujlt/article/view/2539/2103>, accessed 10 November 2016.
- Daithí Mac Síthigh, 2009. "Law in the last mile: Sharing Internet access through WiFi," *SCRIPTed*, volume 6, number 2, pp. 355–376, and at https://script-ed.org/wp-content/uploads/2016/07/6-2-Mac_S%C3%ADthigh.pdf, accessed 10 November 2016.
- Leonardo Maccari and Renato Lo Cigno, 2015. "A week in the life of three large wireless community networks," *Ad Hoc Networks*, volume 24, part B, pp. 175–190.
doi: <http://dx.doi.org/10.1016/j.adhoc.2014.07.016>, accessed 10 November 2016.
- Richard H. McAdams, 1997. "The origin, development, and regulation of norms," *Michigan Law Review*, volume 96, pp. 338–433.
- Robert Poor, 2003. "Wireless mesh networks," *Sensors Online* (1 February), at <http://www.sensorsmag.com/networking-communications/standards-protocols/wireless-mesh-networks-968>, accessed 23 March 2016.
- Eric A. Posner (editor), 2007. *Social norms, nonlegal sanctions, and the law*. Cheltenham: Edward Elgar.

Alison Powell, 2006. "'Last mile' or local innovation? Canadian perspectives on community wireless networking as civic participation," *Canadian Research Alliance for Community Innovation and Networking (CRACIN), Working Paper*, number 18, at: <https://tspace.library.utoronto.ca/handle/1807/32137>, accessed 23 March 2016.

Romain Robert, Mark Manulis, Florence De Villenfagne, Damien Leroy, Julien Jost, Francois Koeune, Caroline Ker, Jean-Marc Dinant, Yves Pouillet, Olivier Bonaventure and Jean-Jacques Quisquater, 2008. "WiFi roaming: Legal implications and security constraints," *International Journal of Law and Information Technology*, volume 16, number 3, pp. 205–241.
doi: <https://doi.org/10.1093/ijlit/ean016>, accessed 23 March 2016.

Mark F. Schultz, 2006. "Copynorms: Copyright and social norms," In: Peter K. Yu (editor). *Intellectual property and information wealth*. Volume 1: *Copyright and related rights*. Westport, Conn.: Praeger, pp. 201–235.

Clay Shirky, 2000. "What is P2P ... and what isn't?" (24 November), at <http://courses.ischool.berkeley.edu/i290-1/f00/10-Ebooks/on-nov-29-2000.pdf>, accessed 23 March 2016.

Lior Strahilevitz, 2003. "Charismatic code, social norms, and the emergence of cooperation on the file-sharing networks," *Virginia Law Review*, volume 89, number 3, pp. 505–595.

Thibault Verbiest, Gerald Spindler, Giovanni Maria Riccio and 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, accessed 23 March 2016.

Editorial history

Received 6 November 2016; accepted 10 November 2016.



This paper is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Alternative rules for alternative networks? Tort law meets wireless community networks
by Federica Giovanella.

First Monday, Volume 21, Number 12 - 5 December 2016

<http://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/7119/5660>

doi: <http://dx.doi.org/10.5210/fm.v21i12.7119>