A Transdisciplinary Gaze on Wireless Community Networks

Stefano Crabu
University of Padova

Federica Giovanella
University of Trento

Leonardo Maccari
University of Trento

Paolo Magaudda
University of Padova

Abstract: This conversation aims at offering a transdisciplinary gaze on the phenomenon of wireless community networks: an emerging typology of local wireless infrastructures, which is built by activists as political and technological statement to face the hierarchical governance of the Internet and the issues of surveillance and control over digital networks. By a transdicliplinary gaze – emerging from the dialogue between science and technology studies (STS), legal studies, and computer science – this conversation focuses on the multi-modal ways and perspectives that can be adopted to study CNs; it also offers a reflection on challenges and opportunities arising from trasndisciplinary scientific work. In the field of STS, a growing body of literature has addressed CNs as an emblematic case study to analyse the engagement of activists and lay people in the emergence of socio-technical infrastructures and technologies. From a computer science perspective, community networks represent a challenge to develop new routing protocols, and standards to technically implement a bottom-up-approach in the building and management of innovative network architectures. Finally, from the point of view of legal studies, CNs offer the case of a still largely unregulated emerging technology, offering a novel field to test existing laws, especially under the point of view of the possible allocation of civil liability.

Keywords: wireless community networks; transdisciplinarity; media infrastructures; sustainable network growth; distributed architectures regulations.

Corresponding author: Stefano Crabu, CIGA & Pa.S.T.I.S, Dep. FISPPA, University of Padova, Via Cesarotti, 10-12, 35200, Padova, Italy – Email: stefano.crabu@unipd.it.

Wireless Community Networks, "Inverse Infrastructures" and the Challenges of an "Interdisciplinary Assemblage"

Stefano Crabu and Paolo Magaudda

1. Wireless Community Networks from an STS perspective

Wireless community networks (CNs) represent a multi-dimensional phenomenon that in recent years has multiplied in several parts of the world including both the US and the EU due to the lowering of the costs of wireless devices and tools. CNs are grassroots network infrastructures based on a so-called "mesh" or "distributed" architecture (Flickenger 2002) and which are built and self-managed by groups or "communities" of people, including a wide range of profiles such as hackers and geeks, engineering students, young political activists and citizens. In many CN experiences, groups gather at the local level to build wireless networks from scratch. These are independent of the global Internet network, and their construction involves an activity that is at the same time technical, social and political, such as the set-up of hardware and software protocols, the physical installation of antennas on roofs (usually upon activists' homes), organizational work aimed at coordinating the group's activities, as well as a social and political effort to enrol new activists and find local support in order to expand the network. CNs require heterogeneous work in which material and technical practices need be constantly aligned and held together with symbolic, political and organizational activities. All this considered, CNs represents an exemplary environment which offers the opportunity to investigate at the local level the processes of heterogeneous "infrastructuring" (Star and Ruhleder, 1996; Star and Bowker 2002) in the domain of digital media technologies (Parks and Starosielski 2015).

The cultural origins of CNs, as counter-networks alternative to the global Internet infrastructure, can be traced back to the very origins of the Internet and to one of the first grassroots networks: the well-known "Memory Project" established in Berkeley in 1973 (see Levy 1984). In the '90s, several alternative (non-wireless) network projects were established in many cities, as in the case of the Seattle Community Network Project (Schuler 1994). These highlighted how, at least in the US, community networks based on users' maintenance were at that time already a relevant phenomenon, in some case also framed within municipal and institutional activities (Carrol and Rosson 2003). Since the early 2000s, the diffusion of low-budget wireless technology allowed these projects to shift from an emphasis on the "local community", to the possibility of establishing a fully autonomous infrastructure, potentially disconnected from the ordinary cables and phone-lines of the global internet and, in so doing, envi-

sioning an emergent way to offer a political alternative to the market- and corporation-driven Internet global network (De Filippi and Treguer 2015).

Several CNs were developed in Europe in the 2000s by adopting such a political framework, as in the case of the CNs Freifunk in Germany, Wlan Slovenija in Slovenia, Ninux.org in Italy and Guifi.net in Spain. This last one, started in the region of Catalunia in 2004, is currently the largest CN in Europe, being used by more 45,000 users, who are also attracted by the possibility to obtaining Internet access independently of the commercial ISPs. Other networks such as Freifunk, Wlan Slovenia and Ninux.org did not develop primarily as competitors of traditional commercial ISPs, but originated mainly from political activism. Consequently, they focussed primarily on the importance of building decentralized and autonomous networks. In these last cases, while the initial drive was for political and ideological reasons, in their development these communities needed to offer to possible new users suitable services in order to expand away from the narrow niche of media activists and experts (De Filippi and Treuger 2015, 6). Especially after the Snowden scandal in 2012 and the mainstream visibility gained by Anonymous's cyber-political actions, public concerns about internet privacy and corporate surveillance increased, turning WCN into a strategic technological intrument in political agenda of countercultural and social movements (Milan 2013).

Being built and maintained by the same users, CNs clearly represent novel emerging places for socio-technical innovation. It is prevalently in this vein that, in these last few years, these phenomena have attracted the interest of several STS scholars, who have identified these phenomena as being cases for the study of the shaping of new models of innovation, and to unfold tensions and contradictions within these emerging "technologically dense environment" (Bruni et al. 2013). Of course CNs represent a relevant case of bottom-up processes of innovation, where the social and technical participation of the end-users (Oudshoorn and Pinch 2003) represent a crucial peculiarity. The growing relevance of these models of "bottom-up" innovation, established by activists and end-users outside the work of institutions or industries, also represent a way in which democratic participation can become a crucial driving force in the processes of construction of science and technology (Jasanoff 2005). CNs are, in fact, a paradigmatic case which recognizes the active role of the user community in the construction of infrastructure, software and services from a collective work, most often disconnected from research centres or public institutions.

In this regard, a study by Van Oost, Verhaegh and Oudshoorn (2009), based on qualitative interviews with participants in the wireless community network of the city of Leiden in the Netherlands, has highlighted the role of users in terms of the dynamics of innovation of these networks, both in the design phase and during the work of maintaining and upgrading the infrastructure (see also Verhaegh and van Oost 2012). The model

of innovation resulting from this CN project has been defined in terms of "innovation community". This concept has been used by authors to identify the process through which an innovation emerges from the collaborative work carried out by a group of people, who are usually considered simply as the end-users of these same technologies.

The ability of grassroots CNs to generate alternative patterns of innovation has also been highlighted in research carried out by Söderberg (2011) into the Czech CN. In fact, the collective work deployed in developing this Czech network has led the participants to create a new hardware device, able to send data through a beam of red light. The research by Söderberg reconstructed the collective work and negotiation through which this new hardware has been developed, highlighting how its design incorporated and reflected a particular philosophy shared among this community, and how it is related with the use of technology. This philosophy was mainly based on the idea that people with few technical skills have to be able to assemble the tools needed to run such a network.

2. Ninux.org and the "Infrastructural Inversion" of an "Inverse Infrastructure"

In Italy, the most relevant example of CNs is the project Ninux.org, that was originally started in Rome in 2001, but in the last few years has spread to other cities such as Florence, Pisa and Bologna. Although independent from each other, all the networks in these different cities are part of the same wider national platform, which is a common framework for all participants. Groups of activists directly involved in the project share a common vision on the role of CNs in society, and on the strategies and goals that these networks should adopt. This common view has been formulated in a "Manifesto" available on the project's website (http://wiki.ninux.org/Manifesto). Major features highlighted in this document include the adoption of a decentralised and mesh architecture; the role played by CNs as democratizing tools and as resources to fight digital divide; their relevance within the current debate on the freedom of expression in the digital society, and also a wider criticism of the hierarchical governance of the Internet. These several instances reflect a whole set of beliefs, motivations and political drives that sustain the discourses and practices of the Italian CN.

In recent years, both this ensemble of motivations, and the citizens' participation in the Ninux.org project have been strengthened following the relevance and visibility that the "Snowden affair" achieved in terms of the public debate about freedom and surveillance in a "connected society". Snowden's revelations about secret programs of mass surveillance of digital communications between the United States and the European Union have brought to the centre of public discussion the complex relation-

ship between national security policies and citizens' right to privacy, especially in relation to the growing pervasiveness of the Internet in daily life. Following these revelations, in the public perception the Internet has increasingly become a controversial digital space deeply interlaced with government strategies and political power struggles, and at times risky and unsafe when it comes to privacy. In this sense, the Snowden affair triggered the opening of the "black box" of the Internet, highlighting the way in which the majority of the network services (such as e-mail, social networks and clouds) are managed centrally by a few operators who not only monitor all data exchanged by users, but also allow governments – both democratic (Clement 2014) and authoritarian (Wilson 2015) – to control citizens' behaviours. This ensemble of issues has pushed a growing number of people to engage in the construction of alternative infrastructures, and is the basis for growing participation in the Ninux.org wireless network.

As previously pointed out, the increasing relevance of these projects has attracted a great deal of attention from STS scholars, who more generally have also focussed on the concept of "inverse infrastructures" (Egyedi and Mehos 2012) to theoretically capture the emerging typology of infrastructures that are not owned and controlled by government or large private firms. Conceptually speaking, these wireless infrastructures are defined as being "inverse", because they feature peculiar modalities of emergence and development, which are opposed to those that characterize more traditional and institutional kinds of networks (such as energy networks and railways), for instance those described by Hughes (1983) in terms of "large-technical systems". Indeed, via the concept of "inverse infrastructure", it is possible to address the process through which these networks are developed from the ground roots, independently and outside of the control regimes of institutions and governments.

Overall, inverse infrastructures, and in particular the CNs rooted in a radical critique of contemporary governance of the Internet, bring to the attention of STS a relevant issue pertaining to the shape of new configurations of power relationships among citizens and governments, and also regarding the asymmetries in distribution in respect to the growing pervasiveness of digitally-mediated communication. In other words, CNs appears as alternative approaches, counteracting the pervasive practices associated with the centralized control of digital communications, therefore shaping more autonomous and self-governed digital interaction spaces. Therefore, CNs, through the effort to materialize specific political claims by shaping an alternative architecture for digital communication, show the potential to trigger a redefinition of power relations pertaining to Internet governance.

As a whole, inverse infrastructures highlight how power is a crucial dimension in the study of technologies and their relevance to daily life, not only because technical devices also emerge as a network of social and power struggle, but because they are an entity that is able to produce and

re-distribute power in multi-modal ways. This considerations open up a crucial question: *how does the concept of power contribute to an analysis of "inverse infrastructures" that may subvert the institutional governance of digital technologies?* Despite its relevance to the foundations of social sciences, the concept of power has been little addressed within the STS. Here, the theoretical and analytical attention to power has instead turned towards the concept of *politics*, and related processes of the politicization of science (Brown 2014). In this context, from a theoretical point of view, the reflections of Foucault can be particularly useful for shaping a dialogue between STS and the notion of power. In fact, the French philosopher analyses power, and its situated articulations, as the emerging outcome of social relations, discursive practices and technical devices. Following Foucault, power must be analysed in relation to the "…strategies, the networks, the mechanisms, all those techniques by which a decision is accepted" (Foucault 1988, 104).

Such reflection suggests to STS scholars the need to take into account power relationships as constitutive elements of the mutual entanglements between human and technology, and to consider the latter as a vector of the production and distribution of power. In this light, CNs represent specific "inverse infrastructures" that open to a re-organization of the political rationality of Internet governance. In other words, CNs define a new type of alignment between the design, management and practices of technologies, redefining the balance of power between users of digital infrastructures and the governance processes that normally shape these same infrastructures. Therefore, in the study of inverse infrastructures, the adoption of an analytical strategy that is able to capture the process by which these alignments are shaped, becomes crucial.

Another concept from the STS toolbox that is useful in terms of making sense of CN is that of "infrastructural inversion" (Bowker 1994), coined in order to emphasize a specific dimension of the "infrastructuring" work through which technologies are designed and maintained. More precisely, the idea of "infrastructural inversion" relates to an analytical sensitivity that allows us to observe infrastructures, their design and their routine use closely. Thus, this concept helps to reveal the multiplicity of discursive elements, political claims, and technical entities that are incorporated in them. In this light, CNs represent a phenomenon that specifically incorporates both discursive elements and technical devices that can support the shaping of new power relationships, and which are able to re-configure and intervene the governance of digital technologies.

This analytical sensitivity has been adopted in this transdisciplinary study[1] of the Italian WNC Ninux.org. In particular, we have emphasized the ways in which the Italian CN embodies specific political motivations, and how these motivations intersect with the technical evolution of the

[1] See research project's website at the following link: http://goldstein.disi.unitn.it/caritro/.

network. In so doing, we have grounded these reflections in terms of an "infrastructural inversion" sensitivity, which allows the study of the mutual entanglement of social, the political and technological aspects in the shaping and maintenance of these networks. This analytical strategy also permits us to highlight how CNs' technical issues are strictly connected and intertwined with the political and cultural frames shared by members of the project. Moreover, in this way, we have the chance to unfold the particular tensions and negotiations that occur between the technological aspects and the political claims connected to a critique of the evolution of Internet governance.

3. CNs as an Interdisciplinary Assemblage

This transdisciplinary research into the Italian CN has represented not only a case study about a heterogeneous "work of infrastructuring", but also offers a further occasion to develop and reflect on a trans/interdisciplinary research activity, whose this "conversation" represents a partial and work-in-progress account. Our transdisciplinary research group has been constituted from the start, sociologists mainly rooted in STS, network engineers interested primarily in morphology and the robustness of bottom-up networks; and law scholars especially focussed on how these emerging network technologies challenge current regulations concerning, for instance, liability, privacy and responsibility (for a wider account of the research see: Caso and Giovanella 2015).

As highlighted by the different and complementary perspectives presented in this "conversation", the object of CN is not only a case where a heterogeneous infrastructure can be studied from a STS perspective, but also a multifaceted entity, which interrogates, in very different ways, the diverse fields and disciplines associated with it. Therefore, this on-going transdisciplinary investigation of the Italian CN has raised several issues connected with the practice of trans/interdisciplinary research, inviting us constantly to develop a reflexive understanding about the opportunities and the constraints arising by the collaboration between different disciplines or "epistemic cultures" (Knorr-Cetina 1999). As Andrew Barry and Georgina Born have recently argued when debating about the configurations of inter/transdisciplinarity in today's research:

> "Interdisciplinarity should not be thought of as a historical given, but as mobilising in any instance an array of programmatic statements, policy interventions, institutional forms, theoretical statements, instruments, materials and research practices – *interdisciplinary assemblages* that have acquired a remarkable and growing salience" (Barry and Born 2012, 10)

In our inter/transdisciplinary research project with regard to CNs, the multiple presence of different disciplines has required not only to share and interchange our distinctive starting problems and research questions, or specific conceptual and theoretical frameworks. A further work has been also necessary to align and harmonise other crucial dimensions of the scientific work, including writing practices, the paper's rhetoric, dissemination strategies, and so on. A phenomenon such as CN is in itself a great invitation for STS practitioners to deploy conceptual tools aimed at understanding innovation processes and the heterogeneous nature of socio-material phenomena. However, at the same time, there is a need for a transdisciplinary perspective that also represents a challenge to put into play a further reflexivity about our research questions and conceptual frameworks, and more in general about the whole set of similar scientific practices: a contingent, processual and work-in-progress activities oriented toward the construction of a specific "interdisciplinary assemblage".

* * *

Sustainable Growth for Community Neworks: New Solutions to Avoid Known Pitfalls

Leonardo Maccari

1. My Engagement with Community Networks

In the first half of the year 2000s in the ICT research community (to which I belong) there was a high attention for distributed systems and for the so-called mesh and ad-hoc networks. These networks are wireless distributed networks built with a non-planned approach. A mesh network may start with as few as two persons climbing up to the roof of their houses to mount wire-less antennas to communicate with each other. Then, a third person joins the network connecting his own antenna to one of the existing ones. Then a fourth, a fifth, and so on. At the time, Wi-Fi consumer devices were starting to be affordable and a little of antenna-hacking allowed to cover distances of several hundreds of meters or even kilometers, which made this vision possible.

In the same period public administrations were supporting the deployment of broadband connections in cities, and were facing hard times trying to imagine how to bring them also to rural areas. Matching the two

concepts was intuitive. Many scientific papers imagined a world in which "last mile" connection was not going to be provided by a cable, but by a mesh network. Many speculations were made on how in a few years mesh technology would have defeated the digital divide. Irrespective of the optimism of many authors, mesh networks never really become a mass phenomenon, even if they maintained their importance in certain niches.

It was 2012 when I found myself in an Italian hacker-camp, the MOCA camp in Pescara, and discovered the existence of Ninux.org, a wireless community network set-up by a lively group of people in Rome. These people, together with other European communities, were able to set-up mesh networks made of hundreds, and in some cases thousands of nodes. At the time I used network simulators (as many ICT researchers do) to study mesh networks that could scale up to tens of nodes, and I realized that there were in-production infrastructures made of thousands of nodes. Not only, many of these networks were present in densely inhabited areas where both home and mobile broadband connections were available. Those CNs, that were relegated to the role of "last mile replacement" by ICT researchers, had been silently growing as alternative networks up to a scale than my network simulator never allowed.

From that day I dedicated most of my time researching on this theme. Quickly enough, though, I understood that CNs are not just like all other networks, plus "distributed". They are distributed networks because they could not be anything else. The communities that run them (albeit different one from the other) consider a CN not much a network that connects people but primarily a community that builds a network. And since technology does not force them to build a hierarchical network infrastructure, they also try to maintain a horizontal social infrastructure. This in turn produces a feedback to their technical choices, meaning that some solutions that are applied to other contexts cannot be used in a CN. Not because they are technologically incompatible, but because the community would not accept them. Technology influences the community, and the community gives constraints on the technology.

At that point it was clear that research that wants to help CNs to grow must be trans-disciplinary, and thus started the cooperation with the other authors of this "Discussion" space.

2. Technical Research on Community Networks: Background and Motivations

Communication and information management are central to modern sociey but they remain anchored to traditional, centralized and market-based models. CNs instead are participatory, co-operatively governed, commons-based initiatives, that represent a successful alternative approach to traditional networks. CNs are blooming in many European

countries, the most prominent example being the Spanish network www.guifi.net with currently about 30.000 nodes.

Some CNs are connected to the Internet, thus giving Internet access to the participants at a generally lower price than purely commercial initiatives, therefore, the initial scientific interest for CNs in the early 2000s was driven by their potential as a tool to overcome the digital divide (Jain 2003). Still today, CNs are a key component for the ICT4Dev (ICT for development) research community (Saldana et al. 2015).

But CNs are more than just a replacement for last-mile Internet connectivity. A CN acts as a small-scale local Internet populated with community-managed services (telephony, cloud-based services, peer-to-peer exchanges etc.) and managed with a peer-to-peer (P2P) technological and social approach. This original approach gained importance in the light of recent events that showed how the Internet, and networking in general, is a key instrument both in the hands of those that want to defend democracy, and in the hands of their adversaries. A key example is provided by the already mentioned "Datagate" scandal, which revealed that a single agency, cooperating with a very restricted group of network operators and service providers uses the Internet as a mass-surveillance instrument. The progressive centralization of networking infrastructures (in the hands of a few network providers) and of cloud-based services (in the hands of a few giant companies) contributed to make this scenario possible. A second example is the acknowledged importance that networking has played in many countries where people are fighting for democracy: networks act as an amplifier of the outer visibility of the protest, and as an internal system of organization of the protests themselves (Howard and Muzammil 2013). It is no surprise that regimes actively monitor, filter, control and disconnect personal communication platforms in order to turn them against their opponents (Morozov 2012). CNs use a decentralized approach both in the technical and social layer which reduces the number of single points of failure and makes it hard to filter, censor, or to shut down the whole network. Under this lens, the existence of independent, community-owned, locally managed networks that offer some protection against intrusion, disconnection, and commercial influence is an important novelty in the ICT panorama.

For this reason CNs recently re-attracted the attention of the research community. In the last few years, dedicated scientific workshops have been realized, special issues on relevant scientific journals have been published (both in the ICT and in the social science field[2]), and Dagstuhl seminars have been organized in order to reunite the diverse scientific communities active in this field (Crowcroft et al. 2015). At the same time, CNs have become an attractive topic even for funding agencies. The Eu-

[2] See the forthcoming "Special Issue on Community Networks" in the Elsevier Computer Networks Journal, and the "Special Issue on Alternative Internets" in the Journal of Peer Production.

ropean Union has financed various research projects focused or at least related to CNs (such as the CONFINE, CLOMMUNITY, P2PValue, and netCommons ICT projects accounting for more than 12M€ in the last 4 years) and some of them use an inter-disciplinary approach.

One theme in which technical research itself cannot cope with the complexity of this subject is given by the challenges of a sustainable growth for CNs, that is the core of this contribution. To introduce this theme, it is worth to quote a discussion I had with a well-known professor in the networking field, active in the P2P community. We were both watching a presentation from a Ph.D. student that was trying to justify his research on P2P systems, "because centralized systems cannot scale easily, while instead, P2P systems naturally scale with the number of users". This was an assumption that was easy to find in many technical research papers in the 2000s, and today we can say that it was groundless in many cases. In 2013 Facebook opened a new datacenter in Luleå, Sweden[3], claimed to contain the equivalent of four soccer fields filled up with servers. Servers that are powered only by renewable energy sources, and cooled by the "fresh air" of Northern Sweden. Such data center operates with an efficiency level that any distributed system can not even dream to reach. We changed the motivation of the Ph.D. to "we do P2P systems, because we don't like centralized ones". The reason why we don't like them can not be only technological, and CNs are an exciting experimentation field to understand it.

3. An Open Research Theme: Sustainable Growth for CNs

The definition of a suitable concept of sustainability that can be successfully applied to CNs is an open research theme. The sustainability of a commercial ISP, for instance, can be split into technical sustainability and economical sustainability. The first is given by a technical design that allows to scale-up the network and deliver good services when the user-base grows. The second is given by a positive economic balance. While some CN do have a business model, the cost of the infrastructure is generally crowd-shared by the community. A CN indeed offers a social model, thus, a CN needs to achieve technical sustainability together with social sustainability.

At the network layer, CNs face scalability problems that commercial net-works do not have to face. Commercial networks are organized with a top-down network design. Given the market demand in a certain area the net-work is organized in a hierarchical infrastructure implemented using differ-ent technologies. The Internet Service Providers (ISP) network

[3] See: http://www.theguardian.com/technology/2015/sep/25/facebook-datacentre -lulea-sweden-node-pole

generally starts in our own houses with a wireless router that we rent from the ISP. A copper/fiber/wireless connection covers the "last mile" to a first switching center, connected to a larger switching center, and so on. Every level of this hierarchy operates with different hardware, different network protocols, and requires distinct expertise to be managed. Their management is hierarchical, meaning that the technical choices that are taken on top of the pyramid are then propagated down to the base. This kind of organization is cost-efficient, it is widely used and the market offers many professionals that can be hired to manage one of the network layers. It is also one of the reasons why it was possible for the NSA to set-up a mass surveillance system. If a few high-level technologists and managers handle the data of billions of people, it is easy to force them to share such data in a stealthy way.

CNs instead enlarge when a new person joins the community. The growth of the network is spontaneous and unpredictable so it is extremely hard to apply any state-of-the-art planning strategy used for other kinds of networks. Moreover, a wireless mesh network is in itself a flat architecture. There is no specific technical provision to make a certain node more important than any other, and any person could be the owner of a very important node (a node in a strategic position of the network). This is a key feature of a CN.

Under a technical point of view, this is extremely challenging. CNs tend to grow with a flat architecture, and push their network protocols to their scalability limit, but the most interesting research is not technological only. CNs have a social goal, that is to re-empower the users with the control on their communications and use a decentralized organization to avoid the concentration of power: since the technology allows to have a flat infrastructure, there is no need to build a hierarchical social infrastructure. Experience has shown that having a non-hierarchical technical and social organization does not allow to justify the assumption that the network is less controllable, less fragile and more fairly managed than any other kind of network (Goh et al. 2001). Many different kind of networks, spontaneously evolve towards a network topology in which very few nodes are extremely important, and the large majority of nodes are irrelevant. We have shown in the past that CNs are no exception, that even in networks made of hundreds of nodes as few as five nodes route more than the 90% of the traffic, and if a few key nodes are removed, the network is badly partitioned in tens of disconnected islands (Maccari 2013; Maccari and Lo Cigno 2015). The reason for this evolution is intuitive, even if people genuinely attempt to build decentralized networks, a centralized system is simply easier to reproduce. Consider for instance the typical initial situation of a CN: when activists create the first nodes the network is composed by only a few disconnected links. Then, it may happen that a new person installs a node on a geographically dominating position (i.e. on top of a hill) and suddenly allows to connect all the disconnected stubs. That node becomes important, and the community starts to

invest in it. New people that want to join will help with its configuration and will finance the installation of new antennas to cover a wider section of the city. This will make it more likely that new people will join the network connecting to that node, which will make it even more important. This kind of growth reflects the Preferential Attachment algorithm introduced by Barabasi and Albert (1999). The B-A algorithm creates so-called scale-free networks, which are pervasive in our world and have a distinctive feature: a few nodes are critical for the life of the network and a large majority of other nodes are unimportant. This trend shows that the natural tendency of a CN is to go towards a centralized network topology, hidden behind the idea of a decentralized one.

Something similar happens with the social organization of CNs. It is not sufficient to claim to have a horizontal organization in order to have a well-balanced community. It is not sufficient to use a mailing list as the principal communication means to claim that the community is horizontal (Lovink 2004). Again, CNs are no exception, in previous works we have analyzed how the group of people behind a large Italian CN is actually led by a very small number of individuals that own the majority of the critical nodes and influence the discussions in the CN mailing list (Crowcroft et al. 2015).

A distributed socio-technical network that relies on a very small number of nodes, owned by an even smaller number of people that also influence the decisions of the community is not a P2P organization, and will collapse when this small group of people will leave the network or start to misbehave for any reason.

4. Network Metrics: the Pulse of the CN

One way to help the development of CNs is to define "sustainability metrics" that represent the state of the network and guide its growth. Those metrics will represent the "pulse" of the CN with respect to the founding political motivations and will guide future decisions.

This first step to design such metrics is to analyze qualitatively the founding principles of the CN. CNs are all different, there are some that have a strong political motivation and other ones that behave like cooperative ISPs. Qualitative research is needed to understand what are the founding values of each community, and to set-up instruments to self-assess the level of satisfaction that the community has reached, related to those funding values. This phase of the work is extremely important because it is necessary to capture those values and translate them in suitable metrics that can be analytically and automatically computed.

The second step is to analyze the network. The primary source of information is the network graph enriched with information about the ownership of the nodes and the services available on the nodes. A second source of information is the graph of interactions of the community

members acquired via the analysis of social networking instruments (mailing lists, forums, bug-trackers, Q&A systems and so on). Using this approach, known metrics can be applied to the graph in order to determine the cliques of nodes and persons that achieve an excessive control on the CN. Social scientists have defined several metrics to determine the importance of a node, or a group of nodes in a social graph, such as centrality metrics (Freeman 1977). These can represent a base on which to build suitable socio-technical metrics to periodically analyze the state of the network.

Finally, these metrics can be integrated in the on-line instruments that the communities use to manage the CN (Kos et al. 2015). These instruments are used to visualize, organize and debug the network, and are vital for the CN. With enriched metrics, they can be used to take important decisions on the life of the network. For instance, the community can decide on the creation of a new link, or a new node in order to reduce the centrality (and thus the degree of control) that a single person has on the network. Also the management of existing key nodes, or key social functions in the community organization can be split among people in a way the keeps a low concentration of control and enforces a rotation of responsibilities.

The final goal of this research is to produce information that will guide the community to grow in a way that is respectful of the founding principles they have set for themselves, and avoid known pitfalls. We have to remember that even if the Internet has been going through a centralization process, at its very beginning it was imagined to be a decentralized network, and CNs should not follow the same path.

* * *

Community Networks under the Lenses of Private Law

Federica Giovanella

1. A New Instance of an Old Problem. Namely, "Law vs. Technology"

Community networks represent a new instance of an old problem: when dealing with a new technology, law needs to evolve and adapt. As it often happens with the advent of new technologies, the birth and development of CNs has come as an unexpected event for lawmakers. Some of

the peculiarities of CNs are especially thorny, because they challenge existing laws. CNs go even further: they challenge the very same rationale behind some of the current regulations, a rationale that is the result of century-long theories and of their application.

Many aspects of CNs call for the attention of law and legal scholars. A first peculiarity of CNs is their "distribution". Distributed networks have been analyzed by legal scholars for many years (Elkin-Koren 2006), but they have gained much more attention in the last years due to their increasing application in different spheres of the information and communication tech-nology realm. Famous phenomena like BitTorrent or Bitcoin rely on distributed structures; but distributed technologies have been applied to many other kinds of services, such as data storage, microblogging, social networking. In distributed architectures both contents and actions can be distributed, with great impact on some rules, like those regulating liability, as I shall later explain.

Another aspect of CNs is their attention to anonymity. Even if each node has its own Internet Protocol (IP) address, users can choose their own IP address and change it at any time. Furthermore, contrary to what happens in the Internet environment, there are no databases in which these IP addresses are registered. There are no obligations to retain these data. Since a single IP address can be used only by a single user, users usually have a prospect in which they publicly display the IP address they self-assigned to their node. But this prospect is far from reliable, since it can be changed very easily by any member of the community. This feature of CNs, coupled with the use of anonymizing software or encryption techniques, greatly impairs the applicability of liability rules, since the possibilities to identify the person behind the screen decrease dramatically.

In the meantime, anonymity represents also an effective tool to enhance freedom of expression and to protect users' privacy. Under this point of view, CNs pose legal scholars some enduring questions: should users' privacy prevail or should other rights prevail and obtain enforcement? Should anonymity be preserved at any price? Such questions cannot obviously be answered in a vacuum; rather, they need to be placed within a concrete case.

Another aspect that characterizes many CNs is the absence of norms for their internal organization. More precisely, within a community network there are neither written norms to regulate relations among users, nor rules that attribute special powers to a possible central authority. Normally, there is a list of principles to which users have to agree (such as the "Pico Peering Agreement")[4]. These principles only reflect the behavior of users taking part to CNs. People who join the network are typically motivated and, most importantly, they share the common principles of community participation and knowledge diffusion. It is up to other

[4] See http://www.picopeer.net/PPA-en.shtml (retrieved on November 7, 2015).

members of the community to decide whether to accept the newcomers or not. There is no formal board or authority, even if some people can be seen as representing the heart of the community; these people can decide whether new users can join the network or not. An another aspect peculiar to many CNs is that, once a person joins the community, if she infringes its (more or less informal) rules, the community can take technical measures with the aim of excluding her. For instance, if a node moves its antenna to point in another direction, this can cut off some of the connected nodes, namely the nodes of those who are not ac-cepted by the community anymore.

Given these peculiarities, CNs probably constitute a case of system governed by social norms, meant as informal standards and rules applied within a given group, which that group perceives as binding. Hence, for legal schol-ars the internal governance of CNs can constitute a fascinating field of re-search.

Legal implications of CNs are not limited to those mentioned so far; for instance, CNs could also potentially be used for illicit purposes of different kind, such as sharing data protected by intellectual property or organizing cyber- or terroristic attacks. This short paper will focus only on the issue of civil liability and the hurdles posed by CNs to the structure of civil wrongs as we have known it for centuries.

2. Wrongful Actions and Damages without Liability? The Challenge posed by CNs to the Law of Extra-contractual Obligations

In this section I focus on what I believe is one of the main challenges posed by CNs to private law, namely: the apparent impossibility to enforce "extra-contractual obligations". Extra-contractual obligations are those arising outside the realm of contracts, and that typically require a person to pay for the damages caused. The distributed structure of CNs implies the fragmentation of conducts, so that it becomes difficult, if 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 very problematic to define who contributed to the violation of a right (Dulong de Rosnay 2015).

The issue becomes even more problematic if one considers that the IP addresses of the people taking part to these networks are usually undetectable or, at least, are very hard to match with real identities. When anonymization software or encryption techniques are applied, the situation worsens.

To explain which kind of obstacles the structure of CNs poses to the enforcement of law, I shall make an example. Let us suppose that a net-

work's user – and owner of a node – acts in a way that defames a subject either within or outside the network. In a "classical" case of defamation, the person causing the damage would be identified, sued and eventually condemned to pay damages. In the realm of Internet the wrongdoer would be identifiable through her IP address: with the collaboration of the Internet access provider, the damaged person would obtain the real identity of the user and then sue her[5]. In some specific instances, in accordance with European Directive 2000/31 on Electronic Commerce[6], also an Internet service provider could be held liable (Julià-Barceló and Koelman 2000; Baistrocchi 2003; Verbiest et al. 2007).

Transposing this example into CNs world, one could imagine the following liability situations: the first involves the user-wrongdoer; the second concerns the provider, for the case the wrongful action destination is placed outside the CN; the last one implicates the CN itself. In addition, another user – different from the wrongdoer – could also be held liable for the case she shares her Internet connection with other nodes, acting as a so-called "gateway node".

With regard to user's liability, as mentioned, the first step would consist of identifying the person behind the screen, meaning the owner of the node from which the wrongful content came. Here comes the first "wall" that CNs erect against law enforcement: given the above-illustrated impossibility to identify users behind screens, technology could not be useful in finding the possible infringer and the damaged person could not reach its goal of obtaining justice. This represents a first "failure" for extra-contractual obligations enforcement.

Whenever 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 public IP address. However, at least in the Italian framework, the gateway node owner would not be held liable, as there are rules introducing this kind of third-party liability (Giannone Codiglione 2013, 123-135). A possibility would be to consider the owner of the gateway as concurring in the wrongdoing (for example under art. 2055 of the Italian civil code). This technique might be a solution to find a way for the victim to obtain redress for her damages; however, under the point of view of the sustainability of the network, such a solution would be a deterrent for a node's owner in sharing her Internet connection with other users and, ultimately, with the community.

[5] This is a simplistic description of a scenario that can actually be much more complicated. For the sake of clarity let us assume that it works this way. More generally, the description made in this paper is necessarily limited, for a deeper analysis see Giovanella (2015).

[6] 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.

In the last case illustrated, namely: if the wrongful actions are committed through a gateway, the provider supplying the Internet connection to the gateway user may be considered as a possible defendant. These providers enjoy the liability limitations introduced by Dir. 2000/31 under art. 12. Put it simply, they cannot be held liable if they do not take part in or somehow affect the transmission of illicit content made by users. In addition, very often contracts between users and access provider include a liability limitation clause and expressly forbid the customer to share the connection. The user sharing her connection would therefore breach the contract and be liable for that; in addition, the user might also be asked to act as a warrant for damages suffered by the provider as a consequence of the illicit conduct committed through the gateway (Giannone Codiglione 2013, 107; Mac Síthigh 2009, 366-369; Robert et al. 2008, 217 ff.).

Finally, in case the wrongful action takes place entirely within the CN, one could wonder whether the network itself could be liable. As earlier highlighted, CNs originate spontaneously within communities. These communities are self-organized and without a central authority. Contrary to what happens to a provider, they are not incorporated as companies. CNs do not have a person in charge that could be held liable for cases of wrongful actions. As a matter of fact, in the majority of cases CNs do not have legal personality and it would not be possible to sue them as entities. The only possibility would be to sue them as a community, i.e. to sue all the people within the CN. However, the same consideration made above for users' and gateway nodes' liability applies here.

A different conclusion could be reached in case the CN organizes itself as an association or takes another form, such as a foundation[7]. In this event, specific norms, which already exist, would apply.

It follows from what has been told so far that the structure and functioning of CNs pose a number of hurdles to the enforcement of liability rules. Normally, 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 tends to be impossible.

3. The Interplay between Different Sciences as a Tool to Overcome Current Hurdles

The described scenario provides an idea of the challenges that law must face when a new technology arises. Lawmakers should consider whether to adopt specific laws for CNs and, if so, what regulation would

[7] This is for example the case of the Barcelona network 'guifi.net', which is part of a foundation; see http://fundacio.guifi.net/index.php/Fundaci%C3%B3 (retrieved on November 7, 2015).

be the most effective. It would be fundamental to implement solutions that balance CNs' needs with right holders' ones, in order to discourage wrongful actions while allowing CNs to further develop and prosper (Dulong de Rosnay 2015; Giovanella 2015). However, regardless ofthe possible solutions that law-and policy-makers could (or should) apply to fill the existing gaps and overcome the illustrated difficulties, there might be solutions that CNs themselves could im-plement.

As emerges from the previous paragraphs, CNs are currently in a vacuum as for civil law enforcement. However, it might not be distant the time in which things will change. As CNs are growing both in number of people involved and in popularity, the possibilities that wrongful actions occur and that someone seeks redress are also growing.

In this perspective, the interaction between different sciences might play a key role. There might be technical tools that the network could implement taking into account existing laws and possible infringements. The enactment of specific technical measures – such as filters or detectors – might be both a deterrent for infringing conducts and a possible defence in case of lawsuits. In this situation, lawyers and engineers could work one with another with the aim of strengthening CNs: both could detect the weaknesses under their own point of view and try to help the network in gaining a stronger structure. While this would aid the "physical" aspect of the network, a similar approach could be taken for the "intangible" aspects of the community. This could be possible through the study of the internal relationships between the community's members, as well as of the role of some specific users. This task clearly reminds of sociological research. The study of the dynamics among users could reveal whether there are some users that *de facto* represent the network or manage it. Since these users could be more easily the subject of legal claims, such a study would help again strengthening CNs.

All in all, transdisciplinary research proves to be not only fruitful, but also necessary for legal scholars to confront new and emerging technologies and to understand both their effects on law and, in turn, the effects of law on these technologies.

Acknowdledgments

Federica Giovanella and Leonardo Maccari wish to thank the University of Trento that supported this work under the project "Wireless Community Networks: A Novel Techno-Legal Approach" – Research Projects 2014.

In compliance with Italian academic folkways, Stefano Crabu and Paolo Magaudda acknowledge that the former wrote paragraph 2 and the latter wrote paragraphs 1 and 3.

References

Baistrocchi, P. (2003) *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, in "Santa Clara Computer & High Technology Law Journal", 19 (1), 111–130.

Barabási, A.L. and Albert, R. (1999) *Emergence of scaling in random networks*, in "Science", 286 (5439), pp. 509–512.

Barry, A. and Born, G. (2013) *Interdisciplinarity: reconfigurations of the social and natural sciences*, London, Routledge.

Bowker, G.C. (1994) *Science on the run: Information management and industrial geophysics at Schlumberge*r, 1920–1940, Cambridge, MIT Press.

Brown, M.B. (2014) *Politicizing science: Conceptions of politics in science and technology studies*, in "Social Studies of Science", 45 (1), pp. 3–30.

Bruni, A., Pinch, T. and Schubert, C. (2013) *Technologically Dense Environments: What For? What Next?*, in "Tecnoscienza: Italian Journal of Science & Technology Studies", 4 (2), pp. 51-72.

Carroll, J.M. and Rosson, M.B. (2003) *A trajectory for community networks*, in "The Information Society", 19 (5), pp. 381–393.

Caso, R. and Giovanella, F. (eds.) (2015) *Reti di libertà. Wireless Community Networks: un'analisi interdisciplinare*, Napoli, Editoriale Scientifica.

Clement, A. (2014) *NSA Surveillance: Exploring the Geographies of Internet Interception*, in "iConference 2014 Proceedings", pp. 412–425.

Crowcroft, J., Wolisz, A. and Sathiaseelan, A. (2105) *Towards an Affordable Internet Access for Everyone: The Quest for Enabling Universal Service Commitment (Dagstuhl Seminar 14471)*, in "Dagstuhl Reports", 4 (11), pp. 78–1377.

De Filippi, P. and Treguer, F. (2015) *Expanding the Internet Commons: The Subversive Potential of Wireless Community Networks*, in "Journal of Peer Production", 6, pp. 1–11.

Dulong de Rosnay, M. (2015) *Peer-to-peer as a Design Principle for Law: Distribute the Law*, in "Journal of Peer Production", 6, pp. 1–9.

Egyedi, T.M. and Mehos D.C. (2012) *Inverse Infrastructures: Disrupting Networks from Below*, Cheltenham, Edward Elgar Publishing.

Elkin-Koren, N. (2006) *Making Technology Visible: Liability of Internet Service Providers for Peer-To-Peer Traffic*, in "N.Y.U. Journal of Legislation & Public Policy", 9, 15–73.

Flickenger, R. (2002) *Building wireless community networks*, O'Reilly, Sebastopol, CA.

Foucault, M. (1988) *On power*, in L. D. Kritzman (Ed.), *Politics, philosophy, culture: Interviews and other writings 1977–84*, New York: Routledge, pp. 96–109.

Freeman, L.C. (1977) *A Set of Measures of Centrality Based on Betweenness*, in "Sociometry", 40 (1), pp. 35–41.

Giannone Codiglione, G. (2013) *Indirizzo IP, Reti Wi-Fi e responsabilità per illeciti commessi da terzi*, in "Diritto dell'Informazione e dell'Informatica", 1, 107–143.

Giovanella, F. (2015) *Liability Issues in Wireless Community Networks*, in "Journal of European Tort Law", 6 (1), 49–68.

Goh, K.I., Kahng, B. and Kim, D. (2001) *Universal behavior of load distribution in scale-free networks*, in "Physical Review Letters", 87 (27). doi: 10.1103/PhysRevLett.87.278701

Howard, P.N. and Muzammil, H.M. (2013) *Democracy's Fourth Wave? Digital Media and the Arab Spring*, Oxford, Oxford Press.

Hughes, T.P. (1983) *Networks of Power: Electrification in Western Society 1880-1930*, Baltimore, Johns Hopkins University Press.

Kos, J., Milutinović, M. and Čehovin, L. (2015) *Nodewatcher: A substrate for growing your own community network*, in "Computer Networks". doi:10.1016/j.comnet.2015.09.021

Jain, S. and Agrawal, D. (2003) *Wireless community networks*, in "Computer", 36 (8), pp. 90–92.

Jasanoff, S. (2005) *Designs on Nature: Science and Democracy in Europe and the United States*, Princeton, Princeton University Press.

Julià-Barceló, R. and Koelman, K.J. (2000) *Intermediary Liability: Intermediary Liability in the E-Commerce Directive: so far so good, but it's not enough*, in "Computer Law & Security Review", 16 (4), 231–239.

Knorr-Cetina, K. (2009) *Epistemic cultures: How the sciences make knowledge*, Harvard, Harvard University Press.

Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*, O'Reilly, Sebastopol, CA.

Lovink, G. (2004) *My First Recession: Critical Internet Culture in Transition*, Rotterdam, NAi Publishers/V2-Organization.

Mac Síthigh, D. (2009) *Law In The Last Mile: Sharing Internet Access Through Wifi*, in "SCRIPTed", 6 (2), 366–369.

Maccari, L. (2013) *An analysis of the Ninux wireless community network*, in "Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International", Lyon, pp. 1–7. doi: 10.1109/WiMOB.2013.6673332

Maccari, L. and Lo Cigno, R. (2015) *A week in the life of three large wireless community networks*, in "Ad Hoc Networks", 24 (Part B), pp. 175–190.

Milan, S. (2013) *Social movements and their technologies: Wiring social change*. Palgrave, Macmillan.

Morozov, E. (2012) *The net delusion: The dark side of Internet freedom*, New York, PublicAffais.

Oudshoorn, N. and Pinch, T. (2003) *How users matter: the co-construction of users and technology (inside technology)*, Cambridge, Cambridge University Press.

Parks, L., and Starosielski, N. (Eds.) (2015) *Signal Traffic: Critical Studies of Media Infrastructures*, Champaign, University of Illinois Press.

Robert, R., Manulis, M., De Villenfagne, F., Leroy, D., Jost, J., Koeune, F., Ker, C., Dinant, J.M., Poullet, Y., Bonaventure, O. and Quisquater, J.J. (2008)

WiFi Roaming: Legal Implications and Security Constraints, in "International Journal of Law and Information Technology", 16 (3), 215–241.

Saldana, J. Arcia-Moret, E.A., Braem, B., Pietrosemoli, E., Sathiaseelan, A. and Zennaro, M. (2015) *Alternative network deployments. taxonomy, characterization, technologies and architectures. Version 01*, Informational RFC Draft, in https://tools.ietf.org/html/draft-irtf-gaia-alternative-network-deployments-00 (retrieved 9.10.2015).

Schuler, D. (1994) *Community networks: building a new participatory medium*, in "Communications of the ACM", 37 (1), pp. 38–51.

Söderberg, J. (2011) *Free Space Optics in the Czech Wireless Community: Shedding Some Light on the Role of Normativity for User-Initiated Innovations*, in "Science, Technology & Human Values", 36 (4), 423–450.

Star, S. L. and Bowker, G.C. (2002) *How to Infrastructure*, in L.A. Lievrouw and S.L. Livingstone (Eds.), *Handbook of the New Media*, London, Sage, pp. 230–245.

Star, S.L. and Ruhleder, K. (1996) *Steps toward an ecology of infrastructure: Design and access for large information spaces,* in "Information Systems Research", 7 (1), 111–134.

Van Oost, E., Verhaegh, S. and Oudshoorn, N. (2009) *From innovation community to community innovation: User-initiated innovation in wireless Leiden*, in "Science, technology & human values" 34 (2), pp. 182–205.

Verbiest, T., Spindler, G., Riccio, G.M. and Van der Perre, A. (2007) *Study on the Liability of Internet Intermediaries*, in http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf (retrieved on November 7, 2015).

Verhaegh, S. and Van Oost, S. (2012) *Who Cares? The Maintenance of a Wi-Fi Community Infrastructure*, in T.M. Egyedi and Mehos D.C. (Eds.), *Inverse Infrastructures: Disrupting Networks from Below*, Cheltenham, Edward Elgar Publishing, pp. 141–160.

Wilson, S. (2015) *How to control the Internet: Comparative political implications of the Internet's engineering*, in "First Monday", 20, 2.