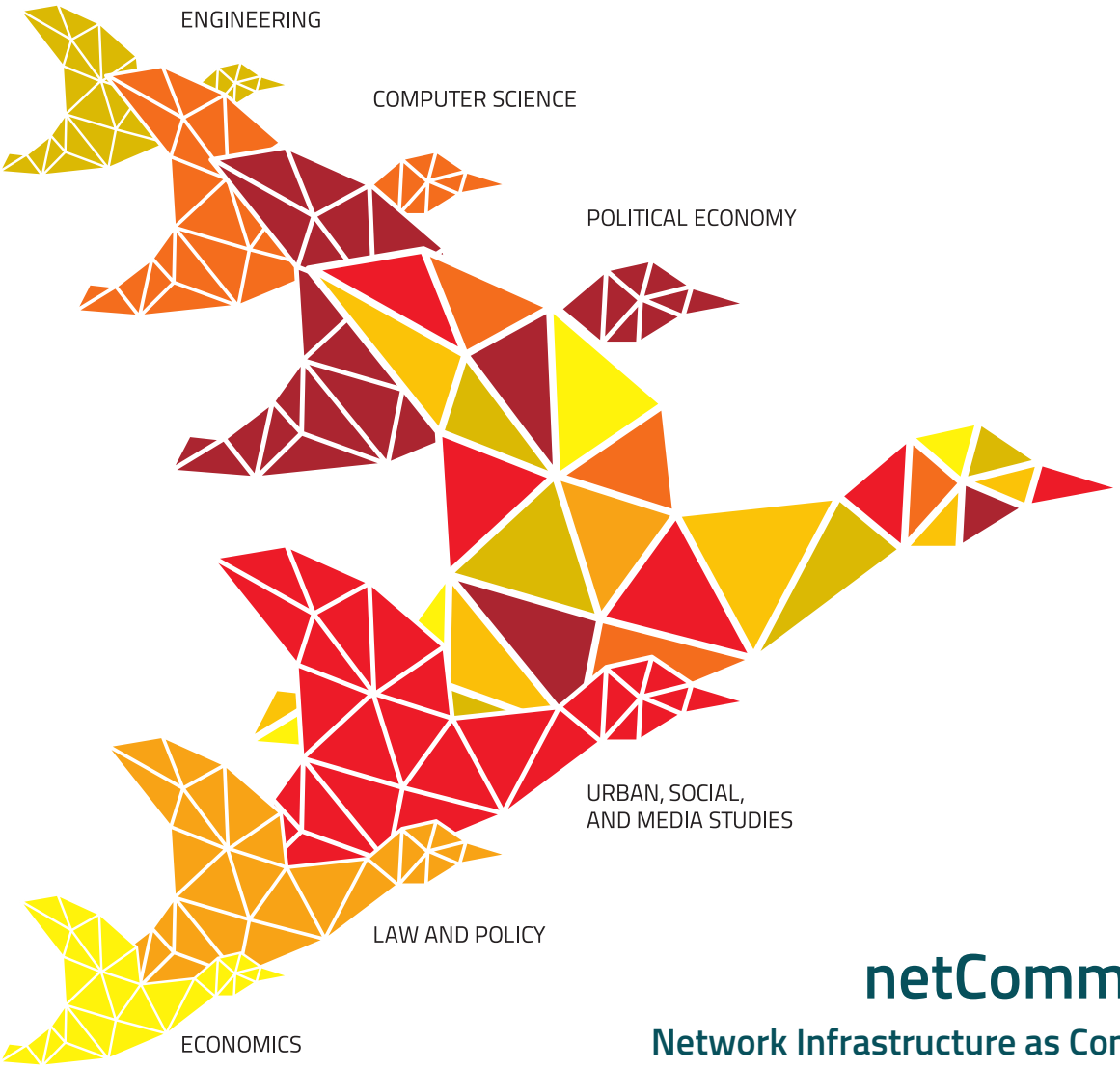


netCommons

Network Infrastructure as Commons

European Legal Framework for Community Networks (CNs) (v2)

Deliverable Number D4.2
Version 0.51
July 1, 2017

Co-Funded by the Horizon 2020 programme of the European Union
Grant Number 688768

netCommons.eu

Project Acronym:	netCommons
Project Full Title:	Network Infrastructure as Commons.
Call:	H2020-ICT-2015
Topic:	ICT-10-2015
Type of Action:	RIA
Grant Number:	688768
Project URL:	http://netcommons.eu

Editor:	Mélanie Dulong de Rosnay, CNRS
Deliverable nature:	Report (R)
Dissemination level:	Internal
Contractual Delivery Date:	December 30, 2017
Date of Present Release	July 1, 2017
Number of pages:	59
Keywords:	Community Networks, Civil Liability, Privacy and Data Protection, Electronic Communications Code, Advocacy
Authors:	Mélanie Dulong de Rosnay, CNRS Federica Giovanella, UniTN Arthur Messaud, CNRS Félix Tréguer, CNRS
Peer review:	Renato Lo Cigno, UniTN

History of Revisions

Rev.	Date	Author	Description
v0.1	19/06/2017	Federica Giovanella	First draft
v0.2	21/06/2017	Mélanie Dulong de Rosnay	Comments, suggestions
v0.5	29/06/2017	Federica Giovanella	Implemented suggestions and comments; added new appendixes
v0.51	30/07/2017	Renato Lo Cigno	Formal fixes and goal clarification

Executive summary

This deliverable is a draft of D4.2 that is due at M24 and it illustrates the current stage of development of T4.1 describing what has been done between the starting date at M13 and M18 and the next steps of the research to be developed and finalised. In the spirit of netCommons project this draft is made public on the project website[1], so that it can have an early diffusion and dissemination, even if it is not final and its conclusions are provisional. In no way can this draft be considered a formal obligation or delivery to the European Commission (EC), albeit it can be used by anyone to follow and benefit from netCommons activity and work.

The goal of this document is to describe the steps taken so far in order to reach the objectives of the second year of the project in WP4, with a focus both on what has been done and on what still needs to be done within the end of year 2.

It draws on the findings of D4.1 [1] that described existing legislation and case law relevant to Community Networks (CNs). D4.1 goal was understanding whether the existing laws allow the prosperity of the current CNs and of new ones, or they impair them.

Based on these findings, D4.2 describes the actual application of laws within community networks as it emerges from some face-to-face interviews conducted by netCommons researchers with CNs' members. The answers obtained through these interviews helped to shape a survey that will be circulated in the next two months amongst CNs' members, in order to try to collect as much information as possible about the way CNs deal with legal issues.

The results of the survey will be included in the final version of D4.2 (due at M24), which in turn will be the basis to draft some "Best practices guide for CNs" (T4.3 – D4.5, due to at M36).

The report also illustrates the actions taken by netCommons to raise the awareness of CNs and to influence the European policy makers in the process of adoption of the new Electronic Communications Code. In particular, this part of the WP includes two main actions: first, an open letter that was circulated among CNs and then sent to the EU policy makers, followed by blog posts and legal analysis of the amendments to the Telecom Package; second, a conference that is being organized and to be held in Fall 2017 at the European Parliament and involving some Members of the Parliament. This actions are strictly intertwined with Task 1.3 on "Advocacy capacity-building" and its forthcoming deliverable D1.5 due for M24 and for which an early draft has been prepared for internal review (not yet public) also at M18.

The report also describes what are the next steps to be taken to reach the needed outcome and to allow netCommons researchers to reach the goal of sustaining CNs as for the legal aspects.

[1] All public deliverables can be browsed and downloaded at http://netcommons.eu/?q=content/deliverables-page.

Contents

List of Acronyms

CN	Community Network
EC	European Commission
ECS	Electronic Communications Service
EECC	European Electronic Communications Code
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
IAP	Internet Access Provider
NRA	National Registration Authority
ToS	Terms of Service
VPN	Virtual Private Network

1. Introduction

This draft deliverable illustrates the current stage of development of T4.1 describing what has been done between M13 and M18.

The goal of this deliverable is to describe the steps taken so far in order to reach the objectives of the second year of the project in WP4, with a focus both on what has been done and on what still needs to be done within the end by M24.

It draws on the findings of D4.1 [1] that described existing legislation and case law relevant to CNs. D4.1 was aimed at understanding whether existing laws allow the prosperity of the current CNs and of new ones or they impair them.

Based on these findings (summarized briefly in Sec. 2.1), this draft of D4.2 describes the actual application of laws within community networks as it emerges from some face-to-face interviews conducted by netCommons researchers with CNs' members (Secs. 2.3 and 2.4). The answers obtained through these interviews helped to shape a survey that will be circulated in the next two months amongst CNs' members, in order to collect as much information as possible about the way CNs deal with legal issues.

The results of the survey will not only be described in the final version of D4.2 due to at M24, but they will also serve as a basis to draft some "Best practices guide for CNs" (T4.5-D4.5).

This draft also illustrates the actions taken by netCommons to raise the awareness of CNs and to influence the European policy makers in the process of adoption of the new Electronic Communications Code (Chapter 3). In particular, this part of the WP includes three main actions: first, an open letter that was circulated amongst CNs to collect signatures and then sent to the EU policy makers (Sec. 3.1); second, some notes drafted to assist the Members of the Parliament of the EU to adopt a text of the Electronic Communications Code that will take into account also the rights and needs of CNs and its users (Sec. 3.2); third, a workshop that is being organized and will be held in Fall 2017 at the European Parliament, involving some Members of the Parliament (Sec. 3.3).

The last section draws some brief conclusions (Chapter 4).

2. European Legal Framework for Community Networks

2.1. First year findings

In order to allow a better comprehension of the research that has been carried out in the past few months, a brief summary of the findings of the first year of research will be summarized hereinafter.

It is fundamental to stress that although D4.1 focused on three main issues, namely: telecommunications policy, civil liability, and personal data protection, the current research focuses only on the two latter.

The reason why we decided to narrow down the scope of our research is mainly related to the fact that the regulatory framework for telecommunication is undergoing significant changes at the European Level. More precisely, as it will be described later in this report, the EU policy makers are in the process of adopting a "**European Electronic Communications Code**" (European Electronic Communications Code (EECC)). The proposal for a Directive establishing the EECC will merge four existing Directives on telecommunications: Framework Directive (Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services), Authorisation Directive (Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services), Access Directive (Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities) and Universal Service Directive (Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services).

Given the ongoing modifications, we decided not to focus on the application of these rules on CNs, but rather on the possibility to influence the making-process of the Directive through advocacy actions (see part 3).

2.1.1. Liability Issues

"**Civil liability**" can be defined as the **liability arising from private wrongs or breach of contractual duty** and that is **not criminal** liability; normally, civil liability implies a duty to compensate for damages.

Civil liability can for example arise when someone causes damages to someone as a consequence of a privacy breach or defamation, or in cases of intellectual property rights' damages. These are classical cases arising from the use of the Internet. The diffusion and use of CNs might entail similar cases.

An example will help to clarify how the current European and national rules apply.

Let us suppose that a user shares a movie within the CN without having the right to do so. This is a case of copyright infringement. Who could be held liable for such infringement?

Three hypotheses might be considered.

2.1.1.1. Liability of the final user

The **first case** is the liability of the final user. It might however be difficult in the context of CNs to allocate liability to the final user, for two reasons:

- the **illicit action might be allocated to a high number of different users' machines** and it becomes impossible to understand who is the person that actually committed the action;

- sometimes specific **software shields users' identity and allows anonymity**.

2.1.1.2. Liability of the gateway node's owner

If a video is **uploaded** by a user to the Internet **through a gateway node**, the person who runs the gateway node would be identifiable through his/her public IP address. This person might be considered liable depending on national laws:

- **Some countries** (for instance, Germany with the Störerhaftung doctrine and France with HADOPI law) **hold someone liable for the mere fact of not securing his/her Wi-Fi network.** In such countries an individual can be ordered by a court to put a password on his/her Wi-Fi network and if s/he does not, s/he would be held liable in case of damages suffered by a third person. In the example, the action of sharing the video could cause a damage to the copyright holder of the video. The copyright holder may not be able to identify who uploaded it and could sue the owner of the gateway node (of course the prior step of identification of the gateway owner by the provider would be needed).

  Other countries do not have similar laws (Italy, for example).
- In addition, the owner of the gateway node normally signs a **binding contract with an Internet Access Provider (IAP)**, in which **often a clause expressly forbids the customer to share the connection**. Another frequent clause is the one that considers the **customer liable for the damages** suffered by the provider as a consequence of a conduct that is prohibited by the contract itself. Therefore, for the **mere fact that the customer shares his/her connection s/he will be liable for breaching the contract and** – in case of damages caused by a third party's wrongdoing – **s/he could also be asked to compensate the victim.**

2.1.1.3. Liability of the CN

Can the CN be held liable? This **depends** on two main issues:

- Is the CN organised as an association or a foundation? In other words, **has the CN a legal status?**
  - **If so, national rules applies.** Usually one or more individuals are in charge of the legal entity and these individuals are those who can be held liable for the wrongdoings occurring within the CN.
  - **If the CN does not have a legal status, it is not possible to hold it liable.**
- Is the CN also an I**nternet Access Provider** under national law?
  - If so, European rules on Internet Providers' liability apply. In particular, access providers are those providers that transmit information provided by a recipient of the service or provide access to a communication network.
  - **Art 12, Dir. 2000/31** [2] – and its corresponding implementation in national law – states that a "provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. 2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission".
  - If a CN is an ISP it qualifies for the liability exemptions under Dir. 2000/31 and therefore it might be held liable only if it does not comply with art. 12 above quoted.
- Recently the Court of Justice of the European Union (*Tobias Mc Fadden vs. Sony Music Entertainment Germany GmBH*, September 15, 2016) decided that in order to discourage the illegal sharing of works protected by intellectual property rights a court can order a provider who runs a Wi-Fi network to

password-protect the network. In case users want to access the network they must be identified, so that they cannot act anonymously. If a CN is qualified as an IAP this decision might be easily applied by national courts as well. This means that although the CN would be exempted from liability under art 12, Dir. 2000/31 (see above under IAP's liability), it could be the target of this kind of orders.

2.1.1.4. Open questions after the Mc Fadden case

Open questions remain after the CJEU's decision:

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

2.1.2. Data Protection and Privacy

2.1.2.1. General Obligations

CNs shall comply with the obligations imposed by the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) [3] when they **process** (collect, store, use or disclose) **personal data** (information relating to an individual and which may be directly or indirectly attributed to this individual), or may be fined up to 20,000,000 EUR. These obligations are imposed on all CNs, irrespective of their legal status.

1. Processing shall pursue and be limited to a lawful purpose, which is the case where:
   - users have freely given their explicit, informed and specific **consent**;
   - processing pursues a "**legitimate interest**" which is not overridden by users' own interests (CNs shall balance these interests);
   - processing is necessary for performing a **contract** with users; or
   - processing is necessary for complying with a **legal obligation**.
2. CNs shall implement security measures preventing accidental or unlawful processing and notify any security breach to authorities within 72 hours (and, in some cases, to individuals).
3. CNs shall provide users with complete information about each processing action (its purpose and duration, whether data are disclosed to third parties or transferred outside the EU).
4. CNs shall allow users to freely exercise their rights (obtaining a copy of their data, asking for the rectification of inaccurate data or the erasure of unlawfully processed data) and comply with their requests within one month.
5. CNs shall maintain a record of its processing and, where a processing result in specific risks, carry out a prior impact assessment.
6. CNs shall only **transfer** data to a country **outside the EU** in three cases:
   - the European Commission has issued an "**adequacy decision**" about this country (Argentina, Canada, Switzerland, Israel, Uruguay, New-Zealand... or US companies which have submitted to the Privacy Shield);
   - data are transferred to a third party which has entered into a contract with the CN containing **standard contractual clauses or appropriate safeguards**;
   - users have **consented** to the transfer or the transfer is necessary for the performance of a **contract** with users.

CNs shall comply with these general obligations whenever the process personal data, but they can be subject to fewer or more obligations depending on their activities, as explained in the next section.

2.1.2.2. Specific Obligations

1. The main activity of CNs is to provide access to their network and to **transmit communications** over it: both the content and traffic data of such communications are personal data;
   - transmitting these data on behalf of users **always pursues a lawful purpose** (whether or not users have explicitly given their consent);
   - such transmission is regarded as an "**electronic communications service**" (Electronic Communications Service (ECS)).
2. Other activities of CNs (such as VoIP or email) imply processing personal data:
   - CNs shall pursue a lawful purpose (consent, "legitimate interest" or contract);
   - some of these services may be regarded as ECS (whose legal definition remains unclear).
3. Art. 6, Dir. 2002/58 [4] provides that CNs may only **reuse the traffic data** processed for the provision of an **ECS**:
   - if the data have been fully anonymized; with user's consent;
   - in order to bill users or for interconnection payments;
   - or, in France and Germany, in order to ensure network's security.

   ! CNs **may not reuse** such data for pursuing any "legitimate interest".
4. National laws provide that CNs have to **retain all traffic data** processed for the "transmission of communications" (IP addresses and date and time of call or log-in and log-off, IMSI, location data...):
   - In **Germany**, for ten weeks or may be fined up to 500,000 EUR;
   - In **Spain**, for one year or may be fined up to 20,000,000 EUR;
   - In **Italy**, for one year for Internet access and two years for telephone service, or may be fined up to 50,000 EUR;
   - In **France**, for one year or may be fined up to 375,000 EUR; in addition French hosting providers shall retain during one year information about users.

   ! The European Court of Justice has recently found that such laws may be **violating the Charter of Fundamental Rights of the EU** (case *Tele2 v Post-och telestyrelsen*, December 21, 2016)[1], but these laws have yet to be repealed.

2.1.2.3. Specific issues regarding decentralized networks

In practice, complying with these obligations may be **excessively constraining** for decentralized structures such as CNs. Thus, CNs may try to **adapt** these rules to their specific structure or to change them through **advocacy**. Otherwise, they should comply with the **strict framework** described below, as imposed by the GDPR.

1. Where decisions are made by a central legal entity and participants carry out processing on its behalf:
   - the central entity is liable for compliance with all CN's obligations;
   - participants shall implement security measures, keep records, retain traffic data;
   - participants shall enter into a **contract** with the central entity, providing for specific obligations.

[1] Joined cases Tele2 Sverige AB v. Post-och telestyrelsen (C-203/15) and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15), December 21, 2016.

2. Where decision are **collectively** made by the participants:
    - participants shall enter into a **collective contract** determining their respective obligations (who shall obtain users' consent, provide them with required information or answer their requests, for instance);
    - each participant shall retain the traffic data he/she individually processes.

2.2. Scope, goals and methodology of the second year of research

The second year of research is aimed at understanding how CNs deal with legal obligations and duties imposed both by European and national legislation.

In order to collect this information, we have conducted a few face-to-face interviews with some CNs members. We mainly contacted people in charge of the community or people dealing with legal issues (for example, the interviewed person could be a lawyer that is involved in a CN).

The interviews are conducted in the language spoken by the interviewed person and then transcribed and translated into English. The interviewee's name is not mentioned, in order to allow a high level of anonymity. After transcription, the recorded interview are deleted.

Based on the interviews conducted in the first months of 2017, we designed a questionnaire (Appendix A) that will be circulated amongst CNs and their members. The questionnaire is being created through "limesurvey"[2], an online tool that allows anonymization (for more details on ethical assessments, consider D8.1 Ethics Requirements[5], in particular par. 2.1.5).

In the next section we summarize the information collected with the interviews.

As the number of interviews is still low, we are not able to illustrate clear findings. Therefore the information is collected in Tabs. 2.1 to 2.5, in order to allow a first comparison of the collected answers.

2.3. Information Collected through Interviews

As mentioned, we decided to focus only on two specific legal issues, namely civil liability and personal data protection. As for telecommunications policy, our efforts have concentrated on the advocacy activities later described (Chapter 3).

This paragraph will therefore **summarize the findings of the first few interviews** carried out with CNs' members. In an attempt to be clear, we will convey the information through some tables. The questions made in the face-to-face interviews were very close to those included in the survey (Annex 1).

We grouped the information collected into five main areas (and tables): **organisation** (Tab. 2.1), **services offered (Tab. 2.2**, **relationship with users** (Tab. 2.3), **processed data** (Tab. 2.4), **data retention** (Tab. 2.5).

Each subject area aims at clarifying the functioning of CNs and their way of dealing with specific obligations imposed by the law, especially from the point of view of personal data protection and data retention. At the same time, organizational and contractual aspects should help to clarify what would happen if a case of civil liability occurred.

[2] https://www.limesurvey.org/

CN France 1	▷ Organized as an association ▷ General decisions are made by the members and/or board of CN ▷ Specific technical decisions are made by system administrators ▷ The CN is legally an IAP
CN France 2	▷ Organized as an association ▷ General decisions are made by the members and/or board of CN ▷ Specific technical decisions are made by system administrators ▷ The CN is legally an IAP
CN Italy 1	▷ Does not have any legal existence. ▷ Decisions are taken either through the mailing list or in personal meetings – the CN is a very small group of people (less than 10). ▷ With regard to the single nodes, each member does what s/he likes most. ▷ Some members do also manage other people's nodes (for instance because these people lack technical skills or because they are not interested in taking part to the CN, but allow to use their balcony/roofs and so on). ▷ There is an online board through which the CN manages projects (for instance: to create web applications)
CN Italy 2	▷ The CN was created in 2007 ▷ It became an association in 2011 ("associazione non riconosciuta" under the Italian legal system) ▷ In 2015 it applied to become an ISP but it has not had any answer yet. ▷ The services are managed by the representatives of the association. ▷ The representatives of the association also choose what services to provide and how. ▷ The general assembly was asked more than once to express their needs, but they never did.

Table 2.1: Organisation

CN France 1	▷ CN provides its subscribers with an access to the Internet through ADSL/VDSL.
	▷ They have access to the following services:
	  ▷ Mail
	  ▷ Domain name, hosting
	  ▷ Bittorent tracker
	  ▷ Virtual machine
	  ▷ VPN
	  ▷ Also, any user may use an ”open bar” VPN, which is not logging any information about users
	▷ Subscribers must pay around 30 euro per month.

CN France 2	▷ CN provides its subscribers with an access to the Internet through ADSL/VDSL.
	▷ They have access to the following services:
	  ▷ Mail
	  ▷ Domain name, hosting
	  ▷ Bittorent tracker
	  ▷ Virtual machine
	  ▷ VPN
	  ▷ Also, any user may use an ”open bar” VPN, which is not logging any information about users
	▷ Subscribers must pay around 30 euro per month.

CN Italy 1	▷ There is no payment ▷ The network is open; when someone connects to it, usually it introduces him/herself to the other community members. ▷ The CN is connected to the Internet because some users share their personal Internet connection. ▷ No services are offered against payment; any member can offer his/her own services: for instance some allow storing information of other users on their servers. There is a cloud server, but only for internal use.

CN Italy 2	▷ Access to the network is reserved only to those who are part of the association
	▷ Each associate gives an annual contribution (around 100 euros) to be part of the association.
	▷ To be part of the CN, a person has to be member of the association.
	▷ They offer internet connection, as they buy fiber; currently fiber to the cabinet – 160 mb (trying to have fiber to the home)
	▷ They offer some other services, including:
	  ▷ e-mail;
	  ▷ hosting;
	  ▷ cloud services;
	  ▷ game server;
	  ▷ some cameras that record the landscape and publicly displays the weather and the panorama in a website (publicly accessible).
	  ▷ an sms service for other associations (associations that are members of the CN): through this system, the representatives of the association has its own user profile and can send sms to any associate who subscribed to the service.

Table 2.2: Services offered

CN France 1	▷ Subscribers must become members of the CN association in order to access the services. This is done through a contract which describes that personal data are processed (but not really how or for what purpose)
CN France 2	▷ Subscribers must become members of the CN association in order to access the services. This is done through a contract which describes that personal data are processed (but not really how or for what purpose)
CN Italy 1	▷ There are no limitations on the admission of people ▷ Those who want to join must agree to the pico-peering agreement. ▷ There is no distinction between users and members. When someone connects to the network it agrees to have her data collected (see below).
CN Italy 2	▷ Those who enter the association have to sign a form with the Terms of Services (ToS). ▷ The ToS warn users that they are responsible for what happens using their login/password; that they bear the civil and criminal liability for wrongdoing committed by themselves or someone else using their login/password. ▷ Users also commit themselves not to use p2p software, in order not to impair shared resources (detected and stopped through a "next generation firewall" - NGF) ▷ The ToS also forbid some other possible uses of the network by its users.

Table 2.3: Relationship with users

CN France 1	▷ CN collects and stores users name, postal and email addresses, phone number, IBAN. Members may access these info and change them on a personal page of CN website ▷ These information are associated with the IP address allocated to the user. ▷ CN gives users' address and phone number to other operator for interconnection matters (ex: Orange needs to know which line CN will use in order to give it access). However, CN fails to specifically inform users about such transfer. ▷ CN monitors how some of their services are used: if some is downloading a lot of data for a long time through VPN, a system administrator will usually detect it and try to ask this users (through is email) to stop. ▷ Personal data are also used for billing and anonymized statistics. ▷ Only a limited part of CN board members may access users' personal data. Each individual access is not logged.
CN France 2	▷ CN collects and stores users name, postal and email addresses, phone number, IBAN. Users do not have the power to modify personally this data. ▷ These information are associated with the IP address allocated to the user. ▷ CN gives users' address and phone number to other operator for interconnection matters (ex: Orange needs to know which line CN will use in order to give it access). However, CN fails to specifically inform users about such transfer. ▷ CN monitors how some of their services are used: if some is downloading a lot of data for a long time through VPN, a system administrator will usually detect it and try to ask this users (through is email) to stop. ▷ The bandwidth consumption of each user is logged: how much was used during each hour of the last day; during each day of the last month; during each month of the last year. ▷ This information is displayed on users personal page and system administrators may access it for debugging and monitoring. ▷ Personal data are also used for billing and anonymized stats ▷ Only a limited part of CN board members may access users' personal data. Each individual access is not logged.
CN Italy 1	▷ There is no real collection of data; who connects is not given any specific information. They must register their IP, however, or the network does not work (they cannot connect to the CN). ▷ There is a map server, publicly available on the website of the CN. On the map server one can see the nodes and each node has information attached (for instance IP addresses). ▷ Information is not necessarily real, but at least a valid e-mail address must exist. ▷ IP are not public; the internal network has a double addressing. There is a Wki with the ipv4. When a node is on it is possible to build a list of active node. ▷ Given that private and public addressed must be unique, the CN registers them there. ▷ Internal IP are always the same. They can be found on the website of the CN. ▷ No logs are saved.
CN Italy 2	▷ The Tos includes an informed consent to be signed by each member. ▷ A database includes members' personal information: name, surname, date of birth, tax code, home address and a copy of their identification document. The information is given by each member at the time of entering the association. ▷ Information can be updated at least every year when the annual association quota is paid. ▷ They collect this information only for maintenance reasons. ▷ They do have a map of the nodes but it is not public, it is used only internally by the administrators/representatives of the association/CN. ▷ Users can modify their information; each year they are asked to check whether their information is correct or must be updated. ▷ The CN applies a technical monitoring: for instance to understand how much band is used. ▷ The CN uses a "next generation firewall" (NGF), to detect and to stop the use of p2p.

Table 2.4: Processed data

CN France 1	▷ For Internet access and VPN, for the duration of the contract : name, addresses, IP addresses, phone number + for 1 year time of start and end of the connection ▷ For email, for 1 year, information logged by default by the software used on the email server: ▷ users' login ▷ email addresses of sender and receiver ▷ message size ▷ IP and time from where the user's box was accessed ▷ IP and time from where the user send the message ▷ For web hosting, for 1 year, information logged by default by the server software (Apache): ▷ IP address of each person accessing a page + which page is accessed, when ▷ For bittorent tracker for 1 year: login of the user uploading a .torrent file
CN France 2	▷ For Internet access and VPN, for the duration of the contract : name, addresses, IP addresses, phone number + for 1 year time of start and end of the connection ▷ For email, for 1 year, information logged by default by the software used on the email server: ▷ users' login ▷ email addresses of sender and receiver ▷ message size ▷ IP and time from where the user's box was accessed ▷ IP and time from where the user send the message ▷ For web hosting, for 1 year, information logged by default by the server software (Apache): ▷ IP address of each person accessing a page + which page is accessed, when
CN Italy 1	▷ Technical information is kept for technical reasons (maintenance). ▷ Only IP are stored, together with what is it written in the website of the CN (including home addresses) ▷ Except for the table including IP addresses, no other information is collected. There is only information on the node, to which an e-mail address is linked. The map servers is managed by 2 or 3 people from the CN. ▷ Only those 2 or 3 people can access and modify data. ▷ Only if users give their data and consent to their publication, this data is public. ▷ There is a mailing list and e-mail are retained. ▷ E-mail addresses are stored, but personal information do not need to be added. ▷ Only the addresses of the nodes are kept, to build the map of the network. ▷ This data is saved on servers owned by some users of the CN.
CN Italy 2	▷ The CN stores the internal IP connections (some IP are static, some dynamic) towards the Internet: logs: door, protocol, date and time. ▷ Personal information and technical information are kept on two different servers. ▷ Users' personal data are on a server which is located within the premises of the association; the premises are locked with a key. These servers are not connected to the Internet. Any information is backed-up daily. ▷ Personal data are kept to know who is member of the association; log and other technical information are kept for security reasons. ▷ They record any access to a service, but not its length. ▷ They store IP addresses and logs because they believe there are data retention obligations (decreto Pisanu); for no more than 6 months in case the police came.

Table 2.5: Data retention

2.4. Preliminary Results

The answers summarized in the table allow to draw some preliminary conclusions, although limited from the point of view of geographical distribution.

As for **civil liability**, three out of four CNs are organized as associations. This means that national laws would apply in case a civil wrongdoing happened. Normally, this entails that the president of the association will be responsible and liable for these wrongdoings. In the case of "CN Italy 2", also other people in charge of the association's obligations might be held liable, in case the wrongdoing happened as a consequence of their actions (for instance, a leakage of information is due to the lack of update of a software and the update was to be carried out by a specific person within the association). In the meantime, however, users – who are also members of the associations – sign a contract in which they bear the civil and criminal liability for wrongdoing committed by themselves or someone else using their login/password. They also commit themselves not to use p2p software, in order not to impair shared resources.

CN Italy 2 offers Internet to its subscribers; however it is not an IAP from a legal point of view. Hence, it cannot enjoy the liability limitations offered by art. 12, Dir. 2000/31 and its Italian correspondent art. 14, d.lgs. 70/2003. The opposite is true for the two French CNs that qualify as IAP and therefore can enjoy the liability limitations introduced by EU law.

In the case of "CN Italy 1" there is no legal entity behind the community; the community seems to be highly decentralized and with no person in charge of it. This would probably mean that in case of wrongful action no one could be held liable, unless everyone could be considered as a contributor to the wrongdoing. There is however the issue of shared connections. Although in the Italian context there is no liability for wi-fi sharing, the gateway user (that is, the user sharing their connection) might be contractually liable towards their IAP in case the contract forbids sharing the connection.

As for **data protection**, "CN France 1", "CN France 2" and "CN Italy 2" ask their users to sign Terms of Service (ToS) in which they also agree to the processing of personal data.

However, the information given to users is sometimes incomplete; for instance, in both French CNs the ToS do not specify all the kind of processing that are actually carried out. In the case of CN Italy 2, the information that the users have to sign is outdated, as it refers to a law (L. 31.12.1996, n. 675) that was repealed and substituted many years ago. In addition, no attention is paid to "sensitive data", although it could be part of what is stored – for instance – through the cloud service.

The French CNs collect and **retain personal data** for billing purposes. In the case of "CN Italy 2" data is also retained as a database of the association. Users can modify their data: for instance in "CN Italy 2" they can ask modification at any time and every year they are asked to confirm whether the information stored by the CN are still accurate. In the two French CNs users can access a personal page where they can modify their information.

All of the four interviewed CNs retain technical data to allow for maintenance; the data is retained to allow for security. In addition, the French CNs as well as "CN Italy 2" retain log data to comply with the national laws. In particular, the French CNs retain data for 1 year; the Italian one retains data for 6 months. This is in partial contrast with our findings of the first year, as according to the Italian legislation data should be retained for 1 year.

The same three CNs also monitor and retain some data in order to understand whether there are violation of the ToS, for instance whether there is P2P traffic.

2.5. Next Steps

The next steps involve the distribution of the survey amongst European CNs and their members. The survey will be circulated between M19-M21.

The collected answers will be the base for the final version of D4.2 due to at M24. D4.2 will in turn be the bases to draft some "Best practices guide for CNs" (T4.5-D4.5) at M36.

More precisely, next steps will include the following:

- circulate the survey, collect and analyse the answers in order to understand how CNs deal with legal obligations;
- based on these findings, write some guidelines adopting a user-friendly language; the aim of these guidelines will be twofold: first, they will help CNs dealing with existing obligations and legal hurdles; they could help to shape possible defenses in case of legal actions (4.2 - M24);
- by M30 the guidelines will be better defined, based also on some more feedback that will be asked to CNs;
- in the meantime, "Best practises for CNs" that would include legal, technical, governmental, economic and policy contribution will be developed, also thanks to a Booksprint[3], a week of residency gathering experts between M25 and M28 (depending on the project evolution to collaboratively develop a reader of technical, legal and other educational material). These best practises will be produced by M36.

[3] https://www.booksprints.net/

3. Advocacy Activities

3.1. Open letter to EU policy-makers

After discussion with European CNs, we decided to draft an open letter to EU policy-makers, illustrating "Policy recommendations for sustaining community networks" (see the related blog post - Appendix D)[1].

The letter was thought as a way to convey CNs' needs to EU policy-makers that in the past few months have been working on an overhaul of the telecommunications regulatory framework[2].

In particular, on September 14, 2016 the European Commission adopted set of initiatives and legislative proposals that will change the regulatory framework for electronic communications in the next few years. As above explained, the proposal for a Directive establishing the "**European Electronic Communications Code**" (EECC) will **merge four existing Directives** on telecommunications: Framework Directive (2002/21/EC); Authorisation Directive (2002/20/EC): Access Directive (2002/19/EC) and Universal Service Directive (2002/22/EC).

In addition, the EECC will affect **Spectrum Regulation**[3] and could affect **end-to-end encryption** for interpersonal communication, with a clear impact on privacy and personal data protection.

The letter was drafted in collaboration with several European CNs and advocacy groups and it was intended to offer a collective voice to this growing movement.

The content of the letter covered eight main issues, that can be summarized as follows:

1. **Lifting unnecessary regulatory and financial burdens**: we asked to review the regulatory framework and get rid of unnecessary regulatory burdens, such as fees or red-tape that are unnecessary or illegitimate when imposed on small non-profit entities. The proposed code for electronic communications should harmonize procedures for declaration fees (first registration) as well as administrative charges (annual fees). We asked EU lawmakers to ensure that the fees and charges imposed by any National Registration Authority (NRA) are null or negligible for non-profit ISPs and reasonable and proportionate for micro and small businesses.
2. **Getting rid of third-party liability when sharing Internet access**[4]: as above explained some countries' regulation prevent the sharing of Internet connections amongst several users by making people responsible (and potentially liable) for all communication made through their Wi-Fi connection. This is the case for instance of Germany and France. We asked EU policy-makers to abolish third-party liability for sharing Internet access and, in the same spirit, to prohibit contractual clauses that forbid subscribers to share their connection.
3. **Expanding the spectrum commons**[5]: currently Wi-Fi frequency bands are very limited. Not only are they getting increasingly subject to congestion in densely populated areas, they are also exposed to new technical standards that use the so-called ISM frequency band (like LTE-U) that hamper the reliability of Wi-Fi communications. In addition, existing frequency bands for Wi-Fi (5,6 Ghz and 2,4 Ghz) have physical constraints that prevent them for being used for longer radio links. We therefore requested the EU policy-maker to adopt a new approach to spectrum management through different actions: 1. expand unlicensed Wi-Fi bands; 2. make available other types of frequencies on unlicensed schemes or at least with affordable and flexible authorization schemes; 3. Include "white spaces" in lower frequencies

[1] http://netcommons.eu/?q=content/letter-eu-policy-makers-making-regulation-work-community-networks
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0590:FIN.
[3] Cf. D4.1 par. 2.6.4.
[4] Cf. D4.1 par. 3.2.1.
[5] Cf. D4.1 par. 2.2.

(which allow for cheap and resilient long-distance links), as well as the 12Ghz and the 60Ghz bands (for which radio equipment is affordable and which can help us build high-bandwidth point-to-point radio links).

4. **Updating open-access rules in telecom infrastructures**: Networks built with taxpayers money should also be treated as a commons and, as such, remain free from corporate capture. However, currently their management and exploitation is often delegated by public authorities to corporate network operators. These entities usually adopt aggressive pricing schemes that make it extremely costly for small access providers to interconnect with these networks. Access to these publicly-funded networks should be guaranteed at a reasonable and proportionate cost. Similarly, , in many European markets, the deployment of optical fibre networks is (re)creating monopolistic conditions on local loops through pricing schemes which preclude small actors from accessing these private networks.
5. **Protecting free software and user freedom in radio equipment**[6]: in 2014, the European Union adopted Directive 2014/53 on radio equipment [6]. Although the Directive pursues sound policy goals, it might actually impair the development of CNs. Indeed, they usually need to replace the software included by the manufacturer in radio hardware with free and open source software especially designed to suit their needs. Article 3.3(i) of the said Directive creates legal pressure for manufacturers of radio devices to ensure the compliance of the software loaded on these devices with the European regulatory framework. As a result, there is a strong incentive for manufacturers to lock down their devices and prevent third-party modifications of the hardware. We therefore asked policy-makers to consider a general exception for all free software installed on radio devices by end-users and operators, so that users' rights are safeguarded.
6. **Abrogating blanket data retention obligations**: Community networks strive to safeguard the right to privacy and the confidentiality of communication. Despite recent rulings by the Court of Justice of the European Union held that indiscriminate retention of metadata violates the Charter of Fundamental Rights (case *Tele2 v Post-och telestyrelsen*, December 21, 2016), some member states try to circumvent these rulings to protect capabilities for indiscriminate surveillance. As EU lawmakers start discussing the overhaul of the 2002/58 ePrivacy Directive[7], we called on them to oppose any blanket data retention obligations and close existing loopholes in EU law to ensure that only targeted and limited retention obligations can be imposed on providers.
7. **Bringing direct and targeted public support**: we called for an increase in actions supporting CNs at a various levels, for instance with small grants or subsidies, which could be used to buy – for instance – radio equipment. CNs have pioneered various models for the provision of free public access points; this could be of help in the WiFi4EU initiative. Local group applying a bottom-up logic can foster the empowerment of local communities and the cohesion of people, at the same time reaching the same policy-goals of mainstream operators but at a much smaller cost.
8. **Opening the policy-making process to Community Networks**: we asked national and European regulators to pay more attention to CNs activities when drafting regulations. CNs should be better and more represented in the policy-making process over broadband policy and other issues that may impact greatly on their development.

The letter was open for signatures both of CNs and of other supporting organizations during February and March 2017. More than 30 CNs and more than 40 organizations – including for instance EDRi, EFF, Free Software Foundation Europe – supported the letter (Appendix B).

On March 16, 2017 the letter was sent to EU institutions, in particular to members of the EU Parliament, national delegations at the Council of EU and to key officials from the EU Commission.

To allow a better understanding and a wider diffusion of the letter, it was translated into many European languages[8].

[6] Cf. D4.1 par. 2.3.
[7] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications
[8] https://wiki.laquadrature.net/Paquet_Telecom_2017/lettre_NetCommons

On the same day the letter was sent, there was also a joint press release to give to make the letter spreading widely.

The letter was also covered by news, as for instance on the Italian ANSA (Agenzia Nazionale Stampa Associata - National Agency Associated Press) website[9].

The letter is the first of several initiatives, including a policy workshop to be organized in Brussels at the European Parliament premises.

3.2. Notes on the European Electronic Communications Code

After sending the letter to the EU policy-makers, we started working more closely on the EECC.

Right after the aforementioned letter was sent to the EU policy-makers, on March 17th, the Industry committee of the European Parliament (ITRE) – responsible for assessing the proposed EECC – issued its draft report that contains the main amendments that will be discussed by the whole Parliament in few months.

Among other issues, the Code initially proposed by the European Commission would prevent small actors to participate in the investment of the network infrastructure, would extend to a minimum of 25 years the duration of the rights to use radio spectrum and would provide for unbalanced Universal Service obligations, making persons geographically isolated or in difficult situations into second-class citizens.

However, the draft report by ITRE proposes to extend to 30 years the duration of radio spectrum rights and to remove the initial provisions in favor of the open spectrum. Its sole merit is to remove the administrative fees for small operators.

netCommons published a blog post on this news (Appendix E)[10], making reference also to the advocacy actions adopted by the French activists of La Quadrature du Net[11].

The EU Parliament is going to decide on this Directive in the next two months. In particular, on June 22nd, the Consumer Protection Committee of the EU Parliament (IMCO) will adopt its report. Then, on July 11th, the Industry Committee of the EU Parliament (ITRE) will adopt its own report. The latter report will be adopted in plenary session and thus be the basis for negotiations between the rapporteur of ITRE and the Council of the EU.

In order to assist the Members of the Parliament of the EU to adopt a text of the directive that will take into account also the rights and needs of CNs and its users, we published a few notes that cover five distinct subjects (Appendix F)[12]:

1. **Enhancing data protection**
2. **Fostering the development of wireless community networks**
3. **Promoting a shared and unlicensed spectrum**
4. **Creating the appropriate conditions for small IAPs**
5. **Enhancing competition and addressing oligopolistic situations**

The notes (Appendix C) included the list of specific amendments tabled in IMCO and ITRE committees that could be in favour of European CNs and users and that could be against them.

For each amendment, the notes explain the reasons why that amendment should be adopted or rejected.

[9] www.ansa.it/sito/notizie/tecnologia/tlc/2017/04/10/tlc-le-reti-nascono-dal-basso_5ca15e80-a142-4c87-a34f-230dd770ca7f.html
[10] http://netcommons.eu/?q=content/draft-report-electronic-telecommunications-code-calls-immediate-action
[11] https://www.laquadrature.net/
[12] http://netcommons.eu/?q=content/notes-european-electronic-communications-code-decisive-votes-european-parliament

3.3. Workshop at the European Parliament

In the same spirit of the just described Notes and in the wake of the Open Letter to the EU policy-makers, we plan to organise a Workshop at the European Parliament.

The workshop is meant to be held in September or October 2017, as it will still be meaningful for influencing the legislative process of adoption of the EECC.

The workshop **aim** is in fact **threefold**:

- **contributing to the discussion on the Telecom Package**
- **conveying stakes for CNs in less technical terms**
- **supporting sustainable commons in telecom infrastructures**.

We contacted Members of the Parliament that are involved in the legislative process. The workshop will also rely on members of the "European Commons Assembly". In terms of organization, we would like to propose topics for panels, including participants from the European Parliament, from CNs, from academia and from regulatory authorities. The obtain the maximum impact, the would exploit a large network of researchers and research centers, as well as contacts with not-for-profit organizations and their contacts. A tentative program of the event, that would ideally last an entire afternoon, could be divided into two panels:

1st panel:

- overview of European CNs and of their achievements (*CNs representatives*)

2nd panel:

- introduction to the EECC (*by a Member of the Parliament*)
- overview of the issues faced by CNs in the current legal framework
  - telecommunications policy
  - personal data protection
  - civil liability
- Proposed amendments to the current draft of the Electronic Communications Code that could help CNs development
- Meaning and sustainability of CNsas "commons"

4. Preliminary Conclusions

From M13 to M18 the research carried out within WP4 has focused on two main goals: the first is to understand how the European legal framework for CNs is actually applied by the communities; the second is to influence the legislative process leading to the adoption of an Electronic Communications Code at the European Union level.

To achieve the first aim, we conducted some face-to-face interviews, the answers of which are above summarized. The same answers also allowed us to draft a questionnaire that will be distributed in the next weeks in order to collect information by as many CNs as possible on the way they deal with legal obligation in everyday life.

As for the second goal, an open letter to EU policy-makers was drafted and circulated amongst CNsfor signatures. After collecting a meaningful number of signatures, the letter was sent to the institutions involved.

Currently a workshop at the European Parliament in Brussels is being organized. The aim of the workshop is – as it was for the notes published on the netCommons blog – to raise awareness of the existence of CNs and of their needs and to influence the legislative process of the Electronic Communications Code in order to make it more suitable for the sustainability and growth of CNs.

Bibliography

[1] M. Dulong de Rosnay, F. Giovanella, A. Messaud, and F. Tréguer, "European Legal Framework for CNs," netCommons Deliverable D4.1, Dec. 2016. http://netcommons.eu/?q=content/european-legal-framework-cns-v1

[2] "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 ('Directive on electronic commerce')," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML.

[3] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=IT.

[4] "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=en.

[5] R. Lo Cigno, R. Guidolin, R. Caso, and M. Dulong de Rosnay, "Ethics Requirements," netCommons Deliverable D8.1 (Confidential), May 2017.

[6] "Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC," http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0053&from=IT.

A. Annex 1

Questionnaire on Legal obligations of Community Networks

netCommons is a research project supported by the European Commission (2016-2018), which proposes a trans-disciplinary methodology to study and support the development of local network internet infrastructures as commons, for resiliency, sustainability, democracy, privacy, self-determination, and social integration.

It published a report investigating the applicability to Community Networks (CNs) of the current European legal framework for liability, privacy and personal data protection. It is now assessing how this legal framework may actually conflict with concrete activities of CNs. For this purpose, we would like to ask you some questions about the organisation and activities of the CN you are part of.

We are aware that some of the questions may involve sensitive issues, for instance with regard to activities which might be illegal in your own country.
To avoid exposing your CN to negative consequences, we will anonymise each questionnaire once received it. In addition, in our report based on the questionnaire, we will not mention specifically what CN the answers refer to.
Answers to the questionnaire will be stored on data centres protected with strong authentication measures.

Please answer each question within the frame below it. The size of each frame intends to help you assess the length of the answers we expect, but feel free to provide shorter or longer ones.
Although the questionnaire is in English, in case you feel more comfortable answering in your own language, feel free to do so.

Please consider that while answering this questionnaire you consent to share your answers with netCommons researchers that will treat your information according to the ethical standards of research and protect it as just explained.

Services provided

- About the network access provided by your CN:

- How is this access technically provided (examples: through cables, Wi-Fi, VPN)?

- Is it provided against payment?

- Is this provision limited in any other way (examples: to members of an association, to adults, to low-income individuals)?

- Is the network connected to the Internet?

- What other services is your CN providing (examples: email, chat, VoIP, VPN, DNS, hosting, torrent tracker, mailing list, Tor node)? Indicate which services are provided against payment or which provision is limited in any other way (examples: to members of an association, to adults).

Organization

- Is a legal entity playing a central role within your CN and, if so, how is this entity organized (example: as an association, foundation or co-operative)?

- Where such a central entity exists:

  - Is this central entity providing the services on its own (through its employees or members) or are the services provided by external, individual participants (not acting on behalf on the central entity)?

  - Where services are provided by individual participants:

    - What is the role of the central entity?

- Who is actually deciding which services are provided by the CN: the central entity (by a vote of its members, for instance) or individual participants?

- Who is actually defining the technical implementation of the services: the central entity or individual participants?

- Where services are provided by individual participants (whether a central entity exists or not):
  - Do participants have to enter into any kind of agreement with each other and/or with a legal entity? If so, how does this agreement distribute obligations and liabilities among them?

- Where decisions are made by individual participants (whether a central entity exists or not):
  - How are these decisions taken (examples: through a collective and horizontal process or independently by each participant)?

In the following questions, the term "CN" refers to the community which provides the services, no matter how this community is organized.

Decentralized wireless network

Answer the following questions if your CN runs a network of wireless relays managed by individual participants (not acting on behalf of a central legal entity).

- Who does legally own the relays (individual participants or a central entity)?

- Who is technically managing the relays (individual participants or a central entity)?

- Is running a relay limited in any way (examples: by joining an association or entering into a contract; in the latter case, describe the content of this contract)?

Liability for users' behavior

- Do CN members apply anonymity software?

- Has it ever occurred in your CN that someone was sued for some wrongdoing (examples: defamation, copyright infringement)?

- Has your CN a form of insurance (examples: real insurance or a 'self-organized'-internal one)?

Personal data

- Indicate below the categories of data collected by your CN about its users.

For each category of data, indicate the purpose(s) for which they are collected and used (examples: email addresses are collected in order to contact users in case of security issues and to send them newsletters; MAC addresses are collected in order to provide and maintain access to the network). Where the purpose of collecting data is to comply with a legal obligation, describe the nature and basis of this obligation (example: the name of users accessing the network is collected in order to "protect" the network from unlawful activities, as provided by a specific law).

  - Data that may allow the identification of users (examples: name, postal and email addresses, birth date):

- Data that have been assigned by the CN to users (examples: IP address, phone number, user ID):

- Data relating to the characteristics of the device through which the service is accessed (examples: MAC address, IMSI):

- Data relating to the characteristics of the line through which the service is accessed (examples: lines ID, postal address):

- Data that may indicate the time and duration of access to a service (example: DHCP operations):

- Data relating to the location where the service is accessed (examples: relays ID, postal address):

- Data that may allow the identification of the recipients of communications (example: their email address and phone number) or of the content accessed (example: URLs of accessed websites):

- Banking information (example: IBAN):

- Which kind of data are associated together, kept separately or anonymised, and how (example: IP addresses are associated with users' names in a central database)?

- Is your CN disclosing data to third parties (example: the postal address of users is disclosed to third party operators for interconnection matters)?

- Is your CN transferring data outside the European Union (example: through a VPN) and, if so, to which countries?

- Is your CN monitoring in any way how users are using the services and, if so, for what purpose(s) (examples: for payment or security issues)?

- As regards decentralized wireless network managed by individual participants:

  - What kind of data is your CN collecting or using about the participants (examples: contact information, location and technical characteristics of their relay)? For each kind of data, indicate the purpose(s) for which they are collected (example: for publishing a node-map).

Relationship with users

- Is your CN entering into a contract or any kind of agreement with each of its users? If so, please attach to your answer a copy of this agreement.

- What kind of information is your CN providing its users with as regards the collect and use of personal data (examples: they are informed that their name is associated with their IP address or that their postal address is disclosed to third party operators)?

- How are users provided with such information (example: on a website, within a contract)?

- How can users access their personal data and ask for their rectification or erasure (example: on a "user page" of your CN's website)?

- If any, what kind of personal data is your CN refraining from collecting or using without the consent of users? How is this consent given?

- As regards decentralized wireless network managed by individual participants:
  - How are participants informed of the use of their personal data? How may they access and modify their personal data? When is their consent required?

Security

- Technically, how and where are the personal data processed by your CN stored?

- What measure has your CN implemented in order to protect the data (examples: personal data can only be accessed by a limited number of individuals and each access is logged)?

- Has any kind of security breach ever affected your CN? If so, describe it. Was it notified to authorities and users?

Data retention

Answer the following questions if your CN is retaining data in order to comply with national law.

- Indicate which categories of data are retained (note that you should have already listed them with the personal data collected by your CN; if not, please complete your previous answers):

- Where, by whom and for how long are the retained data stored?

- Have authorities ever requested your CN to give them access to such data? If yes, how many times, concerning what categories of data and for what purposes? Was your CN able to comply?

Thank you for your answers!

B. Annex 2

POLICY RECOMMENDATIONS FOR SUSTAINING COMMUNITY NETWORKS

OPEN LETTER TO EU POLICY-MAKERS
POLICY RECOMMENDATIONS FOR SUSTAINING COMMUNITY NETWORKS

PREAMBLE

We represent European Community Networks, a growing movement of organizations that operate local communication infrastructures, sometimes federated at the regional or national levels. These networks, most of which also provide access to the global Internet, are operated as a commons. That is, rather than being driven by for-profit motives, our key focus is on providing connectivity while striving for democratic governance, social inclusion, education, and human rights with respect to communication technologies.

Our organizations vary considerably in terms of sizes, types of network infrastructures and political cultures. Yet, despite this diversity, we are united by the common objective to build networks that meet the communication needs of humans (rather than those of objects and machines), through networks that are built and run by our communities, for our communities, focused on local empowerment, affordability and resiliency.

Today, we collectively provide broadband connectivity not only to tens of thousands of individual European citizens and residents in rural or urban settings, but also to organizations including small and medium sized companies, schools, healthcare centers, social projects and many more. In many cases, we have out-competed mainstream operators, by providing cheaper and faster Internet connectivity than incumbent players. Thanks to our infrastructures and through our various activities, we foster scientific and engineering experiments, we help local hosting and service providers come together to mutualise investments and share costs, we support digital literacy and data sovereignty through workshops and other educational activities.

Yet, despite our achievements, policy-makers at the national and European levels have so far mostly neglected our existence and specific regulatory needs. Worse, regulation is often hampering our initiatives, making the work of our participants and volunteers harder than it should be. This is why, as you start working on a European code of electronic communications, we decided to contact you and voice our ideas and recommendations regarding the future of the legal and policy framework regulating our activities.

1. Lifting unnecessary regulatory and financial burdens

We first ask you to review the regulatory framework and get rid of unnecessary regulatory burdens, such as fees or red-tape that are unnecessary or illegitimate when imposed on small non-profit entities. In Belgium for instance, the registration fee that telecom operators must pay to the NRA is at 676€ for the first registration, plus 557€ every following year (for those whose revenues are below 1M€, which is the case for many community networks).

Even such small fees can hinder the growth of small networks that efficiently serve tens of households. In France, Spain and Germany, it is free, which might explain why the community networkmovement is much more dynamic in these countries. The proposed code for electronic communications aims to harmonize procedures for declaration fees (first registration) as well as administrative charges (annual fees). EU lawmakers must ensure that the fees and charges imposed by national NRAs are null or negligible for non-profit ISPs and reasonable and proportionate for micro and small businesses. Likewise, taxes designed for large corporate firms in the telecom sectors should not apply to smaller, non-profit operators.

2. Getting rid of third-party liability when sharing Internet access
Several laws seek to prevent the sharing of Internet connections amongst several users by making people responsible (and potentially liable) for all communication made through their Wi-Fi connection, and create legal risks for people sharing their connection. In Germany, rights-holders have used a "secondary liability" doctrine to chill the growth of the community networks movement. In France too, copyright law imposes a secondary liability regime that creates significant legal uncertainty for people sharing their network connections with other users. The so-called "mere conduit", inscribed in EU law since 2000 in the directive on information society services, needs to be guaranteed and expanded to small-area wireless access points. In the same spirit, contract clauses that forbid subscribers to share their connections with others should be prohibited. Promoting a right to share Internet connections is all the more vital considering the economic and ecological crises, as well as the rapid increase of populations that cannot afford access to the Internet. In this context, connection sharing can play a critical role in fostering a more equitable and sustainable use of telecommunications infrastructure.

3. Expanding the spectrum commons
It is not just Internet wireless access points that can be shared, but also the intangible infrastructure on which radio signals travel. Wi-Fi, as an unlicensed portion of the spectrum and therefore a commons, is a key asset for community networks willing to set up affordable and flexible last-mile infrastructure. However, these Wi-Fi frequency bands are currently very limited. Not only are they getting increasingly subject to congestion in densely populated areas, they are also exposed to new technical standards that use the so-called ISM frequency band (like LTE-U) that hamper the reliability of Wi-Fi communications. Last but not least, existing frequency bands for Wi-Fi (5,6 Ghz and 2,4 Ghz) have physical constraints that prevent them for being used for longer radio links. In the face of such challenges, a new approach to spectrum policy is needed. Policy-makers should expand unlicensed Wi-Fi bands. Other types of frequencies should also be made available either on an unlicensed (preferred scenario) or, if not possible, based on affordable and flexible authorization schemes. Such frequency bands for instance include so-called white spaces in lower frequencies (which allow for cheap and resilient long-distance links), as well as the 12Ghz and the 60Ghz bands (for which radio equipment is affordable and which can help us build high-bandwidth point-to-point radio links). Once made accessible to community networks, they can help roll-out and expand cheap and resilient wireless infrastructures.

4. Updating open-access rules in telecom infrastructures
Networks built with taxpayers money should also be treated as a commons and, as such, remain free from corporate capture. Today, their management and exploitation is often delegated by public authorities to corporate network operators. These entities usually adopt aggressive pricing schemes designed for incumbent players that make it extremely costly for small access providers to interconnect with these networks. Access to these publicly-funded networks for non-profit entities like community networks as well as small businesses should be guaranteed, at a reasonable and proportionate cost. Similarly,

community networks often cannot have access to the private local infrastructures of incumbent players, despite the fact that these are the only way to connect willing subscribers. Indeed, in many European markets, the deployment of optical fiber networks is (re)creating monopolistic conditions on local loops through pricing schemes which preclude small actors from accessing these private networks. Policy-makers and regulators should ensure that every area is covered by at least one telecom operator with a so-called "bitstream" offer affordable for smaller players.

5. Protecting free software and user freedom in radio equipment
In 2014, the European Union adopted Directive 2014/53 on radio equipment. Although the Directive pursues sound policy goals, it might actually impair the development of community networks. Indeed, community networks usually need to replace the software included by the manufacturer in radio hardware with free and open source software especially designed to suit their needs, a collective process that improves security and encourages the recycling of hardware, among other benefits. Article 3.3(i) of the said Directive creates legal pressure for manufacturers of radio devices to ensure the compliance of the software loaded on these devices with the European regulatory framework. As a result, there is a strong incentive for manufacturers to lock down their devices and prevent third-party modifications of the hardware. We therefore ask policy-makers to provide a general exception for all free software installed on radio devices by end-users and operators (the latter being liable if their software lead to violations of the regulatory framework), so that users' rights are safeguarded.

6. Abrogating blanket data retention obligations
Community networks strive to safeguard human rights in communication networks, and in particular the right to privacy and the confidentiality of communication. While we welcome recent rulings by the Court of Justice of the European Union holding that indiscriminate retention of metadata violates the Charter of Fundamental Rights, we are concerned about several member states' willingness to circumvent these rulings to protect capabilities for indiscriminate surveillance. As EU lawmakers start discussing the overhaul of the ePrivacy Directive, we call on them to oppose any blanket data retention obligations and close existing loopholes in EU law to ensure that only targeted and limited retention obligations can be imposed on hosting and access providers.

7. Bringing direct and targeted public support
Countless other policy initiatives can help support community networks and the significant associated benefits they bring. Such policies include small grants, crowd-funding and subsidies to help our groups buy servers and radio equipment, communicate around their initiative, giving them access to public infrastructures (for instance, the roof of a public building to install an antenna), but also to support their research on radio transmission, routing methods, software or encryption. As many local authorities have found, supporting community networks is a sound policy option. As EU lawmakers move forward on the WiFi4EU initiative, we would like to remind you that we have pioneered various models for the provision of free public access points. We believe that public money invested in this initiative should primarily go to groups pursuing a bottom-up logic, seeding local groups that can foster the empowerment and cohesion of local communities, nurture competition, and meet the same policy-objectives at a fraction of the cost that would be charged by mainstream telecom operators.

8. Opening the policy-making process to Community Networks

Although we have often partnered with municipalities and local public authorities, we ask that national and European regulators pay more attention to our activities when drafting regulation. Community networks have both the expertise and legitimacy to take an integral part in technical and legal debates over broadband policy in which traditional, commercial ISPs are over-represented. Community networks can bring an informed view to these debates, allowing for a policy-making process more attuned to the public interest.

We thank you for your attention and very much look forward to engaging with you on these important issues,

First signatories (EU-based community networks)
020wireless (Netherlands)
AIL-Network (France)
Alsace Réseau Neutre (France)
Aquilenet (France)
Association Ribaguifi - Eresué 2.0 (Spain)
Asoc. SevillaGuifi (Spain)
Common Net (Italy)
FAImaison (France)
FDN (France)
FFDN (France)
Franciliens.net (France)
Freifunk.net (Germany)
Fundació guifi.net (Spain)
Funkfeuer (Austria)
Grenode (France)
Grifon (France)
Ilico (France)
Illyse (France)
Iloth (France)
Neutrinet (Belgium)
Ninux.org (Italy)
Open Network in Croatia (Croatia)
Progetto Neco (Italy)
Progetto Wireco Ciminna (Italy)
Rézine (France)
Sarantaporo.gr NPO (Greece)
SCANI (France)
Tetaneutral.net (France)
Tourraine Data Network (France)
Wireless België (Belgium)
Wireless Leiden (Netherlands)
WirelessPT.net (Portugal)
Wlan slovenija (Slovenia)

Supporting organizations (signing in support of the general approach and/or specific proposals put forward in the letter)
ApTI (Romania)
ARTICLE 19 (UK)
Bits of Freedom (Netherlands)
BlueLink.net - Civic Action Network (Bulgaria)
Brazilian Association of Digital Radio (Brazil)
Chaos Computer Club (Germany)
Chaos Computer Club Lëtzebuerg (Luxemburg)

Colnodo (Colombia)
Common Ground (Germany)
Commons Network (EU)
Dugnadsnett (Norway)
EDRi (EU)
EFF (US)
Electronic Frontier Norway (Norway)
epicenter.works (Austria)
Free Knowledge Institute (Netherlands)
Free Software Foundation Europe (EU)
Frënn vun der Ënn (Luxemburg)
GreenNet (UK)
hackAIR (EU)
Initiative für Netzfreiheit (Austria)
Instituto Bem Estar Brasi (Brazil)
Instituto Nupef (Brazil)
La Quadrature du Net (France)
MAZI (EU)
netCommons (EU)
netHood (Switzerland)
Network Bogotá (Colombia)
NEXTLEAP (EU)
NURPA (Belgium)
Nuvem (Brazil)
One World Platform (Bosnia Herzegovina)
Open Rights Group (UK)
Open Technologies Alliance- GFOSS (Greece)
P2P Foundation (Netherlands)
P2P Lab (Greece)
PIE News Project (EU)
Project Arig (Israel)
Rhizomatica (Mexico)
Renewable Freedom Foundation (Germany)
VECAM (France)
Xnet (Spain)
Zenzeleni Networks (South Africa)

C. Annex 3

Notes on the European Electronic Communications Code

1. Enhancing data protection

Articles 40, 93

Data protection, a core value of Community Networks (CNs)

In Europe, Community Networks (CNs) are a growing movement of organizations that operate local communication infrastructures, sometimes federated at the regional or national levels. These networks, most of which also provide access to the global Internet, are operated as a commons. That is, rather than being driven by for-profit motives, their key focus is on providing connectivity while striving for democratic governance, social inclusion, education, and human rights with respect to communication technologies.

As such, one of their core values is to protect the privacy of their users and not to process their personal data for business purpose or any other purpose not necessary for the provision of their services.

Obstacles faced by community networks

Governments of numerous Member States intend to abolish users' freedom to encrypt their communications. Furthermore, they have lately adopted several laws strengthening the powers of intelligence services to intercept communications and to monitor networks for purposes such as protecting national economical health or the detection of minor crimes or simple misconducts.

In the same spirit, and in breach of the Charter of Fundamental Rights (as clearly interpreted last winter by the Court of Justice of the European Union in its Tele2 case), many Member States are refusing to revoke or review their national laws which require telecommunication operators to retain traffic data of all their subscribers.

All of these issues directly and drastically impact CNs' activities, by preventing them from implementing policies that fulfill one of their core social values.

Amendments

IMCO

Amendments **377 and 378 should be adopted** as they would make end-to-end encryption mandatory for interpersonal communication service providers (such as mail and chat).

Amendment **530 should be adopted** as it would explicitly force Member States to comply with the Tele2 case of the European Court of Justice.

ITRE

Amendments **565, 566, 567 and 568 should be adopted** as they would make end-to-end encryption mandatory for providers of interpersonal communication services.

Amendment **1099 should be adopted** as it would provide a framework anchored in fundamental rights for the interception of communications by competent national authorities.

2. Fostering the development of wireless community networks

Articles 2, 55, 95

Freifunk, a wireless community network

Freifunk is a German community network whose members are single-handedly installing and maintaining free networks, using their own Freifunk firmware on off-the-shelf wireless (WiFi) devices and routers. Every member of the network configures his or her router to relay the traffic of other participants to the Freifunk network. In return, he or she can also transmit data, such as text, music and movies through the network or use services setup by participants. Many members also share their Internet access and allow others to use it to access the World Wide Web and other internet services.

In 2013, there were 40.000 Freifunk relays all over Germany and neighbouring countries and, given the coverage achieved in Berlin, more than 350,000 people can have access to the network. Since the provision of free Internet for all is part of Freifunk core identity, its network is essential for many communities, such as underprivileged individuals.

Finally, based on user-driven networks, services and usages, Freifunk depends on perpetual innovation through, for instance, the development of new communication protocols that any other operators or companies may freely used to provide innovative services all over the EU.

Obstacles faced by Freifunk

Several national laws seek to prevent the sharing of Internet connections amongst several users by making people liable for all the communications made through their Wi-Fi connection. In 2017, two German courts have found individuals sharing their Wi-Fi connection liable for copyright infringements committed by other users. They were found liable because, despite having been warned by rights-holders about such infringements, they did not take measures to stop those infringements and to prevent new ones.

Such liability is a major threat for Freifunk members and a clear distortion of competition since 'traditional' Internet access providers cannot be liable for infringements committed by their users, even if they are aware of them, as provided by article 12 of Directive 2000/31/EC ('Directive on electronic commerce').

Furthermore, while they do not benefit from the same liability regime as professional providers, CNs are subject to the same strict obligations. Some of these obligations are clearly unjustified and disproportionate where imposed on individuals.

Finally, two practical obstacles may prevent individuals from sharing their Internet connection. Firstly, router manufacturers may prevent users from loading into their devices customized software necessary for maintaining free and open wireless networks (such as those developed by Freifunk). Users' ability to use Free Software in order to regain control over their devices is also threatened by ambiguous language in the Directive 2014/53 on radio equipment. Secondly, Internet access contracts may directly forbid subscribers to share their connections with others, or charge them for doing so.

Amendments

Article 55 of the proposed Code intends to foster the development of wireless community networks but fails to address the obstacles underlined above.

IMCO

Amendment **68 should be rejected** as it would hinder the development of community networks by making the community liable for the actions carried-out by end-users.

Amendments **408 and 409 should be adopted** as they would explicitly extend the protective liability regime of Internet access providers to individuals sharing their Wi-Fi connection.

Amendment **411 should be adopted** as it would allow members of Community Networks to install Free Software (software that can be freely used, studied, modified and shared as such) onto their wireless devices, which is a prerequisite and standard practice in wireless networks.

Amendment **566 should be rejected** as it would have the opposite effect.

ITRE

Amendments **298**, **316 and 333 should be adopted** as they would exclude individuals sharing their Wi-Fi connection from the scope of obligations imposed on professional providers, thereby fostering the development of wireless community networks.

Amendments **702**, **703 and 706 should be adopted** as they would explicitly extend the protective liability regime of Internet access providers to individuals sharing their Wi-Fi connection.

Amendments **708 and 710 should be rejected** as they would remove the provisions giving end-users the rights to access wireless networks of their choice and to share their own access with other uses.

Amendments **712 and 713 should be adopted** as they would not allow Internet access provider to charge users in case they want to share their Wi-Fi connection.

3. Promoting a shared and unlicenced spectrum

Articles 4, 18, 45, 46, 49

Tetaneutral, a not-for-profit Internet service provider

Tetaneutral is a not-for-profit French Internet service provider that provides connectivity for everyone, including digital exclusion areas. While fibre optic networks are costly, wireless networks are a flexible and affordable way to provide broadband wireless network to all citizens.

Through WiFi unlicensed spectrum, Tetaneutral is able to deliver symmetrical very high capacity network (up to 30 megabytes) in all areas, including where fiber is not deployed. It is a key enabler that supports the digital uptake in rural areas and spreads digital literacy. It involves users in the deployment of the network and thus empowers citizens in both urban and rural zones. To that extent, bringing connectivity to everyone crucially depends on wireless unlicenced spectrum.

Obstacles faced by Tetaneutral

The lack of shared (through flexible authorisation schemes) and unlicenced spectrum is an obstacle for deploying community networks. Deployment of 4G and 5G should not be an excuse to reduce or even slow the release of shared and unlicenced spectrum (supported by the European Commission), which embodies the core principle of general authorisation mechanism enshrined since 2002 in the current telecoms package. To prevent the often exagerrated risk of congestion, technical harmonisation within the EU should ensure the coexistence of both spectrum licensed through individual rights and of free spectrum.

Besides, the duration of rights to use radio spectrum shall be limited and subject to regular review in order to assess the efficiency of the use of spectrum in light of technological and market evolution, and ensure that spectrum policy continues to serve the public interest. Authorisations should be withdrawn if necessary and National Regulatory Authorities (NRAs) have appropriate powers to carry out such assessments.

Amendments

ITRE

Amendment **393 should be rejected** as it aims at reducing the obligations of the Member States to develop the shared and unlicenced spectrum.

Amendment **420 should be rejected** as it aims at limiting the possibilities for Member States to add amendments to spectrum usage plan.

Amendment **603 should be adopted** as a solution for increasing the access to shared and unlicenced spectrum.

Amendments **636 and 645 should be rejected** as they would increase the number of cases where authorisations to use radio spectrum are needed, which is not an efficient way to foster innovation but would on the contrary add constraints.

Amendments **670 and 674 should be adopted** as they would enable regular reviews of the authorisations to use radio spectrum.

4. Creating the appropriate conditions for small Internet service providers

Articles 59, 70, 71, 72

French Data Network, a not-for-profit Internet service provider

French Data Network (FDN) is the oldest French Internet service provider (ISP) still operatingI It exists since 1992.

FDN provides hundreds of subscribers with services that major French ISPs do not offer: it systematically provides static IP addresses (a critical condition for self-hosting), refrains from monitoring the behaviour of its users for any commercial purpose and guarantees the neutrality of its network far beyond what is imposed by the Open Internet Regulation.
FDN is a non-profit entity: it provides access to the Internet against payment, but its revenues are entirely dedicated to the development of its network and services. Its governance is open to anyone.

Obstacles faced by FDN

As most landine ISPs, FDN has not enough funding to deploy its own cables. It has to rent access to the wired network of big operators in order to provide users with its enhanced services. It may rent two kinds of access: passive and active.

Passive access means that a provider actually rents physical cables, installs its own equipment on the network and manages every technical aspect of the access provided to users. It is usually expensive since ISPs have to rent space in each local infrastructure (thousands of euros per month for each) in order to install their equipment. Thus, passive access is more suited for providing Internet access to many users in the same area or to companies with very specific needs.

Active (also called “bitstream”) access means to simply use part of a network already managed by another operator. It does not require to install equipment nor to rent space. It is much cheaper and adapted for providing Internet access to fewer users in each location. It does not give as much control as passive access but still allows ISPs such as FDN to provide the services their members and subscribers are looking for.

Regarding ADSL lines, operators are obliged to grant passive and active access to ISPs requesting so. Therefore, there are now thousands of ISPs in France that provide customized and enhanced services to individuals or SMEs through the ADSL infrastructure of a few big operators.

However, this situation is limited to ADSL: operators are free not to grant access to their fibre-optic lines at all. Since FDN and most ISPs are not in a position to deploy their own lines (nor participate in the deployment of fibre lines), they simply cannot and do not offer any fibre access to end-users.

This impedes competition drastically, limits the diversity and the quality of services provided to SMEs and individuals and is destroying the pre-existent economic fabric of small ISPs used to work with companies. Now, these companies may only rely on the four big French ISPs which are unable to provide them with services specifically fitting their needs.

Amendments

Article **59** (symmetric regulation), **70** (access to civil engineering), **71** (general access including active) of the proposed Code intend to create obligations to grant access (active and passive) at relevant cost (article **72**) but fails to address efficiently the obstacles underlined above.

ITRE

The following amendments **should be adopted** as they would strengthen operators' obligations to grant access and NRAs' power to order them to do so: **737, 738, 743, 745, 748-752, 757, 905, 907, 908, 909, 912, 939, 940, 948, 953, 954, 959, 965-970, 974, 976, 977, 979, 980**.

The following amendments **should be rejected** as they would have the opposite effect: **735, 746, 747, 889, 893, 894-900, 906, 913, 918, 924-926, 932-937, 943, 971, 984**.

Amendments **917 and 923 should be adopted** as they would specifically ensure that active access is not relegated to a minor role compared to passive access.

The following amendments **should be rejected** as they would have the opposite effects: **739, 740, 741, 742, 880, 930, 931**.

5. Enhancing competition and addressing oligopolistic situations

Articles 61, 65, 71, 72, 74, 77

Federation FDN, a federation of not-for-profit ISPs

The Federation FDN gathers 26 not-for-profit Internet service providers in France and Belgium. Some rely on bitstream access provided by incumbent players. Others create their own fiber-optic or wireless networks in both urban and rural settings, in many cases bringing connectibity to "white zones".

Obstacles faced by Federation FDN

In France, more than 1000 operators are on the ADSL market, offering connection to both individuals or companies. To some extent, this allows competition between a variety of actors, and can ensure the possibility for users to choose between several offers. While ensuring competition at a retail level, such providers also stimulate competition on wholesale markets.

But the situation on the fiber-optic local loop is very worrying: only four operators are developing this kind of infrastructures in France, which cannot be considered as the same competition conditions as for the ADSL market. Furthermore, operators are often alone in a specific area, which leads to a monopolistic situation from the end-users point of view, as they cannot choose between several operators. The root cause is that there is currently no bitstream offers allowing smaller operators or Community Networks (CNs) to use the infrastructure of the dominant players to provide their services to end-users. This situation brings national markets back to the early days of European regulation where single dominance is the rule but with several players theoretically active. Deprived of the proper regulatory incentive to remedy this situation, NRAs are not taking the necessary steps to ensure competition.

To solve these issues, the definition of "significant market power" (SMP) should be broadened, so as to include all operators having a position equivalent to dominance, including through a commercial or co-investment agreement, and be subject to an asymmetric regulation. This would ensure competition in the face of oligopolistic situations.

Also, smaller operators or Community Networks need more flexibility and less administrative burden, such as analysed by the Federation FDN within its answer to the French consultation on the land-line market (www.ffdn.org/en/node/129). Community networks (CN) can be a solution for non competitive markets in bringing connectivity over the territory, such as observed in the scandinavian countries (https://openmedia.org/en/access-success-nordic-countries-0).

Regulatory holidays (art 74-77), limitations to symmetrical regulation (art 59.2) and amendments going further in this direction will inevitably lead to duopolistic and non-competitive situations Thanks to access regulation, this is precisley what we have so far avoided in Europe. As the political economy of networks further concentrates, if CN are not supported (notably through bitstream access) we will step back from this situation.

Amendments

IMCO

Amendment **436 should be adopted** as it deletes the provision on article 72 that would reduce the NRA regulation powers depending on the investments. The role of NRAs is not only to secure the investments of operators but to ensure a harmonious development of faster and affordable networks across territories.

Amendment **440 should be rejected** as it aims to put the burden of proof on NRAs when they aim at regulating costs and tariffs. Due to classical asymmetry of information issues, NRAs cannot face such a burden and would deprive them of the capacity to regulate tariffs even when reasonable and not cost oriented.

Amendment **441 should be rejected** as it aims to remove any transparency related to cost accounting system. Again, transparency is crucial when related to cost-regulation. Cross susbidies issues could not be properly addressed under such circumstances.

Amendment **442 should be adopted** as it gives back to NRAs the capacity to appreciate how much New Network Elements shall be subject to regulation. On the contrary, automatic and potentially temporary deregulation would greatly disturb the market and impede competition.

Amendment **444 should be rejected** as it worsens the European Commission's proposals by letting monopolistic players unregulated.

Amendment **448 should be rejected** as it aims to put at the same regulatory level any kind of agreements among market players, and would lead without any control mechanism to raise barriers to market entry for any operators that are not part of such agreements.

Amendment **449 should be adopted** as it clarifies that co-investment agreement must have been concluded in order to be taken into account by NRAs. Assessing a mere co-investment offer is not enough to allow NRA to play its role and ensure a proper competitive dynamic.

ITRE

Amendments **793, 794, 800 and 818 should be adopted** as they would also enhance the definition of SMP and remove provisions that weaken the SMP regime.

Amendment **971 should be rejected** as it aims at securing the network investments by operators whereas the role of NRAs is to ensure a harmonious development in the territories and give to all equal access to the market and services.

Amendment **973 should be rejected** as it would worsen the oligopolisation of fiber-optic networks and thus worsen the distortion of competition. This amendment gives operators more possibilities to exclude competitors either by increasing prices or discriminating the undertakings.

Amendment **1045 should be adopted** as it removes article 77 that imposes less obligations to vertically separate undertakings. As it stands, this article would leave monopolistic players unregulated.

Amendment **1130 should be adopted** as it would enable local ISPs to participate in the investments and thus enhance connectivity and competition at the local level.

About netCommons

netCommons is a Horizon2020 research project supported by the European Commission (2016-2018), which proposes a trans-disciplinary methodology to study and support the development of local network internet infrastructures as commons, for resiliency, sustainability, democracy, privacy, self-determination, and social integration.

netCommons is participated by 4 universities, one research center and one ONG (UniTn, UPC, AUEB-RC, UOW, CNRS and Nethood, respectively from Italy, Spain, Greece, UK, France and Switzerland). The consortium brings together research groups and institutions in the area of “networks” and collaborative platforms with expertise in engineering, computer science, economics, law, political science, interdisciplinary research.

netCommons aims to help existing community networks like guifi.net and ninux.net, to grow and replicate in more European cities and rural areas. To become more extrovert, more inclusive, and better understood by the wider population. To empower them to form both a means for equitable and affordable access to the Internet and community-owned infrastructures for the provision of local services.

D. Annex 4

netCommons

THE PROJECT GET IN TOUCH MEDIA RESULTS

Letter to EU Policy-Makers: Making Regulation Work for Community Networks

SUBMITTED BY MELANIE ON FEBRUARY 21, 2017 - 1:48PM

UPDATE: *The consultation is now closed and a joint press release is published on March 16th, 2017. Help us to spread the word!*

After many discussions with many European Community Networks (CNs), researchers from netCommons are happy to present a draft open letter on "policy recommendations for sustaining Community Networks".

The letter is targeted at European policy-makers, who recently started working on an overhaul of the telecom regulatory framework. It is drafted in collaboration with several European CNs and advocacy groups and is meant to offer a collective voice to this growing movement.

Until March 15th, we would like to collect signatures from as many European CNs as possible, as well as other supporting organizations (be they advocacy groups, research projects, non-profits, SMEs, local authorities, etc.).

After this consultation period and the collection of signatures, we would like to send the letter to members of EU Parliament, national delegations at the Council of the EU, as well as to key officials from the EU Commission.

Several outcomes can be expected, including:

- The publication of a joint press release by all signatories to disseminate the open letter as widely as possible (by the end of March).
- Proposals for amendments reflecting the recommendations of this open letter, to be sent to key members of the EU Parliament before the first crucial vote on the Telecoms Package in late April.
- A policy workshop to be organized later this year in Brussels.

Of course, all of these potential outcomes will depend upon the involvement of signatory organizations, and in particular of the willingness of CNs to work together.

But first, we are sharing the draft to a wider circle of CNs and other people interested in their activities for consultation and potential amendments to the text. Until March 8th, many people read and commented on the draft letter, offered corrections and suggested changes or additions by using co-ment, an online tool for collaborative writing, in the iframe below or directly on the dedicated co-ment page.

If and when you agree to sign the letter, please send the name of your organization, the country where it is based and its high-resolution logo before **March 15th** to: advocacy@netcommons.eu

(note that if your signature is dependent on the response brought to a specific comment you have made, please be sure to tag comment as "blocking").

https://lqdn.co-ment.com/text/RI42W44XAc6/view/

-/ **1** discussione (filtro: 1/1 commento 2/3 repliche), naviga per: posizione

commento

OPEN LETTER TO EU POLICY-MAKERS

POLICY RECOMMENDATIONS FOR SUSTAINING COMMUNITY NETWORKS

The letter has been sent to EU institutions on March 16th, 2017.

For background, see: http://netcommons.eu/?q=content/letter-eu-policy-makers-making-regulation-work-community-networks).

Translations in various European languages are available at this page: https://wiki.laquadrature.net/Paquet_Telecom_2017/lettre_NetCommons

If your organization want to **sign the letter, please send the name of your organization at: advocacy@netcommons.eu**

PREAMBLE

We represent European Community Networks, a growing movement of organizations that operate local communication infrastructures, sometimes federated at the regional or national levels. These networks, most of which also provide access to the global Internet, are operated as a commons. That is, rather than being driven by for-profit motives, our key focus is on providing connectivity while striving for democratic governance, social inclusion, education, and human rights with respect to communication technologies.

Source URL: https://lqdn.co-ment.com/text/Rl42W44XAc6/view/

Image:

melanie's blog

Recent blog posts

Notes on European Electronic Communications Code before decisive votes in European Parliament

Stockholm Internet Forum

Draft report on "Electronic Telecommunications Code" calls for immediate action

E. Annex 5

Draft report on "Electronic Telecommunications Code" calls for immediate action

SUBMITTED BY FEDERICA ON MARCH 22, 2017 - 7:40PM

On March 16th, more than 30 European Community Networks, joined by over 35 supporting organizations from around the world, sent an open letter to EU policy-makers. The letter, which was translated in many European languages, aims at including CNs' needs in the upcoming reform of the telecommunications policy of the European Union through an "Electronic Communications Code", which is currently discussed in the European Parliament.

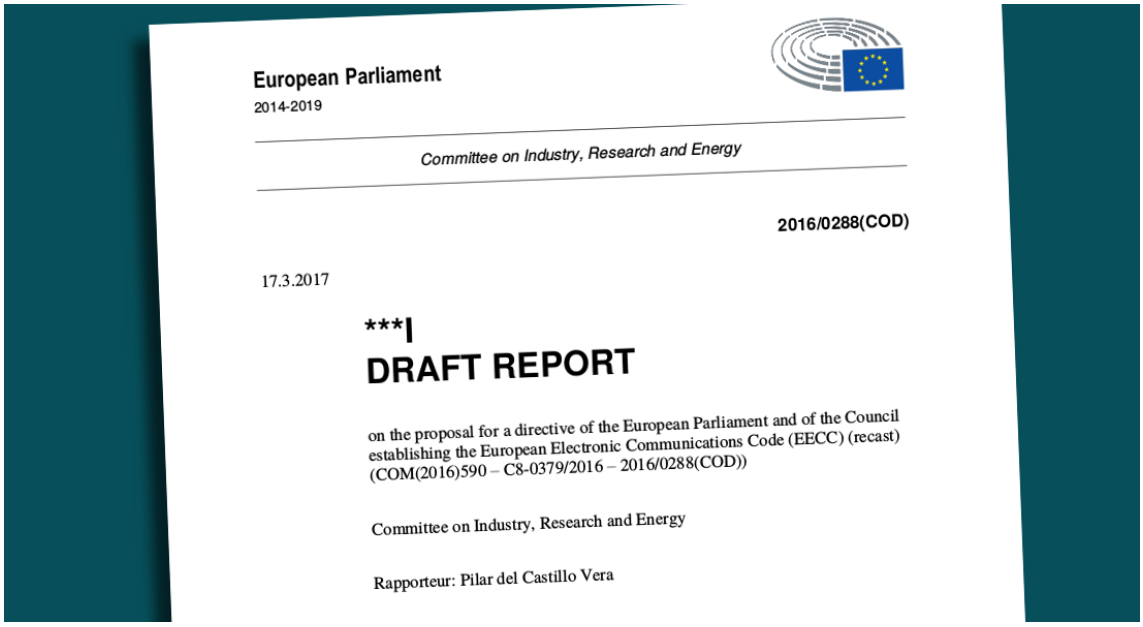
The Code will repeal the existing directives on telecommunications and mainly aims at increasing connectivity in the EU territory. While an harmonization and an update of the current policy seem more than appropriate, the upcoming Code could greatly hamper CNs development. Among other issues, the Code initially proposed by the European Commission would prevent small actors to participate in the investment of the network infrastructure, would extend to a minimum of 25 years the duration of the rights to use radio spectrum and would provide for unbalanced Universal Service obligations, making persons geographically isolated or in difficult situations into second-class citizens.

On March 17th, the Industry committee of the European Parliament (ITRE) – responsible for assessing the proposed Code – has issued its draft report, which will contain the main amendments that will be discussed by the whole Parliament in few months. Until April 4th, members of the ITRE committee may propose further amendments to this report (La Quadrature du Net works hard to provide them with positive amendments).

Such additional amendments will be necessary given that, in its current state, the draft report is even worse than the initial proposal, aggravating the gap between small operators and incumbents, extending to 30 years the duration of radio spectrum rights and removing the initial provisions in favor of the open spectrum. Its sole merit is to remove the administrative fees for small operators.

The report and its amendments will be voted on 11th July. Until then, members of the ITRE committee should be encouraged to defend the amendments under preparation in favor of CNs. Once adopted by ITRE, the report will go before the whole European Parliament: then, all MEPs will have another opportunity to table positive amendments before the Code being ultimately voted, possibly before the end of the year.

Image:


European Parliament
2014-2019

Committee on Industry, Research and Energy

2016/0288(COD)

17.3.2017

***I

DRAFT REPORT

on the proposal for a directive of the European Parliament and of the Council establishing the European Electronic Communications Code (EECC) (recast)
(COM(2016)590 – C8-0379/2016 – 2016/0288(COD))

Committee on Industry, Research and Energy

Rapporteur: Pilar del Castillo Vera

federica's blog

Recent blog posts

Notes on European Electronic Communications Code before decisive votes in European Parliament

Stockholm Internet Forum

Draft report on "Electronic Telecommunications Code" calls for immediate action

Letter to EU Policy-Makers: Making Regulation Work for Community Networks

CNs promoted as 'the other' way to connectivity at IGF2016

netCommons at the NinuxDay, the meeting of the ninux Community Network

Sarantaporo.gr Non Profit Organization is awarded financial and consulting support by the Ashoka Impact Project

DIY networking: the path to a more democratic internet

Finding "commons ground" with Sarantaporo.gr

Workshop on the History and Theory of Alternative Media

More

Log in

Credits

Co-Funded by the Horizon 2020 programme of the European Union Grant Number 688768

F. Annex 6

Notes on European Electronic Communications Code before decisive votes in European Parliament

SUBMITTED BY ARTHUR ON JUNE 7, 2017 - 1:11PM

In February, European Community Networks (CNs) and supporting organisations have expressed their concerns about the upcoming "European Electronic Communications Code" in an open letter sent to EU policy-makers.

The European Parliament will soon have two major opportunities to address these concerns.

First, on **June 22th**, the Consumer Protection committee of the European Parliament (IMCO) – one of the two associated committees responsible for the draft Code – will adopt its report.

Second, on **July 11th**, the Industry Committee of the European Parliament (ITRE) – the other and responsible associated committee – will adopt its own report (based on the alarming draft report it issued on March 17th, and on the IMCO report).

The ITRE report will be adopted in plenary session and thus be the basis for the negotiations between the rapporteur Pilar del Castillo and the Council of the European Union. The coming votes are therefore key for the next steps.

In order to assist Members of the European Parliament to adopt a text that take into account the rights of CNs and users, as well as to help Europeans to understand how the European Electronic Communications Code may impact them, netCommons is publishing five notes on the following subjects:

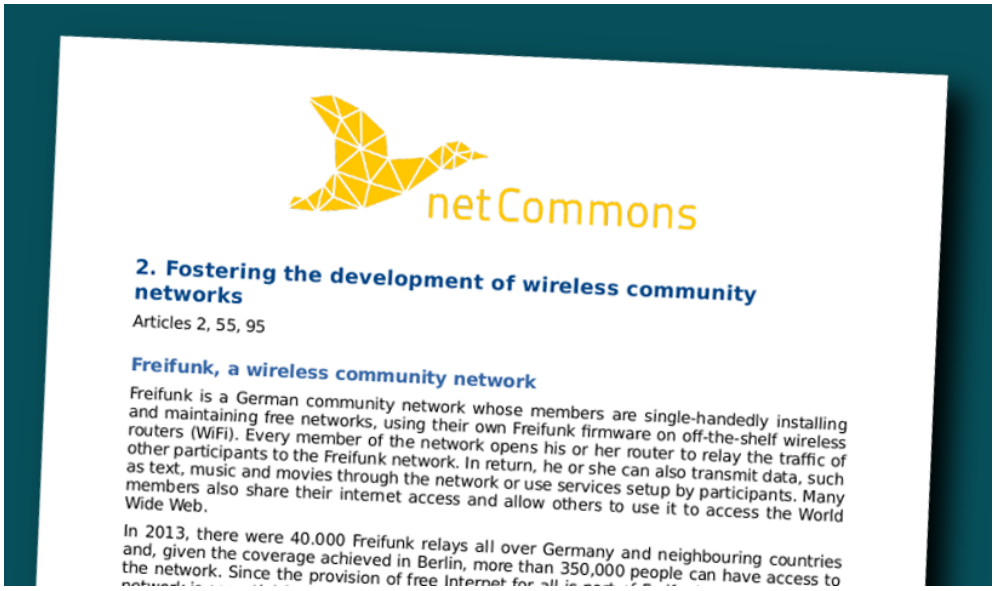
1. Enhancing data protection
2. Fostering the development of wireless community networks
3. Promoting a shared and unlicenced spectrum
4. Creating the appropriate conditions for small Internet access providers
5. Enhancing competition and addressing oligopolistic situations

These notes also intend to list which of the specific amendments tabled in IMCO and ITRE would be in favor or against Eureopeans' interest, as identified in the open letter and the netCommons work.

Download the detailed notes

Call an MEP

Image:



attachment:

netcommons_eecc_notes_imco_itre.pdf

Arthur's blog

Recent blog posts

Notes on European Electronic Communications Code before decisive votes in European Parliament

Stockholm Internet Forum

Draft report on "Electronic Telecommunications Code" calls for immediate action

Letter to EU Policy-Makers: Making Regulation Work for Community Networks

CNs promoted as 'the other' way to connectivity at IGF2016

netCommons at the NinuxDay, the meeting of the ninux Community Network

Sarantaporo.gr Non Profit Organization is awarded financial and consulting support by the Ashoka Impact Project

DIY networking: the path to a more democratic internet

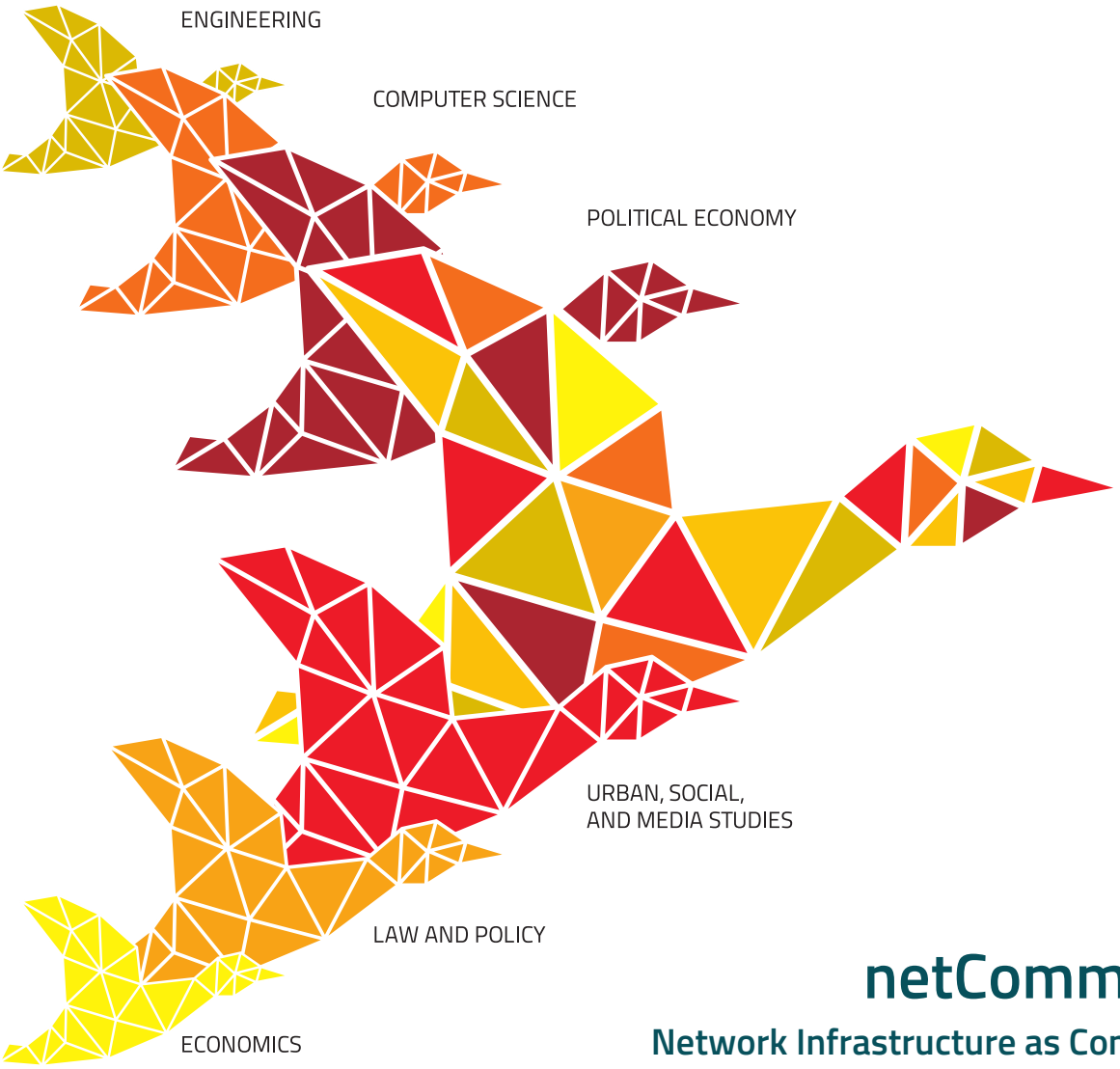
Finding "commons ground" with Sarantaporo.gr

Workshop on the History and Theory of Alternative Media

More

Log in

Credits



netCommons

Network Infrastructure as Commons

European Legal Framework for CNs (v2)

Deliverable Number D4.2
Version 0.51
July 1, 2017

netCommons.eu