Fostering sustainability of Community Networks: Guidelines to Respect the European Legal Framework

Virginie Aubrée, Melanie Dulong de Rosnay

8 Fostering sustainability of Community Networks: Guidelines to Respect the European Legal Framework

Virginie Aubrée and *Mélanie Dulong de Rosnay*

Abstract

This chapter proposes guidelines to help Community Networks (CNs) to cope with the applicable European legal framework and mitigate legal risks while protecting users' rights and enforcing core values such as privacy. It covers three main topics that are key to the activity of CNs: civil liability, data protection, data retention and provides concrete recommendations on the legal choices to be made, as well as suggestions for CN governance choices.

The chapter is based on the analysis of the legislation and case law applicable to 'electronic communications services', 'electronic communications network', and 'services providers' of an 'information society service'. The legal analysis was informed by a survey, which gathered replies on the practices of CNs from six EU countries (France, Italy, Germany, Greece, Portugal and Slovenia) in five main areas: organization, services offered, relationship with users, data protection and data retention law.

The chapter presents our findings and recommendations in the areas of civil liability, data protection law, data retention, and makes governance recommendations to address these challenges and mitigate CNs legal risks.

Acknowledgments

This article has been conducted within the project 'netCommons' (Network Infrastructure as Commons), financed by the European Commission, H2020-ICT- 2015 Programme, Grant Number 688768. <https://netcommons.eu/>.

The authors are grateful to Félix Tréguer for comments on the chapter, and to Maria Michalis, Roberto Caso and Renato Lo Cigno for suggestions on the project deliverable this chapter is based on.

8.1 Introduction

This chapter proposes guidelines to help Community Networks (CNs) coping with the applicable European legal framework and mitigate legal risks while protecting users' rights and enforcing core values such as privacy (De Filippi and Tréguer, 2015).

It covers three main topics that are key to the activity of CNs: civil liability, data protection, data retention and provides concrete recommendations on the legal choices to be made, as well as suggestions for CNs governance choices.

The proposed guidelines are based on the analysis of the legislation and case law applicable to 'electronic communications services', 'electronic communications network', and 'services providers' of an 'information society service'. The legal analysis was informed by a survey which gathered replies on the practices of CNs from six EU countries (France, Italy, Germany, Greece, Portugal and Slovenia) in five main areas: organization, services offered, relationship with users, data protection and data retention law.

The chapter present our findings and recommendations in three areas of civil liability (Section 8.2), data protection law (Section 8.3), data retention (Section 8.4), and make governance recommendations to address these challenges and mitigate CNs legal risks (section 8.5).

It is important to note that service providers can be held liable if they do not comply with specific behaviors requested of them by law. Regarding civil liability of open WiFi networks, we are considering the 2016 MacFadden ruling of the Court of Justice of the EU, on data protection law, the recent General Data Protection Regulation (GDPR) update, and on data retention legal obligations, the 2014[165] and 2016 Tele2[166] rulings, which invalidated obligations for indiscriminate, blanket data retention.

---

165 See CJEU, Judgment of the Court (Grand Chamber), 8 April 2014. Digital Rights Ireland Ltd v Minister for Communications (C 293/12 and C 594/12).

166 See CJEU, Judgment of the Court (Grand Chamber), 21 December 2016. Tele2 Sverige AB (C 203/15) Secretary of State for the Home Department (C 698/15).

8.2 Civil liability

Civil liability has proved to be a problem for a number of CNs, particularly in Germany where Freifunk participants for years had to deal with the risk of third party infringement[167]. To ensure the lawfulness of personal data processing, the chapter provides suggestions for security measures and transfer of data, anonymizing and "pseudonymizing" data.[168]

Entering into a contract with the users of CN services can be an interesting solution to mitigate the risks associated with both the applicable liability regime and the data protection framework. For the same reasons, incorporating a CN through a non-profit legal status could also help alleviate legal risks and clarify the distribution of liability within the community. In this sense, the community can reflect on these risks and anticipate them rather than being forced to act in the context of a legal crisis.

Regarding civil liability, it is important to stress that providers can be held liable only if they do not comply with specific behaviors requested of them by law (Baistrocchi, 2002; Busch, 2015; Giovanella, 2015). These behaviors vary depending on the different roles played by CNs, which can qualify as "mere conduit", "caching" or "hosting" providers.[169] For instance, hosting providers can be held liable if they do not remove expeditiously an allegedly illegal piece of information when they receive a notification by a third party (*e.g.* a user of their services) highlighting the existence of the infringing information.[170]

---

167 Germany used to have a form of strict secondary liability, the so called doctrine of Störerhaftung. This doctrine was abrogated by the new version of the Telemedia Act of October 2017 (§7-10). The full-text in German is available here: <https://dejure.org/gesetze/TMG> ; For further information on this issue, see CJEU, Judgment of the Court (Third Chamber), 15 September 2016, Tobias Mc Fadden v Sony Music Entertainment Germany GmbH (C-484/14) and an analysis on CNs in Aubrée et al (2018).

168 According to GDPR recital 26 "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."
According to GDPR art. 4(5) "'pseudonymization' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;"

169 These terms are defined in articles 12, 13 and 14 of EU Directive 2000/31/EC, commonly referred to as the E-Commerce Directive.

170 See art.14 E-Commerce Directive.

Such an obligation to remove online content is applicable to any kind of data, regardless of the source. This means that, when the CN is considered as a hosting provider, it does not matter whether the data to be removed come from within a CN or not, as long as it is hosted within the networks and to the extent that the CN – and the persons responsible for it – can take active steps to take the targeted content down.

Furthermore, in the context of open WiFi networks[171], CNs can be held liable if they do not comply with an injunction measure requiring to prevent third parties from engaging in copyright infringement. According to the Court of Justice of the EU (CJEU), such measures might involve subjecting the possibility to utilize the CN to the use of passwords so that users "are required to reveal their identity in order to obtain the required password and may not therefore act anonymously".[172]

A general recommendation for CNs would be to distribute as much as possible obligations and liabilities among members of the community and make sure that this distribution is clear for all involved parties.

In terms of liability, two different situations should be distinguished. First, liability concerning unlawful information or content. In reliance with the McFadden case law and specific national provisions, CNs should enjoy the liability exemptions introduced by Directive 2000/31, but at the same time they might be the target of injunctions to secure their connection (such as password-protect it).

Second, liability concerning the whole management of the network as a physical infrastructure able to generate physical damages. As a network is composed of different parts, those can be under the control of a CN – or, more precisely, of the entity through which the CN is incorporated and that is responsible for its management –, a user or a third party. Each situation implies a different outcome regarding liability. In each situation, choices have to be made

171 See Mac Sithigh (2009).

172 For further details, see the McFadden ruling of the Court of Justice of the European Union; Giovanella and Dulong de Rosnay (2017).

between responsibilization of users, mutualization of risks – with an insurance – or decentralization of obligations and responsibility – with a dedicated agreement.

When there is an entity, the use of end-user licenses or terms of use might be a way both to inform users and to limit the CNs' liability: exactly as commercial providers do, CNs may impose specific obligations on their users, interrupt service and/or ask for damages when users do not comply with these obligations. This is for instance one of the clauses included in the FONN License[173] adopted by Guifi.net.

8.3 Data protection law

In the context of the new European data protection framework, established by the entrance into force of the GDPR, a general recommendation would be to anonymize as much as possible the data processed – aside from technical or legal requirements. At the same time, we recommend to pay attention to the provision of intelligible information to users in a clear and plain language and the purpose for data processing for which consent is requested.

The scope of the GDPR and data protection principles does not apply to anonymous[174] data, defined as "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". Simply put, data can be deemed as anonymized as long as they cannot be attributed to any individual, by anyone, in any circumstance (Mourby et al, 2018). Thus, anonymizing data would be a good practice to reduce legal risks. As underlined in the results of our survey, it is encouraging to note that some CNs seem to achieve this goal.

They declared: "we do not collect anything we think is personal data about our users, we also do not know which data we collected is by which user". This assertion could also mean that they do not have knowledge of the link between data and data subject. Now,

173 See the Compact for a Free, Open & Neutral Network (FONN Compact) <https://guifi.net/en/FONNC>.

174 See Art. 29 Working Party, "Opinion 05/2014 on Anonymization Techniques," Apr. 10 2014.

even when CNs apply absolute anonymization, it is still possible to de-anonymize that data and link it to a specific data subject[175]. So even anonymized data can be regarded as personal data and fall within the scope of the GDPR. Therefore, it would be safer for CNs to also take into account obligations regarding informed consent and transparency[176].

Any CN should provide its users/members with information about their rights with regard to their personal data processing. In particular, the information provided through the web page of the CN should comply with the requirements introduced by art. 12, Reg. 679/2016: Information should be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". All CN should provide its users with such information before processing data.

8.4 Data retention

With regard to data retention, CNs face a particularly thorny issue considering the legal limbo surrounding these legal obligations established across Europe to facilitate law enforcement. Given the 2014 and 2016 Tele2 rulings of the Court of Justice of the EU, which invalidated obligations for indiscriminate, blanket data retention, not less than seventeen Member States are, according to our analysis, still in breach of this crucial case law as of June 2018. It will probably be months, or years, before all ambiguities are finally resolved. In the meantime, we have highlighted various strategies that we have observed in the course of research, inviting CNs to choose the path they deem to be most appropriate for them.

These strategies range from the most "conservative" option (*i.e.* deciding to respect national law at the expense of the right to privacy as construed by the "Supreme Court" of the EU in its case law), to

175 For research on re-identification of de-anonymized data, see Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1), 40–81. <https://doi.org/10.1080/17579961.2018.1452176> and Sweeney, L. (2000).Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3.

176 On this subject, Art. 29 WP published guidelines regarding consent at <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item id=623051>.

the most "activist" stance (*i.e.* defying national law while invoking this European case-law to highlight the discrepancy between some EU member laws and fundamental rights), which bears the risk of litigation and, possibly, fines or even jail.

Importantly, according to the primacy principle, EU law shall have primacy over any law of the Member States. This implies that if a national rule is contrary to a European provision, the binding force of this Member State's rule is regarded as suspended[177]. As a consequence, on principle, CNs should comply with the European legal framework. Regarding data retention, this refers to the Tele2 case law[178]. To be specific, in light of this decision, national laws should not provide for:

a) Indiscriminate and general collection of data,

b) Access to personal data for an objective wider than fighting serious crime,

c) Access to personal data without prior review by a court or an independent administrative authority, or

d) Retention without an obligation to store these data within the European Union.

In light of the above, several national frameworks were declared inconsistent with EU law or unconstitutional by local judges (Milaj, 2015). In some Members of the EU, laws were repealed, such as in the Netherlands[179] or Slovakia[180]. In other countries, laws were set aside and operators that did not retain data as prescribed by their national laws were not sanctioned[181]. However, in most of them, there is no clear legal answer to whether national laws should still be in force. In accordance with EU criteria, it is highly doubtful that data retention legislation in Italy, France, Germany, Greece, and Spain comply with CJEU jurisprudence[182].

177 See Court of Justice of the European Community, 15 July 1964, Flaminio Costa v E.N.E.L, Case 6/64; For a clear introduction to the principle, see: <https: //eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14548&from=FR>.

178 See <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62015CJ0203&from=FR>.

179 See <https://edri.org/dutch-data-retention-law-struck-down-for-now/>.

180 See <https://edri.org/slovakia-mass-surveillance-of-citizens-is-unconstitutional/>.

181 See, for instance, three German decisions: OVG Münster 13 B 238/17, VG Köln 9 K 7417/17 and 9 K 3859/16.

182 For Russian data retention requirements, see Zhuravlev et al (2018).

Therefore, where a country has a national statute in breach of EU case law, CNs could theoretically be free not to comply with the law. Yet, in all of these framework serious fines exist for CNs which do not comply with data retention obligations. Therefore, a legal risk does exist for them.

Thus, several hypotheses should be considered:

a) If CNs want to reduce legal risks, they could strictly comply with national law – except when a public statement provided expressly that no fine proceedings would be started against non-compliant providers (as in Germany[183]). However, overcompliance also generates legal risks for CNs. Indeed, if a CN has a data retention system exceeding its legal framework – *e.g.* in terms of scope of data or duration of retention – this activity could be regarded as an unlawful processing since this additional retention would no longer be "necessary for compliance with a legal obligation to which the controller is subject"[184].

b) If CNs want to comply with practical requirements while avoiding overcompliance issues, a compromise could be reached. They could reduce the scope of data retained to the one that is actually demanded by public authority while conducting their investigations: IP addresses and subscriber ID. This would not respect the letter of the law, and therefore implies theoretical legal risks. However, such data would be enough to comply with most request of access – which are very rare in the experience of Community Networks. Empirical evidence from several CNs we have interviewed suggests that law enforcement authorities generally accept this as satisfactory.

c) If CNs want to actively take part of the advocacy against blanket data retention, their third option is to choose to ignore data retention provisions. However, they should keep in mind that this choice come with a legal risk, as they could be prosecuted by national authorities. To mitigate this risk, if they are sanctioned, they still have the possibility to challenge this decision before

183 In reliance with the official press-release of the federal telecommunication regulatory authority (Bundesnetzagentur), available (in German) here: <https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS 113aTKG/VDS-node.html>.

184 See GDPR, art. 7, (c).

national courts, arguing that the obligation is inconsistent with EU law and so is the fine applied to them.

8.5 Governance

This section deals with the internal organizational form of the CNs and the relationship with users or members they may adopt in order to better manage requirements pertaining to the three main legal issues CNs are facing – which were described in the three previous sections of this chapter.

Entering into a contract with the users of CN's services can be an interesting solution to mitigate the risks associated with both the applicable liability regime as well as the data protection framework. For the same reasons, incorporating a CNs through a non-profit legal status could also help alleviate legal risks and clarify the distribution of liability within the community, so that it can reflect on these risks and anticipate them rather than being surprised by law enforcement and obliged to act in the context of a legal crisis.

As regards organization, the survey we conducted highlighted that most respondents are organized as an association. Yet, some of the analyzed CNs do not have a legal form with clearly redefined responsibilities attributed to specific individuals. This absence of official structure allows them to enjoy an informal relationship.This idea is in line with the way decisions are taken in these structures (in a bottom-up consensus-driven fashion). In this regard, all respondents acknowledged the importance of a distribution of power and a horizontal approach as well as a participative and collective decision process within the community. Regarding services provided by CNs, the core of their activity is to provide an Internet access (through Wi-Fi mostly, but sometimes through landline networks too) although, they very often stimulate the development[185] and offer several additional services such as hosting, e-mail, online fora or Tor node services which can imply extra subtleties in terms of civil liability.

185 See Belli, L. (2017). Network Self-Determination and the Positive Externalities of Community Networks, in Belli, L. (Ed.). (2017). Community Networks: the Internet by the People for the People, 35-64. <http://hdl.handle.net/10438/19401>.

In order to be able to undertake their important social and economic function while minimizing risks of liability, we recommend that CNs adopt a suitable legal form to conduct their activity, being incorporated in the form of associations, cooperatives, foundations or other non-profit organization, depending on what legal options are provided by their national frameworks.

Importantly, insofar as CNs determine the means and purpose of the processing of users' data, they qualify as data controller under art. 4(7) of the GDPR. When a CN is organized as an association or cooperative, there is a legal entity and therefore there are no issue in determining who the data controller is, being it a natural or legal person. On the contrary, when the CN does not have any specific legal form, it becomes more difficult to understand who is the controller, and liability might weight on private individuals participating in running the network. Thus, to mitigate legal risks and share liability, it is more suitable for CN to adopt a specific legal form.

Concerning the nature of the relationship with users, the results of the survey we conducted reveal that the 'informal' relationship is also favored in practice. The results show that most of the CNs we interviewed[186] do not use a contractual form to establish a relationship with their members. However, there is a different kind of proximity built with the CN user since there is often a requirement to be a member[187] of the community in order to access to the service provided. This implies a flexible and trust-based relationship with the users. Yet, it can create difficulties regarding data protection law. Besides, CNs tend to highly favor privacy in their relationship with their users. This concern is also shown though their data retention habits, as a large part of the respondents declared that they do not retain any data.

We recommend that Community networks sign a contract or an agreement with their user when acting as legally definable "service provider", be the service Internet access or an additional service.

186 The questionnaire which circulated among Community Networks is available in Aubrée et al (2018) Annex 1, p. 94. See also, for the analysis, Ibid, p. 63-72.

187 A member of a CN "Participant" in the sense of the terminology employed in the Declaration of Community Connectivity available at <https://comconnectivity.org/article/dc3-working-definitions-and-principles/>. and in Belli, L. (Ed.). (2017): 237. <http://hdl.handle.net/10438/19401>.

Concerning data protection law, the GDPR states that a lawful processing of personal data – which CNs have to do in order to provide their services – requires a legitimate interest, consent or contract[188]. For all these legal basis for personal data processing, the most reliable solution is the establishment of a contractual relationship between specifically designated data processor and users. Indeed, in the case of CNs, the extent of the legitimate interest is difficult to evaluate with certainty. Such an agreement could help establish a transparent relationship between a CN and its members and users and could also contain provisions to distribute civil liability.

8.6 Conclusion

The analysis of EU and relevant national laws allowed us to produce a mapping of legal requirements CNs have to respect or to implement in the areas of liability, data protection and data retention. Interacting with CNs through a survey about their practices further contributed to our analysis. It helped us identify gaps and needs, which led to the development of applicable legal guidelines to cope with legal hurdles, towards legal sustainability of CNs, which have special regulatory needs.

In light of these findings, we produced general guidelines in the actual practice areas of CNs, balancing between legal requirements and CNs political ethos: maintaining privacy in their relationship with their users and having a horizontal distribution of power as a participative and collective decision process within the community. These guidelines represent an important step towards the full compliance of CNs with national legal frameworks and, although are limited to the EU framework, can serve as inspiration for other initiatives aimed at fostering CN legality.

8.7 References

Aubrée, V., Dulong de Rosnay, M., Giovanella, F., Messaud, A., Tréguer, F. (2018), European legal framework for CNs (v3). *Deliverable D4.3 of the netCommons project*. <https://www.netcommons.eu/sites/default/files/d4.3_v1.2-2018-08-23.pdf>.

188 See GDPR art. 6.

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

Belli, L. (2017). Network Self-Determination and the Positive Externalities of Community Networks, in Belli, L. (Ed.). (2017). *Community Networks: the Internet by the People for the People*, 35-64. <http://hdl.handle.net/10438/19401>.

Busch, C. (2015). Secondary Liability for Open Wireless Networks in Germany: Balancing Regulation and Innovation in the Digital Economy. <http://dx.doi.org/10.2139/ssrn.272835>.

De Filippi, P., & Tréguer, F. (2015). Wireless Community Networks: Towards a Public Policy for the Network Commons? In L. Belli & P. De Filippi (Eds.), *Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet* (pp. 261–275). Springer.

Giovanella, F. (2015). Liability Issues in Wireless Community Networks. *Journal of European Tort Law*, 6(1). <https://doi.org/10.1515/jetl-2015-0002>.

Giovanella, F., & Dulong de Rosnay, M. (2017). Community wireless networks, intermediary liability and the McFadden CJEU case. *Communications Law*, Bloomsbury, Wiley, 22 (1), 11-20. <https://halshs.archives-ouvertes.fr/halshs-01478116>.

Mac Sithigh, D. (2009). Law in the Last Mile: Sharing Internet Access Through WiFi. *ScriptEd*, *6*(2), 355-376. DOI: 10.2966/scrip.060209.355

Milaj, J. (2015). Invalidation of the data retention directive – Extending the proportionality test. *Computer Law & Security Review*, *31*(5), 604–617. <https://doi.org/10.1016/j.clsr.2015.07.004>.

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review*, *34*(2), 222–233. <https://doi.org/10.1016/j.clsr.2018.01.002>.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 40–81. <https://doi.org/10.1080/17579961.2018.1452176>.

Sweeney, L. (2000). Simple Demographics Often Identify People Uniquely. *Carnegie Mellon University*, Data Privacy Working Paper 3. <http://dataprivacylab.org/projects/identifiability/paper1.pdf>.

Zhuravlev, M. S., & Brazhnik, T. A. (2018). Russian data retention requirements: Obligation to store the content of communications. *Computer Law & Security Review*, 34(3), 496–507. <https://doi.org/10.1016/j.clsr.2017.11.011>.