WLAN Communities and Internet Access Sharing:  
a Regulatory Overview

Giovanni Camponovo *, Davide Cerutti **  
* HEC School of Management and Economics, University of Lausanne  
** Centre de Droit Privé, University of Lausanne  
Giovanni.Camponovo@unil.ch, Davide.Cerutti@unil.ch

Abstract

The widespread adoption of wireless LAN has paved the way for the emergence of a compelling alternative to cellular networks for obtaining Internet access on the move. This has generated interesting opportunities to a variety of players to position in the mobile industry as Wireless Internet Service Provider. Mobile network operators have insofar managed to take control of this sector through aggressive preemptive strategies. However, the rapid emergence of private WLAN networks and broadband Internet connections among households has raised the crucial issue of the sharing of Internet access through these networks. While most owners are unaware of this, some have consciously organized themselves to form free wireless communities aiming at providing free Internet access to members or even to the public. One fundamental concern about this conduct is whether these sharing practices are allowed from a regulatory point of view, determine the rights and obligations of the various parties involved and the sanctions that they may incur. The purpose of this paper is to investigate this important issue by considering two examples of regulation (the French and Swiss ones) and examine its implication for the various actors involved.

1. Introduction

At the turn of the 21st century, Wireless Local Area Networks (WLAN) have received a huge amount of attention in the mobile industry and many have considered it as a potentially disruptive technology which could have threatened the established operator centric models based on cellular networks and especially harm their 3G investments and revenues [1].

At the same time, some other observers argued against this view by pointing out that WLAN has radically different features than cellular networks (e.g. in terms of range, throughput and the type of devices used to access the network) and could have been used by operators as a complement, rather than an alternative, to their cellular networks as well [2].

The origins of WLANs go back somewhat longer, in particular to the 1990s efforts of the IEEE to set up a WLAN standard. Yet, demand was initially stagnating due to high equipment prices, low performance, security concerns and lack of interoperability [3]. The turning point was the issue of the 802.11 standard in 1997 and especially its 802.11b extension in 1999 as well as the interoperability certification service of the WECA. The improved performance, interoperable products, rapidly decreasing prices and the increasing adoption of flat rate broadband Internet access in households made it possible a tremendous growth in the deployment of private WLAN networks by enterprises and residential consumers as an extension or replacement of traditional LANs [4].

For these reasons, private hotspots now represent a huge phenomenon. Consider for instance the extreme case of Manhattan which has a density of private WLAN hotspots which nearly cover the whole territory [5], but many other cities have a large density of private hotspots so that it is possible to find them almost anywhere. This also applies to big Swiss cities such as Zurich, where a simple wardriwing session counted more than 5000 hotspots in 2004 [6].

In parallel, the widening diffusion of WLAN compatible devices created an opportunity to offer commercial WLAN access to nomad users in public locations. In particular, the last three years witnessed an initial vague of public WLAN networks operated by various types of providers like mobile and traditional network operators, Internet Service Providers, start-ups, venues and wireless communities[7-9].

Typical of an emerging industry where a shared conventional wisdom about the way to success has not yet been formed, these players pursued fundamentally different strategic approaches [10]. Among them one
could have distinguished a primary business model based on the traditional ISP logic of providing Internet access upon payment of subscription fees, an emerging business model proposing occasional network usage paid by micro payments, and a neighborhood area network business model based on clustering private hotspots together and offering free access [4, 11].

Being aware of the threat that competing WLAN networks could have represented, mobile operators have opted for avoiding any risk and executing an aggressive preemptive strategy to take control of the sector through strategic alliances and acquisitions. It appears mobile operators have insofar prevailed over the other providers which have initially launched the sector and nowadays seem in a position to control the commercial WLAN Internet Service Provider industry.

Nevertheless, one significant unresolved issue that they have to face is that the massive deployment of private hotspots with broadband Internet connections may constitute a much cheaper alternative, albeit of presumably lower quality, to their commercial WLAN networks to gain Internet access on the move.

The problem is that an impressive number of such hotspots are unintentionally left open for use by other people either because their owners have installed no security mechanisms (e.g. the default configuration of plug and play WLAN hardware) or have opted for an insufficient protection (such as the standard WEP encryption) which can be easily bypassed by reasonably knowledgeable people.

What is more, some owners have even organized themselves to cluster their hotspots together to form wireless community networks aiming at providing free Internet access to community members or even to the population at large [12]. Many wireless communities have appeared in various parts of the world following the examples of the Boston Wireless and the Bay Area Wireless Users Group in San Francisco and wireless communities can be found in most urban areas.

However, one fundamental concern in this practice is whether these sharing practices are allowed from a regulatory point of view. In this respect it is fundamental to determine what are the rights and obligations of the different actors involved and what are the sanctions that they may incur in case they do not conform to them.

The purpose of this paper is to investigate this important issue by investigating two examples of regulation dealing with this matter and examine its implication for the various actors involved: namely the Internet Service Provider, the legitimate owner of the hotspot, the fraudulent neighbor and the regulation authorities. To do so, we present two examples of legislation: the Swiss and French regulations.

The paper is structured as follows. The next section presents the general case from a juridical viewpoint and identifies the rapports between the various parties involved. Sections 3 and 4 respectively illustrate the Swiss and French legal frameworks on this matter. Finally, section 5 discusses the major findings of this regulatory overview.

2. The general case of hotspot sharing

The actors which may be potentially involved, directly or indirectly, in a typical case of Internet access sharing via a WLAN network are the following:

- The WLAN owner (hereafter referred to as A). He possesses an Internet connection obtained from an ISP which he shares via its own WLAN network with other people. Notice that the sharing might be conscious, such as in the case of A adhering to a wireless community or in response to an agreement with other parties to share the Internet connection. However, the sharing might be unconscious as well, such as in the case that A involuntarily leaves its WLAN open or badly secured.
- The third party (hereafter referred to as B) who takes advantage of the WLAN network set up by A to gain access to the Internet for free. He may be a neighbor, a tenant of the same building, a member of the community or simply anyone passing nearby.
- The Internet Service Provider (ISP). He basically provides a broadband Internet connection to A via technologies such as ADSL or cable in exchange of some payment (usually a monthly flat rate fee).
- The Regulation Authority. It sets the regulatory framework governing the use of radio waves and supervises its compliance.

In the two following sections we will examine the rapports between these parties from a legal viewpoint and examine their implications according to the Swiss and French legal frameworks. We will consider these rapports with regard to the civil and penal rights and illustrate the rights and obligations of the various parties involved and the sanctions that they eventually incur in the case they do not conform to them.

In particular, we will in a first time concentrate on the relationship between A and B in order to examine whether B can lawfully gain access to the connection Internet using the WLAN network of A or whether this behavior is illicit and may incur in some sanctions. In this respect, it is necessary to distinguish the case in which the WLAN is left unsecured from the case in which it is secured, but insufficiently to prevent third parties to gain access. In the former case, the network is left open to third parties who can access it without any particular action. In the latter case, the network is
protected by some security mechanisms which must be bypassed to gain access. The difference between these two cases is that in the former case only civil penalties might conceivably be applicable, if any, whereas the second case may also involve penal sanctions. For that reason we will firstly examine the situation from the viewpoint of civil right, and then investigate the legal sanctions which may be applicable in the second case.

In a second time, we will examine the relationship between the ISP and A. This relationship depends on the content of the contract that has been agreed at the time of the subscription to the ISP services, although more often than not the contract does not permit the sharing. As before, it is useful to distinguish two cases according to whether A is unaware of the sharing, e.g. in the case of a not technical savvy user leaving its network open by default, or whether it consciously consents to B to use its network, e.g. in the case of a wireless community or as a result of an arrangement.

Before describing in more detail how these two relationships are treated from the viewpoint of the Swiss and French regulatory framework, it is useful to stress that there is no direct legal relationship possible between the ISP and B: if the ISP wants to act against B he must do so via the intermediation of A. As well, regulation authorities are also partially concerned since they only are expected to exert a limited surveillance such as the respect of emission power limits.

3. Swiss Regulation

Relationship between A and B – Civil Aspects

In principle, any use of the frequency spectrum in Switzerland is subject to licensing from the telecom authorities (Art. 22.1 Law on Telecommunications, thereafter LTC). However, pursuant to the possibility of admitting exceptions to this principle in cases of low importance (Art. 22.3 LTC) and the governmental decree on frequency management, telecom authorities have excluded WLAN networks from the licensing obligation. As a result, two licence-free frequency bands have been released for WLAN systems in the 2.4 and 5 GHz ranges. These bands are allocated to a class known as unprotected group frequencies since their use is permitted to an unlimited number of users and there is no protection admitted from interference from other systems. Yet, in order to contain interferences within an acceptable level, all WLAN hardware must respect a maximum radiated power emission limit of 100 mW in the 2.4 GHz band, 200 mV in the 5GHz band.

One interesting question is whether the free nature of these frequencies does imply that a third party is legitimately allowed to use the same radio waves of a given private network in a way that does not only interfere with the signal (which is allowed by the non protection from interference clause discussed before) but also to enter into this network so as to exploit its resources and namely its Internet connection. In other way, are there some legal norms that protect A against intrusion by third parties in his private network?

A first possibility to answer this question is to turn to the regulation of personal property and especially to the norms governing the protection of possession. Possession is the act of holding control, as a matter of fact, on some things. Such things include not only physical objects, but also intangible assets such as intellectual property rights and natural forces such as electricity. If we admit by analogy that A possesses the signals emitted by his WLAN system that allow him to access the Internet, their usage by B does disturb his possession. Disturbance of possession is sanctioned by the law (Art. 928 Civil Code, thereafter CC), which gives the possessor the possibility to ask the cessation, prevention or reimbursement of the damage caused by such disturbance. However, this seems not applicable in the case of WLAN given that its frequency bands are allocated to a class which does explicitly not admit protection from interference from other systems.

Another potentially relevant regulatory area which may be applicable is the law governing real property and more particularly the portion on the rights of neighbors. The rule is that one is compelled to avoid disturbing his neighbor (Art. 684 CC). Typical examples involve active behaviors such as emitting noise and smoke, but the Swiss Supreme Court has extended this obligation to passive disturbances like denying a neighbor of sunlight (DTF 126 III 452). The fact of reducing the throughput of the Internet connection available to A may hence be considered a disturbance of B. A may thus be allowed to ask the cessation of the disturbance and reclaim damage as allowed by Art. 684 CC.

Likewise, if A and B are tenants of the same building, the situation is very similar as they must respect each other with due diligence (Art. 257f OC). We may likewise argue that the behavior of B of reducing the throughput of the Internet connection available to A is against his due diligence. In this case, the difference is that A must act against the building owner which shall subsequently act against B.

Finally, the last potentially relevant regulatory area are the norms governing the reimbursement of damage caused by illicit acts (Art. 41 Obligations Code, thereafter OC). The law admits that if a party causes damage to another as a consequence of an illicit act, the damage must be repaired. Four conditions must be cumulated for these norms to be applicable: 1) damage must have been caused, 2) the act must be illicit, 3)
there must be a cause-effect relationship between the damage and the act, and 4) there must be culpability. While the last two conditions do not pose particular problems, the first two are more debatable.

With regard the first condition, at first sight damage seems evident given that quality of service obtained by A is reduced by the behavior of B (he pays more for what he gets). However, the norm typically concerns material damage such as the destruction or damage of objects and moral damage resulting from it, but there is no precise answer as to whether impairing the function of an object is judged as damage. The Swiss Supreme Court has admitted it in some particular circumstances (DTF 118 II 176). In view of this jurisprudence, the disturbance of a WLAN might well be considered to constitute a damage, since it impairs the functions it should have accomplished. However, the Swiss legislations generally adopts a restrictive conception of what constitutes a damage known as the theory of difference, which only covers a reduction of the wealth calculated as the difference between the wealth before and after the illicit behavior. The Swiss Supreme Court (DTF 120 II 296 and DTF 127 III 403) and most jurisprudence authors [13-15] seem to adhere strictly to this theory and consider economical damage only. With this interpretation of damage, it is hence difficult to admit the existence of damage in our case. Note that other regulations, such as the German, follow the more open theory of normative damage, which admits that damage includes not only economic wealth reductions, but also the compensation of harm not expressed in monetary terms. This theory would be interesting in our case, but only one jurisprudence author [16] advocates its application in Switzerland as well.

The second condition is that the act causing the damage must be illicit. There are two theories as well which can be used to determine if an act is illicit. The subjective theory (used in France) holds that any act causing damage to another party is illicit. By contrast, the objective theory (used in Switzerland) holds that an act is illicit only if it infringes a legally protected good or behavioral norm. Surprisingly, immaterial properties (except intellectual property rights) are not protected in Switzerland. The disturbance of a WLAN would thus not constitute an illicit act. This view, however, goes back to the origins of the Obligations Code in 1911, when possessions were mostly composed by physical objects. Considering the evolution of society since then and the increasing importance of immaterial goods, the law might be reinterpreted to consider immaterial goods to be protected as well. We are generally not yet there, but a recent norm (Art. 43.1bis OC) holds that the affective value of an animal must be repaid in addition to the material value. At the moment of the creation of this law, the government stated that one must reimburse all the costs caused by his damage, not only the reduction of the material value, but also affective and immaterial costs which can even be bigger than the material value of the animal. The government argued that this principle should apply to the reimbursement of any object as well. By pushing the reasoning further, we could argument that all costs must be reimbursed, not only the economic ones.

It appears from this brief overview of the civil right that the situation under study is in a sort of grey zone which is not precisely regulated and opens numerous reflections areas. Nevertheless, it seems that the Swiss civil right does not easily allow to A to pursue B for the harm that is caused by the fact that B exploits is network.

**Relationship between A and B – Penal Aspects**

By considering penal aspects, several penal norms that are applicable only in the case that A protects his network and B bypasses these protections to gain access to network.

The norm about intrusion on protected systems (Art 143bis Penal Code, thereafter PC) seems at fist sight applicable. This norm has been issued with the idea of punishing hackers who enter in protected information system without authorization and without the goal of enriching himself. In our case, B does indisputably violate the protected system of A. Yet a nuance should be made since this article applies to cases in which the intruder does not aim to enrich himself, while in this case the intruder does enrich by not having to pay to get an Internet connection. In this case the article described in the following paragraph will be applied. Finally, the system may be considered as not especially protected against intrusion depending on the security mechanisms put in place and therefore this article may not be applicable.

Another disposition does indeed apply in the case that the goal of the intruder is to obtain fraudulently for free a service knowing that this service must have been paid (Art. 150 PC). The fact that B obtains a paid service for free is evident. The fraudulent aspect is more disputable, but at the time of issuing the law the government stated that the simple use of a computer or software of others was punishable by this norm. As well, the Supreme Court established that receiving a television channel with a decoder without having subscribed to it is punished. This case presents some analogies with ours as the user uses an installation to get for free signals that he should have paid. It thus appears that this norm may be applicable to our case and that B may incur its sanctions of up to 3 years of imprisonments and a fine up to 40'000 francs.
We may also add the sanction of the interference with the management of public organizations in transport or communications domains (Art. 239 PC). In one famous judgment (case Zschokke, DTF 102 II 85), the Supreme Court has established that the fact of breaking an electric wire and leave an area without electricity for several hours gave the subscribers the right to invoke this article to ask reimbursement to the one who has caused the damage. This means that not only the owners of the infrastructure, but also the clients, can invoke this article. By analogy it might be possible to extend its application to WLAN. However, the fact that the network is used for private purposes should make it inapplicable to our case.

As a result, the penal right seems only applicable if A has protected his network against external access. In this case B must crack the protection system (the fact that this may be very easy does matter, but is subject to the subjective interpretation of judges), in order to gain access to the Internet via the connection of A.

**Relationship between ISP and A**

In Switzerland an organization such as an ISP that provides a telecommunication service is considered to own its lines and can hence decide to whom allow the utilization of its lines. In our case, the ISP contracts with A without knowing that B would also use its lines. Does that mean that if the ISP gets to know this fact, does it have the possibility to act against A in order to prohibit the access of B?

This may be set in the contract between the ISP and A: generally such contract contain a disposition that obliges A to ensure the security of its network and prohibits him to share the access with other parties without the specific consent of the ISP. If A does make it so anyway, it violates the contract with the ISP. In fact, the contract contains an obligation of not doing something, which in turn implies the prohibition of doing the opposite (DTF 114 II 329). In our case, A is prohibited to let other parties use the connection and this violation gives the ISP the possibility to ask the judge to impose to A to stop the sharing with B or to be authorized to stop it by himself. In our case, this might be conceived as to impose to A to secure his system with appropriate security means impeding other parties to access the network. The non respect of these commands is of course punishable. In addition, the ISP may ask A to pay a penalty as a damage refund as well as to break the contract.

In one recent judgment (DTF 129 III 604), the Supreme court has analyzed the relationship between a telephone network operator and a subscriber which, after having made 136 calls to premium numbers in a month he has received a bill more than 16'000 CHF. He denies any call and proposes to have been victim of piratage. The court acknowledges that the subscriber had a cordless phone system which was not conform to the prescription of communications authorities and that there was no piratage. The contract between the operator and the subscriber made the latter responsible of the usage of the phone connection by third parties with or without authorization. The conclusion of the judges is that the subscriber of the phone line must manage his own phone station and is responsible of its use by other parties.

If we transpose this decision to the case of WLAN, the subscriber of the Internet connection would be held responsible of its usage by B. Being responsible, A could therefore not lament with the ISP of the behaviour of B. ISPs normally impose the exclusive usage of the connection by A or anyway free themselves from any responsibility.

If we push the reasoning further, if B exploits the connection of A to visit illegal sites, A may be held responsible. The Swiss law on telecom contains a sanction of imprisonment or a fine up to 100000 CHF for those that permit the use of telecommunication system to third parties without authorization (Art. 52 f Law on Telecom). Both A e B risk to incur a sanction.

In the case that A and B act in agreement, we can also imagine a case of fraud (punished by art. 146 PC) committed by A and B against the ISP resulting from the fact of obtaining an unauthorized sharing of the Internet connection.

A last aspect that may be envisioned is the law on unlawful competition (LCSI). The fact of exploiting the service of a party to provide a service to another party is an illicit act. The open network of A and B can be considered an example of unlawful competition since A resells the service obtained from the ISP to B. The ISP can accordingly file a suit for obliging a to stop his behaviour and ask it to refund the eventual damage incurred. Moreover, A and B also risk a sanction in terms of imprisonment and fines up to 100000 francs according to art. 23 of the LCSI.

**4. French Regulation**

Between 2002 and 2003, the European Union has elaborated a package of laws aimed at simplifying the regulatory framework of the telecommunication sector and which also involved WLAN networks\(^1\). Member states had to adapt their legislation to these new

\(^1\) Directive 2002/20/EC on the authorisation of electronic communications networks and services; Decision 676/2002/EC on a regulatory framework for radio spectrum policy in the European Community; Commission Recommendation 2003/203/EC on the harmonisation of the provision of public r-lan access to public electronic communications networks and services in the community.
European directives. However, these directives tackle the problem of the “public” management of WLAN networks and do not directly tackle our problem.

**Relationship between A and B – Civil Aspects**

The applicable dispositions stemming from the civil law area are similar to the ones in Switzerland given that the origin of both legislations is the same and comes from the Roman law. Accordingly, A disposes of an action to protect his possession from the disturbance of other parties (Art. 2282 e 2283 French Civil Code, thereafter FCC). He can also invoke the actions stemming from the rights between neighbors (Art. 651 FCC and Law on Rural Police), and the regulation about tenants of a same building (Art. 1719.3 and 1721 FCC).

The developments previously exposed for the Swiss regulation are also applicable, mutatis mutandis, to the French regulation. However, the general norm on illicit acts states that “any act whatever of man, which causes damage to another, obliges the one by whose fault it occurred, to compensate it” (Art. 1382 FCC). This is a clear manifestation of the subjective theory of what constitutes an illicit act discussed before. As a result, in principle these norms are applicable to our case even tough it remains to be solved the problem of proving that a damage has occurred.

**Relationship between A and B – Penal Aspects**

With regard to the penal aspects of our case, we can refer the French Penal Code which asserts that “Fraudulently accessing or remaining within all or part of an automated data processing system is punished by one year’s imprisonment and a fine of € 15,000. Where this behaviour causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is two years’ imprisonment and a fine of € 30,000” (Art. 323.1 French Penal Code, thereafter FPC). While the conditions of application are less severe than for the counterpart in Swiss law, as it is sufficient to introduce in an informatic system to incur the sanction, in our case there is no clear sign of a fraud except if there have been protections which must have been cracked.

Remark that the French law (article 323.2 FPC) punishes the interference in another system: “Obstruction or interference with the functioning of an automated data processing system is punished by three years’ imprisonment and a fine of € 45,000”. Using WLAN frequencies to enter in another system and exploit part of its connection can be considered as punishable with this article? It might, depending on the subjective interpretation of judges.

Finally, the post and telecommunication code (art. L39-1 PTC), applies an imprisonment of 6 months and a fine of 30'000 euro for those who perturb a radio-electric equipment.

**Relationship between ISP and A**

In France there is a strong movement which has emerged in favour of free community networks aiming at sharing a wireless Internet access between the various members of the community. From a legal point of view, WLAN community networks are permitted only if the Internet Service does not oppose to such practice and agrees in the contract stipulated with the subscribers that his connection may be shared with third parties.

If A consciously decides to open his network to other parties, he may be considered to commit a fraud (Art. 313-1 FPC). In fact, the definition of fraud is larger than the one retained in the Swiss code as it includes not only act that cause a diminution of the patrimony of the victim, but also the provisioning of a service. If the ISP has agreed, according to the indications of A contained in the contract between the two parties, to grant a service intended to his exclusive use, and A had known that he would have shared his access with other parties, he would be considered as punishable of fraud and risks a maximum punishment of 3 years of arrest and a fine of 375'000 euro.

Finally, proving WLAN networks open to the public is admitted only with the previous authorization of the telecom regulatory authority. If someone decides to manage an open network without the consent of the authority, he may incur a fine of up to 75'000 euro.

**5. Conclusions**

The brief overview of two regulatory regimes contained in this paper suggests that the law appears to have some difficulty to adapt to the development of new technologies and the resulting situations. This creates a sort of grey legal area where there are several legal uncertainties about what the applicable laws are and consequently what behaviours are allowed.

This is certainly the case of the sharing of Internet access through WLAN networks. Our analysis does indeed show that there are no clear and convincing answers, at least in the Swiss and French law codes. Moreover, there is not yet a jurisprudence body on this matter. At this time, one can only formulate reasonable hypothesis about what shall be acceptable on the basis of common sense or similar cases. Nevertheless, the
verification of these hypotheses must wait until some courts pronounce themselves with regard to this matter.

From this analysis, it appears that Internet access sharing through WLAN networks and wireless communities are only lawful with the consent of the ISP. The consent must be explicitly stipulated in the contract between the ISP and the user. This is not currently the case with most of the ISPs, but there are actually some that do agree with such practices.

If this is not the case and the subscriber leaves his network unsecured and hence open to third parties, he can be held responsible for the eventual damage caused to the ISP and for the acts of third parties that use his networks. In this case, the ISP may therefore intervene to stop the situation by breaking the contract or force the user to cease the sharing by installing suitable security mechanisms. He may also ask for damage reimbursement. The user may appeal to his good will: his position would be worse if he had consented to the sharing. In this case, third parties who unduly gain free internet access do not risk penal sanctions and it is questionable whether they may incur civil sanctions.

The situation is somewhat different if the WLAN owner secures his network, perhaps even superficially. In this case, the attacker must bypass some security mechanisms in order to break into the system and may therefore risk the penal sanctions of up to three years imprisonment as well as large fines which have been set up for hackers in addition to the reimbursement of damage. Remark that this may apply even if the access is easy such as in the case in which the attacker uses widely available tools such as airSnort to break WEP encryption in a matter of minutes.

We are aware that the law does not provide certain answer to the questions raised in this paper. We think it is useful to start reflecting on appropriate responses to the problem. Of course, this might be a recalibration of the legal frameworks: new rules that apply to this issue may be proposed. However, we do not believe that this is justified. In effect, current laws already protect users that do not protect themselves shall not be protected for risks that they do not try to avoid. The ISP is also currently protected in all cases. We believe that users that do not protect themselves shall be protected against third parties and to educate users to secure their networks.

Acknowledgements

The work presented in this paper was supported by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005-67322. The authors also thank Prof. Ariane Morin for the interesting insight provided.

References