Kluwer Copyright Blog

CJEU AG suggests that free Wi-Fi providers may not be ordered to password protect their networks

Christina Angelopoulos (CIPIL, University of Cambridge) · Thursday, April 14th, 2016

On 16 March 2016 the CJEU's Advocate General Szpunar handed down his Opinion in case C-484/14, *Mc Fadden*. The case concerns the liability of Tobias Mc Fadden, the owner of a business selling lighting and sound systems in Munich. Mr Mc Fadden operates a Wi-Fi hotspot on the business' premises, deliberately left unprotected by a password, so as to enable free public access to the internet. In September 2010, that internet connection was used for the unlawful download of a musical work by one of the network's anonymous users. The owner of the relevant copyright, Sony Music, decided to bring an action against Mc Fadden, seeking both damages and an injunction.

Are these claims viable? Under German copyright law, a distinction must be made between so-called *Täterhaftung*, i.e. full liability that allows both for the allocation of damages and injunctive relief, and *Störerhaftung*, that holds a party liable as an "interferer" or "disturber" and allows only for injunctive orders to be issued (see Article 97 of the *Urheberrechtsgesetz*, the German copyright act). While the *Landgericht München I*, the regional court hearing the case, rejected the possibility of *Täterhaftung* against Mc Fadden, precedent emanating from the *Bundesgerichtshof* (BGH), Germany's federal court of justice, does suggest that a finding of *Störerhaftung* should be possible: in the 2010 case of *Sommer unseres Lebens*, the BGH had found a private person operating a Wi-Fi network to be an "interferer" and therefore open to injunctions, as he had failed to make the network secure by means of a password and thus allowed third parties to use it to infringe copyright.

Is this outcome compatible with EU law? Before applying this precedent and finding against Mc Fadden, the Munich court submitted a series of 9 questions to the CJEU with a view to verifying precisely this question.

The applicability of the EU's mere conduit safe harbour

The first set of questions submitted by the Munich court concerned the applicability to the material case of Article 12 of the EU's E-Commerce Directive, the "safe harbour" provision that protects so-called "transmission" or "mere conduit" services. Under Article 12 of the E-Commerce Directive, the provider of such a service cannot be held liable for any information it transmits, as long as it: (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.

The Munich court queried whether the safe harbour was applicable to the situation at hand, given that: a) under Article 2(a) of the E-Commerce Directive that directive only applies to services "normally provided for remuneration"; and b) Mc Fadden had not held himself out to potential users as a mere conduit service provider.

With regard to the first of these questions, the Advocate General suggested that the reference to services "normally provided for remuneration" must be understood as denoting services "of an economic nature". He then went on to explain that, according to settled CJEU case-law, a broad interpretation is appropriate in this regard. So, the AG noted that access to the internet may constitute a form of marketing, that Mc Fadden was offering the service in an economic context and that pecuniary consideration was incorporated into the price of other services supplied – all of which facts combine towards the conclusion that the provision of the Wi-Fi hotspot should be understood as constituting an economic activity.

As for the notion of "providing" access to the internet, the AG observed that this should encompass all cases of activity that enables the public to have access to a network in an economic context. The matter is thus an objective one, not influenced by how the person offering the service presents himself to others. And, while the German word "anbieden" might suggest a narrower interpretation, this was not supported by other language versions.

As a result of the above, Article 12 of the E-Commerce Directive is, in the opinion of AG Szpunar, to be understood as applicable to the case at hand: a person operating a Wi-Fi network accessible to the public free of charge may benefit from the protection of the mere conduit safe harbour.

The liability of a mere conduit provider

The mere conduit safe harbour having been found to be applicable to the provision of free, public Wi-Fi networks, the next question to examine concerned the extent of the protection this confers. Consistent with the objective pursued by that provision and the surrounding directives, the AG explained that that protection should be understood as extending not only to claims for compensation, but also to any other pecuniary claims that entail a finding of liability for copyright infringement, such as claims for the reimbursement of pre-litigation costs or court costs.

However, as is clear from Article 12(3) and Recital 45 of the E-Commerce Directive, as well as from Article 8(3) of the Copyright Directive and Article 11 of the Enforcement Directive, what the mere conduit safe harbour does not immunise intermediaries against is injunctive relief – as long as that does not entail a finding of civil liability against the intermediary for copyright infringement. The AG also made clear that, in his opinion, the non-applicability of the safe harbour to injunctions should be understood as including any penalties that attach to non-compliance with an injunction, such as fines.

In this way, the issue was narrowed down to one crucial question: if a Wi-Fi provider is a mere conduit provider, but the mere conduit safe harbour does not protect it from injunctions, what kind of injunctions may be issued against it by the national courts? This is where the Opinion gets really interesting.

The scope of permissible injunctions

According to Recital 59 of the Copyright Directive, the conditions and modalities relating to injunctions issued against internet intermediaries should be left to the national law of the Member

States. At the same time, as AG Szpunar emphasised, certain limitations with regard to the scope of these injunctions do emanate from EU law. Those limitations have, according to the AG, three main sources:

- **Article 3 of the Enforcement Directive**, according to which measures taken for the enforcement of copyright must be fair, equitable, effective, proportionate and dissuasive, not unnecessarily complicated or costly, not entail unreasonable time-limits or unwarranted delays and applied in such a manner as to avoid the creation of barriers to legitimate trade and provide for safeguards against their abuse;
- **Articles 12(3) and 15(1) of the E-Commerce Directive**, according to which such measures must, respectively, be aimed at preventing or bringing a specific infringement to an end and not entail a general obligation to monitor the information which they transmit or store;
- previous CJEU case law, according to which, in the application of the abovementioned provisions, Member States should strive to achieve a **fair balance between all relevant fundamental rights** protected by the Charter of Fundamental Rights of the European Union and in particular: (a) the right to intellectual property, protected by Article 17(2) of the Charter; (b) the freedom of the intermediary to conduct its business, protected by Article 16 of the Charter; and (c) the right of end users to receive and impart information, protected by Article 11 of the Charter.

On this basis, the AG considered the particular terms of the injunction contemplated by the national court.

First and foremost, the court queried whether an injunction issued against a Wi-Fi provider may be formulated in general terms, obliging the provider to achieve a result without prescribing the technology that must be adopted to this end. The AG conceded that the CJEU's previous case law does point towards a positive answer: in the controversial judgment of *UPC Telekabel Wien*, the CJEU had found that so-called "outcome injunctions", which require intermediaries to achieve a given result without specifying the specific measures that should be taken to this end, are compatible with EU law.

At the same time, the AG also underlined that prohibitory injunctions that are formulated in general terms can be a source of significant legal uncertainty for the addressee. The fact that the addressee will be entitled (as *Telekabel* made clear), in any proceedings concerning an alleged failure to comply with the injunction, to show that it has taken all reasonable measures to achieve the prescribed outcome does not entirely remove that uncertainty. Moreover, while in *Telekabel* the CJEU had suggested that it is for the addressee of such an injunction to make sure that, in its choice of measures adopted to comply with the injunction, disproportionate interferences with the fundamental right of internet users to freedom of information must be avoided, the AG now took the opportunity to clarify that, in principle, determining what measures strike a fair balance between the various fundamental rights involved is a task that ought, for the main part, to be undertaken, not by the addressee, but by a court.

Accordingly, the AG observed that "outcome injunctions" should only be possible when it is clear that measures do in fact exist that would enable the provider to achieve the specified result. In such cases, allowing the provider the freedom to choose the measure can provide an advantage that is in line with its freedom to conduct a business. That was the case in *Telekabel.* However, as the AG pointed out, in the case now at issue, whether such measures exist is a subject of considerable

doubt. With this in mind, the AG emphasised that, while a national court may, under certain circumstances, issue an injunction which leaves it to its addressee to decide what specific measures should be taken in pursuit of an objective, it nevertheless must fall to that court to first ensure that appropriate measures do indeed exist that both enable that objective and are consistent with the restrictions imposed by EU law.

On this basis, the AG then went on to examine the specific measures contemplated in the material case by the national court. Those were three:

- the termination of the internet connection;
- the examination of all communications passing through that connection; and
- the password-protection of the internet connection.

All three of these options the AG rejected as incompatible with EU law. The first is manifestly incompatible with the need for a fair balance to be struck between the fundamental rights involved, since it compromises the essence of the provider's freedom to conduct business. Such a measure would also be contrary to Article 3 of the Enforcement Directive, as it would create a barrier to legitimate trade.

Likewise, the second measure would clearly conflict with the prohibition on imposing a general monitoring obligation, as laid down in Article 15(1) of the E-Commerce Directive. The AG confirmed that, in order to constitute a non-general monitoring obligation that would be permitted under Article 15(1), the measure in question must be limited in terms of the subject and duration of the monitoring. As has been made clear in the CJEU's previous rulings in *Scarlet Extended* and *Netlog*, that would not be the case with a measure that entailed the examination of all communications passing through a network.

The analysis surrounding the final option of password-protection was somewhat more complicated. The AG began by noting that imposing an obligation to make a Wi-Fi network secure entails, for persons who operate that network in order to provide internet access to their customers and to the public, a need to register users and to retain their data. The AG observed that the introduction of such an obligation could potentially undermine the business model of undertakings that offer internet access as an adjunct to their other services: if it necessitated investment and attracted regulatory constraints relating to the securing of the network and the management of users, some such businesses might no longer be inclined to offer that additional service. Indeed, adopting such measures could endanger the status of the intermediary as non-active, a condition for enjoying the immunity conferred by the mere conduit safe harbour. In addition, some users would give up the service if it necessitated a systematic obligation to identify themselves and enter a password.

Thus, while such an obligation might be reasonable when applied to telecoms operators, when applied to persons offering internet connectivity as an adjunct to their main activity, it becomes disproportionate. This is especially so, given that of itself the measure would not be effective: it might limit the circle of users, but does nothing to prevent infringement. And, while advanced systems could achieve greater effectiveness, this would only be at the cost of the protection of privacy and the confidentiality of communications.

The AG concluded by noting that the ultimate result could, in practice, prove a net negative for society as a whole, by discouraging easy access to the internet. Ultimately, he concluded that the imposition of an obligation to password-protect a free, public internet connection would be

inconsistent with the requirement of a fair balance between all fundamental rights involved.

In the final analysis, the AG advised against the imposition of damages on the Wi-Fi provider, against the imposition of injunctions phrased in general terms where it is unclear that measures that can achieve the outcome in question exist and against the imposition of injunctions ordering any of the three specific measures contemplated by the national court. If the national court wants to order a different kind of injunction, it has to make sure that appropriate measures do exist that are consistent with EU law.

It is to be hoped that the CJEU will follow this advice: if so, not only will it put an end to the dubious (in view of the EU Charter) banning of open Wi-Fi connections in Germany over the past few years, but will also go a long way to dissipating the uncertainly that was raised by the wording of the CJEU's judgement in *Telekabel* regarding generally-phrased "outcome" injunctions: as AG Szpunar emphasises, such injunctions should certainly be possible, but only when equally fairly balanced options have been ascertained to exist – deciding whether that's the case or not should be a matter, not for the private entities that are the intermediaries, but for the courts of law.

This entry was posted on Thursday, April 14th, 2016 at 12:35 pm and is filed under AG Opinion, Case Law, inter alia, for ensuring that EU law is interpreted and applied in a consistent way in all EU countries. If a national court is in doubt about the interpretation or validity of an EU law, it can ask the Court for clarification. The same mechanism can be used to determine whether a national law or practice is compatible with EU law. The CJEU also resolves legal disputes between national governments and EU institutions, and can take action against EU institutions on behalf of individuals, companies or organisations.">CJEU, Enforcement, European Union, Germany, Infringement, Injunction, Liability, Remedies
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.