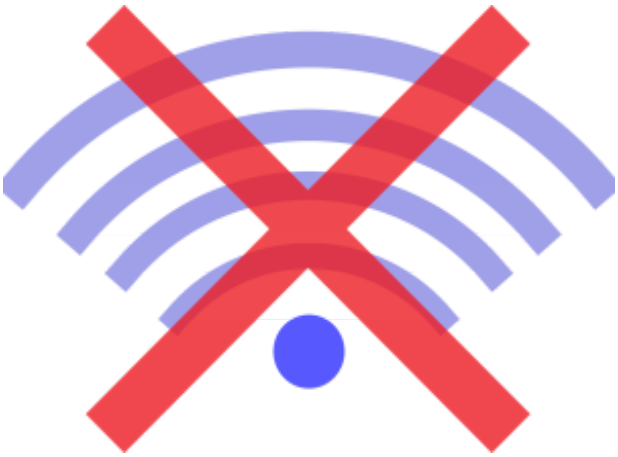
Kluwer Copyright Blog

Mc Fadden Drills Another Hole in the E-Commerce Directive

Martin Husovec (London School of Economics) · Thursday, September 29th, 2016



The last two weeks were truly hard for the future of the digital economy in Europe. First, the European Commission officially declared its regulatory capture. Then the CJEU provided us with a great set of hyperlinking clarifications for their daily use. Now it is completely clear, who, when, and how one can link to avoid liability or licensing. It just takes about 12 steps and 24 new preliminary references. Perhaps after the famous public domain calculator, we might soon need a neat *hyperlinking calculator* (any volunteers?). And as if this weren't enough, a few days later, the same Court caused the weakening of the E-Commerce Directive in *Mc Fadden* C-484/14. What is going on?

To be sure, I am not blaming the CJEU for any tendencies. The Court seems to overall be doing balanced work. However, increasingly it attempts to get things so surgically right in the short-run that it ends up getting them terribly wrong in the long-run. The problem appears to be that the Court's policy outlook does not seem to stretch beyond the nearest preliminary reference. But make your own call regarding the *Mc Fadden* case.

Background

Back in 2010, the German Federal Supreme Court (BGH) in its *Sommer unseres Lebens* judgment (I ZR 121/08) required most of the WiFi operators to password-protect their connections in order to avoid any third-party copyright infringements. The dispute in *Mc Fadden* arose just a couple of months after this judgment, between an entrepreneur selling light and audio systems, Mr. Mc Fadden, who is also a member of the German Pirate Party, and a well-known record label.

The entrepreneur operates an open and free-of-charge WiFi in his store. He uses the WiFi sometimes as a tool for advertising his store (the preloaded home page points to his shop and the name of the network bears its name) and sometimes to agitate for his political views (pointing to particular websites such as data protection campaigns, etc.). After receiving a letter informing him about a copyright infringement allegedly committed via his hot-spot, the entrepreneur unusually sued the right holder pursuing a negative declaratory action. The right holder as a defendant later

counter-claimed asking for damages, injunctive relief and pre-trial costs as well as court fees.

The referring court in Munich was hesitant as to whether the mere conduit safe harbour of Article 12 of the E-Commerce Directive specifically allows injunctive relief on which the German concept of *Stoererhaftung* is based. The referring court came to the conclusion that the plaintiff did not infringe the rights himself, and thus considered what kind of measures can be imposed on a WiFi operator such as the plaintiff. Given the BGH ruling from 2010, certain choices were obvious, though their compatibility with the EU law wasn't clear.

The preliminary reference thus raised a number of important questions: (1) under what circumstances are free-of-charge services covered under the term 'information society service'; (2) are open wireless operators 'mere conduits' in the sense of Art 12 ECD; (3) what is the scope of exempted 'liability' under such a safe harbour; (4) what is the scope of exemptions for injunctions that are permitted by Art 12(3) ECD even if safe harbours are applicable; and (5) how compatible are the enforcement measures consisting of (a) monitoring of passing third-party communication, (b) termination of his Internet access and (c) password-protection of the open WiFi.

Open WiFi as a Service and Mere Conduit

The Court and AG accepted that the E-Commerce Directive applies to open WiFi that also serves as a form of advertising. They also accepted that provision of an open WiFi constitutes 'the transmission in a communication network of information' as required by Article 12 of the E-Commerce Directive. Although the referring court tried to interpret additional requirements into the provision, the Court rejected this agreeing with the Advocate General that there are only three cumulative conditions in that provision; namely that (1) the service at issue provides access to a communication network which (2) does not go beyond the boundaries of a technical, automatic and passive process and (3) he has neither knowledge of, nor control over, the information which is thereby transmitted or stored (paras 61, 64). In particular, the Court explicitly rejected the creation of a new knowledge requirement known from the hosting safe harbour. It held that 'the EU legislature struck a balance between the various interests at stake' and 'it is not for the Court to take the place of the EU legislature by subjecting the application of that provision to conditions which the legislature has not laid down' (paras 68-69).

What Type of Liability is Exempted?

One of the main points of the preliminary reference was the question of what type of claims are actually exempted by the language of the E-Commerce Directive. Art 12(1) ECD provides that the 'Member States shall ensure that the service provider is not liable for the information transmitted'. However, what constitutes such 'liability'?

The stance of the AG would erase these incentives and thus substantially reduce the application of password locking measures. The Advocate General argued that any other finding 'could compromise the objective pursued by Article 12 of Directive 2000/31 of ensuring that no undue restrictions are imposed on the activities to which it relates' (para 77). The mere conduits, in his view, 'may incur liability only after a specific obligation contemplated by Article 12(3) of Directive 2000/31 has been imposed on him' and thus not before the safe harbour is lost or an injunction granted. This reading would still allow the imposition of costs for non-compliance with injunctions in the follow-on enforcement (para 90, AG opinion). It would also leave the currently prevailing practice of allocating costs of website-blocking intact. After all, these are also costs that

are incurred *after* an injunction is granted by an authority.

The Court, however, rejected this sensible interpretation. And by doing so, it drilled yet another hole into the E-Commerce Directive framework. It has ruled that although both pre-trial costs and litigation costs are forms of 'liability' in the sense of Art 12(1) (paras 74, 75), given that the injunctive relief granted by the court or an administrative authority is exempted from this in Art 12(3), the costs associated with it also have to be exempted (para 78). This is a very short-sighted and non-systematic choice of reading. It cracks the armour of liability exemption beyond legislated injunctions. It basically allows the imposition of monetary compensation even *before* any permitted injunction is granted by an authority and even *without* an application ever being made to such an authority. At the same time, it opens up new ways to circumvent the E-Commerce Directive (for more see the paper linked below).

Which measures are compatible?

In the subsequent step, the Advocate General examined three anticipated measures. First, it opined that a measure requiring termination of access clearly compromises the very *essence* of a right to conduct a business of a person who provides internet access, even if only in ancillary fashion (para 131). According to the AG, such a measure would also be incompatible with Art 3 of the Enforcement Directive, which prohibits enforcement of IP rights by measures that create obstacles to legitimate trade. The Court accepted this reading and ultimately rejected such measures, but without reference to the Enforcement Directive. Second, the Advocate General then also very briefly analysed the measure that would require the monitoring of all passing internet communication. He opined that such a measure is incompatible with Art 15 of the E-Commerce Directive, which prohibits general monitoring (para 132). The Court again fully accepted this.

However, the judges had a mind of their own regarding password-locking. They held that although such password-locking interferes with freedom to conduct business and freedom of expression, it does not damage their essence, and only marginally limits them (paras 90-92). This is in particular because open wireless is only one of the means to access information online and thus any passphrase authentication does not entirely prevent access. Because of this, unlike in scenarios of website-blocking, the password-locking 'does not appear to be capable of affecting the possibility made available to internet users using the services of that provider to access information lawfully, in so far as the measure does not block any internet site' (para 94). The Court reiterated its earlier *UPC Telekabel* finding that the threshold of effectiveness is not particularly high. Applying it to the measure of password-locking, the Court noted the following (para 96):

'the Court finds that a measure consisting in password-protecting an internet connection *may* dissuade the users of that connection from infringing copyright or related rights, *provided that those users are required to reveal their identity in order to obtain the required password* and may not therefore act anonymously, a matter which it is for the referring court to ascertain' (emphasis mine)

In other words, the Court seems to suggest that password-locking that is not bundled with identification of users wouldn't be considered an effective measure to begin with. So merely handing out the password on a menu of a local restaurant wouldn't be seen as sufficient. This could mean that password-locking injunctions against open wireless operators have to (sic!) require that the password is shared with the customers only upon their personal identification. If widely implemented in the Member States, it could make anonymous use of third party open wireless

practically impossible. The contrast is striking: while the Advocate General warned against this effect of password-locking, the Court actually seems to require it as a precondition of its effective implementation.

McFadden is a very rich decision. Its consequences for the scope of the E-Commerce Directive are substantial. Although the Advocate General prepared high quality analysis which interpreted many provisions in light of their initial purpose and in the social context, the Court has decided to deviate on two important points. First, by exempting monetary claims, even if an intermediary is covered by a safe harbour; and second, by generally allowing password-locking enforcement measures which require identification of users. Forecasting the effect of the decision is not easy. It is clear that some countries will be impacted by its rulings more than others, depending on their current enforcement set-up and vulnerability to future political pressures.

If you want to learn more about the broader consequences of the decision for the E-Commerce Directive framework, I encourage you to have a look at my upcoming brief article with JIPLP – **'Holey Cap! CJEU Drills (Yet) Another Hole in the E-Commerce Directive's Safe Harbors'** (working version available on SSRN here).

This entry was posted on Thursday, September 29th, 2016 at 4:39 pm and is filed under 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, 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.