

Where do you sue over an app?

With more computer programs being run over the internet through mobile apps, jurisdiction is increasingly important in infringement cases. **Larry Cohen, Steven James, Christian Engelhardt** and **Charles Courtenay** explain the situation in Europe, and compare it to the United States

One of the few constants in technological development has been spatial change. The physical distance between the software and hardware constituents of mobile applications has increased as technological advances have given greater freedom as to from where applications can be operated. It is now common for consumer telecoms companies to have their operating hubs in one country, while the users of their services are located in multiple jurisdictions. Mobile apps are no exception. Establishing jurisdiction for IP rights disputes can be challenging at the best of times: apps, with their content often based in the cloud or a server offshore, could make this task even more complicated.

How apps work

Mobile apps are software programs that run on mobile devices, typically smartphones and tablets. Mobile applications work in the same manner as a web browser by communicating over the internet – some use internet protocols to communicate, others run entirely on a mobile device without the need for server support. They usually comprise three layers – a data layer, a business logic layer and a user interface. When mobile apps interact with a server, there is also a need for a communication and transport layer.

There are various IP rights which are likely to subsist in mobile apps, depending on the nature of the application. They include copyright (in the text, logos, graphics, sounds, (moving) images and source code of the app), patents (such as novel functions of the app), registered and unregistered design rights (in the 2-D icons and features of the apps) and trade mark rights (in slogans, logos and, possibly, the name of the app itself). Database rights might also be involved in the operation of the app.

Jurisdiction

In Europe, in order to determine whether a court has jurisdiction, it must be asserted under the European regime (the Brussels Regulation). Then if jurisdiction is not obviously applicable, the common law rules as to jurisdiction apply. (For the view from the United States, see box opposite.)

Under Article 2 of the Brussels Regulation, the basic rule is that the claimant should sue in the domicile of the defendant. There are however exceptions. A claimant can sue where the “harmful event” or “damage was suffered” – so where the infringement of intellectual property occurred (article 5(3)) while under article 22(4), the validity of IP rights (most notably patents and registered trade marks) must be tried in the country of registration – whether this is raised as a claim or a defence.

From a jurisdictional perspective, arguably the two most important rights to consider in relation to apps are patents and copyright.

Patents

The key issue with patents (and registered trade marks) is that jurisdiction is conferred on the place where the right is registered and in the case of Community trade marks, where the defendant is domiciled. This acts as an exception to the general rule under the Brussels Regulation, that the defendant can primarily be sued in the place of his domicile, and secondly, where the harmful act occurred.

Jurisdictional rules were first put to the test in the UK in *Menashe Business Mercantile & Anor v William Hill Organisation* (2003). The proceedings related to an online gaming system based upon a “terminal computer” or “player stations” (which were essentially the users’ internet-connected PC) and a host computer (the server). William Hill supplied the UK punters with a program on a disc to enable their PCs to operate as “player stations”. William Hill was accused of indirect or contributory

One-minute read



Mobile applications, or apps, are increasingly used both on smartphones and computers as a way to run software through a connection with remote operating hubs. This makes the establishment of jurisdiction in IP infringement cases concerning software harder than ever. Of the many IP rights that can subsist in apps, patents and copyright are the most important. Case law in the UK has been among the most progressive in Europe, though the implications for copyright and patents are rather different.

State law in the United States

In the United States, there is little case law regarding the jurisdictional implications of cloud computing specifically, but a number of courts have addressed the implications for accessing servers in different jurisdictions. As the issue of jurisdiction is one of individual states across the US, these cases refer equally to ideas of jurisdiction over international parties or servers.

The cornerstone of these cases, whether domestic or international, is whether the defendant “purposefully availed itself of the privilege of conducting activities” within the jurisdiction. A court would probably not find that a defendant “purposefully availed” itself without having reason to know the location of the server.

FCStone v Buckley, for example, was a trade secret case in which it was held that the defendant could not have “purposefully directed its activities” with the “mere passage of emails through a server in Iowa” since the defendant did not know that the server was based in Iowa

and only transacted business with the plaintiff in Illinois. In *Ray v Experian* in 2007 the judge ruled that “accessing or sending [a South Carolina plaintiff’s] data . . . to or from a database which happens to be headquartered in Texas is not a *purposeful* availment by [the defendant] of the benefits and protections of Texas’ laws”.

Courts have often found that the defendant “purposefully availed” itself of the server’s jurisdiction if it knew the plaintiff’s principal place of business was in that jurisdiction or could foresee the effects of the disputed action occurring in that jurisdiction. In *Sky Capital Group v Rojas* in 2009, for example, it was ruled that the defendants’ activities were “expressly aimed” within the server’s jurisdiction since they had prior dealings with the plaintiff’s principal place of business, regardless of whether the defendants actually knew the server’s location. In *Rightthing v Brown* in the same year, the defendant was said to have “purposefully avail[ed]” herself of the server’s

jurisdiction by “reach[ing] [the jurisdiction] through her computer wires” since she knew the plaintiff’s principal place of business was in that jurisdiction. Lastly in *Abatix v Capra* in 2008, it was found that jurisdiction existed since the defendant caused a “tortious injury within the state” by “specifically direct[ing] their actions at [the plaintiff’s] server” within that jurisdiction.

With respect to patent claims, Congress has not redefined the scope of jurisdiction in a different manner to other causes of action. Courts therefore use the same standard for finding jurisdiction in patent infringement cases, namely whether the defendant purposefully availed itself of the forum.

In summary, the test in the United States is whether the defendant purposefully availed itself in entering the jurisdiction in which it is being sued, or whether its infringing content happened without the knowledge or input of the defendant to reside on a server in that jurisdiction.

infringement in its supply to its customers (in the UK) of CD ROMs that allowed the customers to access a server located overseas. Under UK patent law, contributory infringement is governed by section 60(2) of the Patents Act 1977 which states that a person (other than the proprietor of the patent) will infringe a patent if, while it is in force and without the proprietor’s consent, he supplies or offers to supply a person (other than a person entitled to use the invention) the “means essential” to put the invention into effect – when he knows or has constructive knowledge that those means are suitable for putting and are intended to put the invention into effect in the UK.

The Court of Appeal in *Menashe* ruled that the supply of the “means essential” must take place in the UK, but also that the customer (subject to the essential means) should also be a primary infringer in that country. Such primary infringement by a customer would be satisfied under 60(1)(a) if the infringer/customer for the purposes of mobile applications “makes, disposes of, offers to dispose of, *uses* or imports the product or keeps it”. Lord Justice Aldous particularly focused on the idea of the customer(s) ‘use’, stating: “Where does he (the customer) use the gaming system? There can be no doubt that he uses his terminal in the United Kingdom, and it is not a misuse of language to say that he uses the host computer (the server) in the United Kingdom...even though it is situated in Antigua and operates in Antigua.” The location of the server was deemed not to be relevant and the pertinent question was who used the gaming system. Having established that the system was being used in the UK, it was straightforward for the Court of Appeal to establish that the supply of CD ROMs to customers in the UK would constitute contributory infringement.

The point came up again in a case relating to mobile devices, *Research in Motion UK v Motorola* (2010), where the High Court held that a patent owned by Motorola relating to a method of providing messages, including e-mail, over wireless networks to an individual device such as a mobile phone was

invalid and not infringed by the BlackBerry systems of Research in Motion. Justice Arnold held that the fact that the server for one of the accused BlackBerry systems was located in Canada meant that that system could not infringe the UK method patent either as a process under 60(1)(b) of the Act, or through the supply of “means essential” under 60(2). The difference between this case and *Menashe* was that in *Menashe*, a product was claimed, and the user was able to use the claimed system in the UK because of the supply of the software which enables the customer to put it into effect in the UK – it did not matter that the server was not in the UK.

Arnold noted that the key questions in such cases are: (1) who uses the claimed system? (2) where did they use it? In RIM’s case, it was RIM who used the claimed system and did so in Canada, and therefore did not infringe the UK patent. While these are simple questions they are driving at an overarching principle – namely, where is the infringement controlled from? The findings in these cases could equally apply to a claim relating to an app, given the nature of the technology behind it and the dynamics of the provider’s relationship with the user. Just as in *Menashe*, an app uses a user’s computer (a smartphone), and connects to an external server; and a developer provides the app to the customer, thus enabling this connection to be established. They could therefore be liable for offering a product or process (the app itself, or a service, depending on how the app is construed) or for contributory infringement under section 60(2).

There is little doubt that a mobile phone hosting the app would be considered a standard item of commerce, or “staple commercial product” under section 60(3) of the Act, and that the customer may have a defence under section 60(5) if its use of the app is for non-commercial, private use. Even the supply of the app itself may not be an infringement, if it does not carry out the functions claimed in the invention, and merely acts as a “gate-keeper” or facilitator to enable the functions to be carried out.

What is key is where the infringement takes place, and this

