Internet Jurisdiction

The internet touches every country in the world and the lives of some two billion people worldwide who use it. The internet's universality is a great part of its strength as a tool for business, but that universality also creates unique business risks. Worldwide access exposes website operators and internet publishers to the possibility of being haled into courts around the globe. A business operating online must therefore account for the risk of being sued in a distant jurisdiction that may provide very different rights and responsibilities than the jurisdiction the business considers its "home."

Court opinions in the EU and worldwide have begun to define the determination of internet jurisdiction by drawing upon legal theories established for jurisdiction, but the internet has created some legal issues that the courts have never before confronted and for which there are no easy solutions.

This concept paper provides an overview of the risks facing businesses in the online space and a description of recent efforts by courts and regulators to diminish that risk—or at least make it more predictable.

The analysis of the treatment of internet jurisdictional issues by legislative bodies in the European Union and in the United States should serve as good examples of dealing with different jurisdictional approaches.

1) The European Union

- E-Commerce Directive

The E-Commerce Directive, which applies only to electronic commerce activities (and more particularly, "information society services") within the EU, suggests that companies should be subjected to the jurisdiction and the law only of the Member State in which they are "established":

This principle is sensible because only the country in which a publisher is "established" can fully regulate its activities. It also is a concept that is sensitive to general principles of international law, discussed below, which recognize that one state should not prescribe its laws in a manner that interferes with a sister state's ability to prescribe its own laws.

- The Audiovisual Media Services Directive - the country of origin principle

The Audiovisual Media Services Directive (the "AVMS Directive") amends and modernizes the older Television without Frontiers Directive. According to its own terms, the core of the AVMS Directive is the country of origin principle. This principle states that "only one Member State should have jurisdiction over an audiovisual media service provider." The Directive makes clear that the principle is "essential for the creation of an internal market," "[ensures] legal certainty for media service providers," and "[ensures] the free flow of information and audiovisual programmes in the internal market."

A Member State has jurisdiction over a provider if the provider is established in that Member State. A media service provider is established in a Member State if:

- Both the head office is located and editorial decisions are taken in that Member State;
- A significant part of the workforce operates in that Member State and either the head office is located or editorial decisions are taken in that Member State; or
- Although editorial decisions are taken in a non-Member State, both the head office is located and a significant part of the workforce operates in that Member State.

Even if a media service provider is not established in a Member State under Article 2(3), Article 2(4) of the Directive still permits the Member State to exercise jurisdiction over the provider in certain other cases, including if the provider uses a satellite up-link located in the Member State.

- "single point of publication" rule

An attempt to make the "country of origin" approach more precise is the advocacy of a "single point of publication" rule to determine which country's law should apply to a particular content claim. Under this approach, claims would be governed by the law of the nation in which the publisher last had an opportunity to exercise editorial control over the publication. This proposal, which members of the U.S. media industry have advanced before the European Commission and the High Court of Australia in an *amicus curiae* brief in the *Gutnick* litigation, is designed for an internet publishing environment in which content can be viewed instantaneously in many locations but there is only one place from which the publisher controls content as a final matter (that is, the point at which final editorial decisions are made and final technical work is done to upload the material). The advocates of the "single point of publication" rule point out that proposal accounts for the widespread phenomenon of inadvertent digital publishing - even publishers who attempt to prevent their publications from being distributed in certain countries may not be able to control circulation completely, especially if a publisher releases content online. The content may be forwarded without the publisher's consent to other individuals, or it may be re-circulated at a later point in time by others.

- the country of destination principle

One of the most expected changes likely to be introduced by the new EU Data Protection Regulation proposed by the European Commission is the criteria to determine the applicability of EU law. Under the current Data Protection *Directive*, the rules are essentially as follows:

* If the controller is based **in an EU Member State** (e.g. Acme (UK) Limited based in the UK), that controller will be subject to the law of that Member State (e.g. the UK Data Protection Act) and to the scrutiny of the regulator of that country (e.g. the UK Information Commissioner).

* If the controller is based **outside the EU** (e.g. Acme Inc.) but uses equipment (e.g. servers or people's computers) to collect information, that controller will be subject to the laws of every single Member State and to the scrutiny of each and every regulator.

However, the rule that determines the applicability of the law to non-EU controllers produces bizarre situations like the potential application of EU law to organisations that have no

presence, employees or customers in the EU but happen to engage an EU-based service provider (with equipment in Europe), or like the non-application of EU law to organisations who may be dealing with millions of Europeans over the Internet but have no real processing equipment in the EU.

Therefore, under the proposed Data Protection *Regulation*, the rules would be as follows:

* If the controller is based **in an EU Member State** and it has one main establishment (e.g. Acme (UK) Limited based in the UK), then it will still be subject to the Regulation but it will only be subject to the scrutiny of one regulator (e.g. the UK Information Commissioner).

* If the controller is based **outside the EU** (e.g. Acme Inc.) and offers products or services to EU residents or monitors the behaviour of EU residents, it will be subject to the Regulation and to the scrutiny of each and every regulator.

First of all, the whole point of the extra-territorial reach of the law (both under the Directive and even more under the Regulation) is to protect people who live in Europe where their data is used elsewhere. The "offering products or services" side of the equation is also clearly aimed at capturing visible commercial relationships where, typically via the Internet, an organisation is making its goods or services available to EU residents.

The meaning of "monitoring the behaviour" is slightly trickier because the recitals only refer to one very specific form of monitoring: Internet tracking and profiling. So the commonplace practice of building an Internet user's picture through the use of cookies with a view to targeting that individual with tailored advertising will definitely be caught – not a very "technologically neutral" provision, it must be said. The question that we will need to be addressed is what is the intended scope of the phrase "monitoring the behaviour" beyond Internet tracking and more precisely, how granular or detailed that monitoring must be to trigger the application of the law.

Some governments and regional bodies have adopted application of the "country-of-destination" principle, which states that the applicable law and court with jurisdiction are those where the consumer resides in the event of a B2C cross-border dispute. Application of this principle will severely limit greater consumer choice and more favorable prices. Compliance with the laws of many different countries would impose tremendous costs on business and would be prohibitively expensive for SMEs.

The complexity of applying the "country-of-destination" principle is exacerbated when it is applied where consumers use "infomediaries" or other interposing technologies to purchase goods or services that are digitally transmitted, and pay with digital cash or any other payment mechanism that does not identify the purchaser. In this situation, a business would never know the law and forum to which it subjects itself as the "infomediary" prevents a company from knowing the identity and location of an individual consumer.

- Brussels I

Under Brussels I, persons domiciled in a Member State generally may be sued in the courts of that Member State. Article 5(3) further provides that "in matters related to tort," persons domiciled in a Member State may be sued "in the courts for the place where the harmful event occurred or may occur." This provision aligns with U.S. notions of specific jurisdiction.

Similarly, for contractual disputes, Article 5(1) permits the plaintiff to bring suit in the courts "for the place of performance of the obligation in question." The Brussels I Regulation also provides consumer protections in Article 16(1), pursuant to which a consumer may sue under a contract in the country where the consumer is domiciled.

Article 4 provides that if a defendant is not domiciled in a Member State, "the jurisdiction of the courts of each Member State shall . . . be determined by the law of that Member State." Thus, under Article 4 of the Brussels I Regulation, a defendant website operator from the United States would be subject to the jurisdictional rules of the EU nation in which the plaintiff chooses to bring suit, not the uniform rules established for the EU generally.

- Rome Convention

With respect to choice of law, the 1980 Rome Convention controls in contractual disputes. The general rule is that the law of the country with which the contract is "most closely connected" will govern, to the extent that the parties have not otherwise agreed to apply a different body of law. In determining to which country the contract is "most closely connected," the general rule provided by Article IV of the Rome Convention is that: the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence, or, in the case of a body corporate or unincorporate, its central administration. However, if the contract is entered into in the course of that party's trade or profession, that country shall be the country in which the principal place of business is situated or, where under the terms of the contract the performance is to be effected through a place of business other than the principal place of business, the country in which that other place of business is situated.

Pursuant to Article II, "[a]ny law specified by this Convention shall be applied whether or not it is the law of a Contracting State."

- Rome II

Choice of law in non-contractual disputes is, with important exceptions, governed by the Rome II Regulation ("Rome II"). Under Rome II, the applicable law is determined as follows. First, as a general matter, the applicable law will be the law of the country where the damage occurred. However, if the plaintiff and defendant both have "habitual residence" in the same country when the damage occurs, the law of that country applies. Finally, "where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with a country other than the countries indicated [by the first two inquiries], the law of that country shall apply."

- lex loci delicti commissi

Significantly for the purposes of jurisdictional issues created by the internet, Rome II does not cover disputes arising from the alleged "violations of privacy and rights relating to personality, including defamation." For these kinds of disputes, most EU Member States continue to apply the rule of *lex loci delicti commissi*, which provides that the law of the place where the act was committed applies to the dispute. Such a rule is inadequate to resolve choice of law questions in complex international dealings.

2) The United States

Most U.S. courts that have addressed the issue of jurisdiction and the internet have done so in the national rather than international context. However, the federal system in the U.S. suggests that the same rationale that applies to jurisdictional questions with respect to U.S. states should apply to foreign countries as well. The U.S. has taken a common law approach to establishing its law relating to jurisdiction and the internet.

- the concept of targeting

Generally speaking, companies that "do business" over the internet and are heavily involved in online sales can expect to be subject to jurisdiction in any state in which such sales are conducted. The key concept that has emerged is "targeting" - if a publisher has not specifically targeted its content toward a specific state, it should not be held to be subject to the jurisdiction and law of that state.

- Zippo's sliding scale

This principle has evolved much as the internet itself has evolved. The first case to recognize that not all websites are created equal was *Zippo Manufacturing v. Zippo Dot Com, Inc.*, which established three broad categories of websites that turn on the sites' interactivity. Under *Zippo*'s "sliding scale" approach, at one end of the interactivity scale were websites that conducted business over the internet with forum-state residents, which would always be subject to jurisdiction. An example of such a website would be Amazon.com, which seeks detailed information from its customers and ships products to them in states across the country. At the other end of the scale are "passive" websites that do "little more than make information available to those who are interested, which is not grounds for the exercise of personal jurisdiction." An example of a passive website would be a used bookstore's site that merely posted the store's inventory along with other information such as directions to the store. In the middle of *Zippo*'s sliding scale are situations in which a defendant operates a website that allows a user to exchange information with the site's server. In such cases, the *Zippo* court said, a court must review the "level of interactivity and commercial nature of the exchange of information" to determine whether jurisdiction may be established.

- targeting the forum state rule

Although *Zippo* remains relevant as a framework, many courts have recently suggested that rather than focusing on the interactivity of the site, the focus now should be on whether the publisher in question has specifically targeted its content to the forum state. Courts that apply this targeting analysis have tended to rely on the Supreme Court's *Calder v. Jones* opinion, in which the Court held that a Florida company was subject to jurisdiction in California in a defamation suit by a California resident because the publishers targeted California readers and knew that the plaintiff would suffer the harmful effects of the publication there. In what has emerged as the leading post-*Zippo* case on internet jurisdiction, *Young v. New Haven Advocate*, the Fourth Circuit relied on *Calder*'s "effects test" in holding that the jurisdictional inquiry should determine whether the publisher "(1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State." This is a realistic, business-oriented focus that is appropriate for the evolution of the industry. In an age when virtually all websites promote some degree of interactivity, the more relevant due process question is whether the website's owner could reasonably anticipate being held to

the law of a particular state and being haled into court in that state. As the *Young* analysis sensibly provides, that question should be answered by determining whether the publisher has actually targeted the state.

3) EU-US

Safe Harbor" framework

A safe harbor is a provision of a statute or a regulation that reduces or eliminates a party's liability under the law, on the condition that the party performed its actions in good faith or in compliance with defined standards. Legislators may include safe-harbor provisions to protect legitimate or excusable violations, or to incentivize the adoption of desirable practices.

- *data protection*

An example of safe harbor can be found in the Data Protection Directive, which sets comparatively strict privacy protections for EU citizens. It prohibits European firms from transferring personal data to overseas jurisdictions with weaker privacy laws, but creates exceptions where the overseas recipients have voluntarily agreed to meet EU standards under the Directive's Safe Harbor Principles.

The agreement is another important step toward international cooperation and differs from other agreements in that it allows specifically for cooperation between the United States and Europe, despite the differing views Europeans and Americans have on the economy and privacy. However, by allowing American companies to “opt in,” the agreement does not promote uniformity. Further, because many companies are not signing onto the terms of the agreement, it is basically ineffectual.

4) Global aspects

Different procedural rules apply when a plaintiff commences a lawsuit against a foreign defendant. Generally, a foreign defendant may be subject to state’s jurisdiction pursuant to the treaty signed either between the UE-US or US and the country EU and the other country where the service is to be affected. Further, the jurisdiction may be also based on other international agreements. Global issues of jurisdiction are even more unclear.