



INTERNET LAW RESOURCE CENTER™

Reproduced with permission from BNA's Internet Law Resource Center™,
Copyright 2011, The Bureau of National Affairs, Inc. (800-372-1033) www.bna.com.

International Jurisdiction and the Internet in the Age of Cloud Computing

Kurt Wimmer, Eve Pogoriler, and Stephen Satterfield

COVINGTON & BURLING LLP,
WASHINGTON, D.C.

Kurt Wimmer is a partner concentrating in technology and media law, as well as intellectual property and data privacy. He represents digital media, television, mobile, publishing, and new technology companies. Eve Pogoriler is an associate in the communications and media group. She also practices in the area of privacy and data security. Stephen Satterfield is an associate in the global privacy and data security practice group. Covington & Burling LLP's web address is <http://www.cov.com>.

The internet touches every country in the world and the lives of some two billion people worldwide who use it.¹ 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." The immediacy of this risk rises exponentially as businesses and individuals increasingly utilize "cloud computing" services in which data is stored on remote servers that could be located in any country in the world.²

This Article 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. Part I introduces the jurisdictional issues related to publishing content and conducting business online. This Part features a discussion of three landmark cases that illustrate the complex jurisdictional problems the internet poses for courts, regulators, and private actors. Part II provides an overview of the three types of jurisdiction encountered in the international context. Part III considers the European Union's approaches to jurisdiction as those relate to cases involving the internet. Part IV explores cases from individual European countries. Part V considers other international approaches. Finally, Part VI evaluates how courts in the United States have handled jurisdictional questions arising out of the internet and summarizes legislative efforts to address these issues.

¹ See <http://www.internetworldstats.com/stats.htm>.

² "Cloud computing" generally refers to thin-client applications in which data is stored on remote servers and made available for access and processing over the internet or dedicated online transmission systems. In cloud systems, software running on users' own computers and IT systems is complemented by applications and services accessed over the internet from remote datacenters, i.e., "the cloud." Cloud computing promises greater efficiencies for organizations to customize and rapidly scale their IT systems for their needs. These services can expand access to computational capabilities previously available only to the very largest global companies and can provide better collaboration through "anywhere, anytime" access to IT for users located around the world.

I. Causes of Action and Complexities Created by the Evolving Internet

Most cases arising out of internet activities that have raised issues of international jurisdiction involve either causes of action based on content or causes of action based on doing business online. These two categories of cases are discussed in this Part.

A. Causes of Action Based on Content

The issues relating to causes of action based on content can be illustrated from the points of view of three seminal cases in the area. These cases—from France, Australia, and Canada—show how courts have attempted to negotiate the competing concerns of plaintiffs—who, though geographically distant from the location of a defendant’s physical operations, may have been harmed by that defendant because of the global reach of the internet—and those of defendants, who despite the internet’s ubiquity do not expect to defend suits in every place the internet reaches. Jurisdiction is a concept based on the limits of a state’s power. These cases show courts in the process of defining those limits in an increasingly borderless world.

1. *Association Union des Etudiants Juifs de France v. Yahoo! Inc.*

In perhaps the best known case in the area, two French organizations dedicated to combating anti-Semitism sued Yahoo!, a U.S.-based internet service provider and web publisher, in France.³ The complaint arose out of the posting of Nazi memorabilia on Yahoo!’s internet auction site. Although the site was in English, targeted at U.S. users, and hosted in California, the plaintiffs argued that its accessibility in France (through Yahoo!. and Yahoo! France) rendered it in violation of a French law prohibiting the possession and sale of Nazi artifacts. The court agreed with the plaintiffs and ordered Yahoo! to, among other things, prevent French users from accessing the auction site. The court also stated that Yahoo! and Yahoo! France would be penalized 100,000 Francs per day of delay in implementing the order—this despite Yahoo!’s presentation of evidence that fully blocking French access to Yahoo.com was technologically impossible. (Later litigation in the United States concerned the extent to which the rulings by the French court may have violated U.S. principles of law and jurisdiction, and is discussed in more detail below.)

2. *Dow Jones & Co. v. Gutnick*

In *Dow Jones & Co. v. Gutnick*,⁴ Australia’s High Court held that Dow Jones was subject to suit in Victoria for allegedly defamatory material that appeared in an online version of *Barron’s*, a U.S. financial magazine, despite the fact that the magazine’s website was created and hosted in New Jersey. The court also ruled, over Dow Jones’s objection, that Victorian law applied to the dispute. Although certain language in the opinion suggests a virtually limitless approach to exercising jurisdiction over web publishers, the *Gutnick* decision imposed some constraints on the exercise of jurisdiction in international defamation cases.

According to *Gutnick*, the questions of jurisdiction and choice of law turned primarily on where the alleged defamation occurred, which, the court held, was the place of “publication.” (The court’s decision also rested, in part, on the subscription nature of the site, which enabled individuals to subscribe using Australian credit cards.) Dow Jones asserted that publication took place in New Jersey, where the article had been uploaded to the website’s server and the last place where Dow Jones had exercised editorial control over the content at issue. Thus, Dow Jones argued, New Jersey was the proper forum for the suit, and the dispute was properly governed by New Jersey law. The court responded that Dow Jones took too narrow a view of “publication,” which, the court reasoned, is a “bi-lateral act—in which the publisher makes [content] available and a third party has it available for his or her comprehension.” The court explained that this “bi-lateral” understanding of publication was necessary because of “defamation’s concern with reputation, and the significance to be given to damage [to reputation].” The place of publication for purposes of defamation must be the place where the plaintiff’s reputation is harmed, which, the court held, is where a third party downloads the content at issue.

Standing alone, this rule would subject a defendant publisher to jurisdiction wherever content is viewed. But the *Gutnick* decision, though certainly unfavorable to publishers, does not stand for so broad a proposition. The court cabined the application of this rule by noting that “due weight must be given to the fact that a claim for damage to reputation will warrant an award of substantial damages only if the plaintiff has a reputation in the place where the publication is made.” The court made much of the fact that *Gutnick* was a Victoria resident suing for damage allegedly caused to his reputation “in Victoria as a consequence of the publication that occurred in that State.” Thus,

³ *Association Union des Etudiants Juifs de France v. Yahoo! Inc.*, 6 ILR 434, Tribunal de Grande Instance de Paris, Nov. 20, 2000.

⁴ 12 ILR 346, [2002] HCA 56 (Dec. 10, 2002).

while *Gutnick* represents an expansive view of jurisdiction in internet defamation cases, it does not represent a limitless one.

3. *Bangoura v. Washington Post Co.*

A third case, from Canada, may be more promising for internet publishers. In *Bangoura v. Washington Post Co.*,⁵ the Ontario Court of Appeal reversed a lower court's ruling that the *Post* was subject to Canadian jurisdiction for content that was available on the internet. The trial court had held that the availability of the content on the *Post*'s website—even though it had been downloaded only once in the forum (by the plaintiff's counsel)—was sufficient for jurisdiction.⁶ “I would be surprised if [the *Post*] were not insured for damages for libel or defamation anywhere in the world,” the judge noted in his opinion. “And if it is not, then it should be.” The Court of Appeal reversed, finding that the content “did not reach significantly into Ontario.” The opinion expressed reciprocity concerns, observing that an exercise of jurisdiction in this case “could lead to Ontario publishers and broadcasters being sued anywhere in the world with the prospect that the Ontario courts would be obliged to enforce foreign judgments obtained against them.”

Although generally considered a more refined approach to the jurisdictional complexities posed by the internet than *Gutnick*, the *Bangoura* decision is largely consistent with the approach of the latter. *Bangoura* rests mainly on the fact that the plaintiff had moved to Ontario several years *after* publication of the offending content, and thus effectively had no reputation to be damaged in Ontario at the time of publication. Indeed, rather than rejecting *Gutnick*'s approach, the Canadian court merely distinguished the latter: while *Bangoura* did not move to Ontario until three years after the publication at issue, “*Gutnick* was a well-known businessman who resided in Victoria at the time of the impugned publication . . . and undertook that he would sue only in Victoria and only in respect of damages to his reputation there.”

There is one respect, however, in which *Bangoura* represents a more nuanced approach to the jurisdictional problems created by the internet than the cases discussed above. Unlike *Yahoo!* and *Gutnick*, *Bangoura* placed some weight on the defendant publisher's contact with the forum. The *Bangoura* court noted that while “*Barron*'s had 1,700 internet subscribers in Australia,” the distribution of the *Washington Post* article in Ontario “was minimal.” But even the consideration of the defendant's connection to the forum was viewed through the lens of the *plaintiff*'s connection thereto. The *Bangoura* court concluded that there was “no significant connection between the *Washington Post* . . . and Ontario” because it was not reasonably foreseeable to the *Post* that the plaintiff would “end up as a resident of Ontario” three years after the publication of the article. In the end, although the *Post* prevailed, *Bangoura* still represents a plaintiff-centered approach to international jurisdiction in internet defamation cases similar to the one found in *Gutnick*. This approach presents significant obstacles to publishers seeking to minimize risks associated with publishing content online.⁷

These cases exemplify two common themes that have run through the decisions that have grappled with international jurisdiction in the internet age. First, courts have tended to emphasize the rights of the plaintiff to seek redress for harm while downplaying defendants' rights to procedural fairness (e.g., a trial in a reasonably predictable forum) and free expression. Second, the decisions do not appear to be guided by clear rules but rather are fact-intensive inquiries that consider a wide array of factors. These tendencies, along with the rapid growth of the internet and the lack of technological expertise of many courts and regulators, have led to an inconsistent body of law relating to international jurisdiction.

⁵ 18 ILR 668, [2005] O.J. No. 3849 (Ont. C.A.), *leave to appeal dismissed*, [2006] SCCA No. 497 (February 16, 2006).

⁶ 15 ILR 342, [2004] 234 D.L.R. 456 (Ont. Super. Ct. J.), *rev'd* 18 ILR 668, [2005] O.J. No. 3849 (Ont. C.A.), *leave to appeal dismissed*, [2006] SCCA No. 497 (February 16, 2006).

⁷ Indeed, two other Canadian cases suggest that *Bangoura*'s significance as precedent may be limited. In *Burke v. NYP Holdings, Inc.*, which was decided the same day as *Bangoura*, the Supreme Court of British Columbia asserted jurisdiction over the *New York Post* in a defamation case based on an internet publication. Although the evidence showed only a single viewing of the article in British Columbia, the court held that the *Post* could be subject to jurisdiction there because (1) the plaintiff had an established reputation there and (2) the subject matter of the article—an incident from a professional hockey game in Vancouver—would have been of interest to British Columbia residents. *Burke v. NYP Holdings, Inc.*, 2005 ILRC 2631, [2005] 48 B.C.L.R. 363 (Can.); *see also* Andrea Slane, *Tales, Techs, and Territories: Private International Law, Globalization, and the Legal Construction of Borderlessness on the Internet*, 71 LAW & CONTEMP. PROBS. 129, 141-42 (2008).

A more recent case from the same court, *Crookes v. Yahoo!*, follows the approaches of *Burke* and *Gutnick* in holding that *Yahoo!* could not be subject to jurisdiction for allegedly defamatory content posted by a user on a *Yahoo!* Groups bulletin board because the plaintiff could not show that the content was viewed in British Columbia. *Crookes v. Yahoo!*, [2007] B.C.S.C. 1325 (Can.).

In response, several efforts have been undertaken to create universal and predictable laws, and at least some courts have begun exercising restraint in asserting jurisdiction over claims that could potentially be brought in any forum in the world.⁸ In addition, there have been promising developments recently to codify the principle that website publishers should be subject only to the laws of their home states.⁹

4. General Principles for Content-Based Causes of Action

These cases discussed above involve situations where a website operator or publisher faces a lawsuit based solely on content that appears on a website. Defamation cases such as *Gutnick* and *Bangoura* are the most common suits of this kind, but this category also includes suits alleging copyright infringement and prosecutions for obscenity, hate speech, and the like. In such cases, defendants typically argue that the website should only be subject to the laws of the country in which it is based in order to avoid a situation in which every website in the world must conform to the most restrictive set of national laws in existence. As *Yahoo!* suggests, however, website content can and has given rise to liability in foreign countries when a defendant is found to be in violation of national laws.

Cases such as *Yahoo!*, *Gutnick*, and *Bangoura* also raise the corollary issue of whether publishers can and should attempt to limit the distribution of content out of deference to certain countries' laws and social norms. The French *Yahoo!* court found that Yahoo!'s attempt to target its U.S. auction site to U.S. users was insufficient to avoid French jurisdiction; apparently nothing less than blocking French access would suffice to avoid liability. And even where a website has not been accessed (or has been accessed only a few times) in a jurisdiction, courts have considered the "effects" of a publication largely read by a nonresident population on the reputation of residents. *Bangoura* illustrates, however, that even where the effects of a content-based cause of action may be felt in a given forum—e.g., a reputational harm that follows the plaintiff—courts will scrutinize their bases for asserting jurisdiction.

An additional complication in cases based on web content is the effect of so-called "user-generated content," i.e., content that is uploaded to a website by an individual with no official relationship with the publisher. The rise of "Web 2.0"—a movement exemplified by publishers such as Facebook that emphasize information sharing and user-centered design—has made questions about when a publisher should face liability for content posted by a user particularly urgent. A troubling example of the imposition of liability on the publisher for content posted by a user is the recent prosecution of four Google executives in Italy after a user posted a video to a Google website showing the bullying of a disabled child.¹⁰ The video was available for two months before Italian authorities notified Google and Google removed it. Three of the defendants—none of whom were aware of the posting until being contacted by the authorities—were convicted of violating Italy's Personal Data Protection Code and given suspended six-month sentences. Although the U.S. generally provides publishers with immunity from liability based on user-generated content,¹¹ the trend elsewhere has been to impose the often-infeasible requirement that publishers monitor all content that appears on their sites, and remove content that may be in violation of the law.¹²

B. Causes of Action Based on Conducting Business Online

Another important subset of cases raising questions of international jurisdiction involves situations in which a company is conducting business over the internet. These cases typically involve e-commerce websites and implicate causes of action such as breach of contract and products liability. In common law countries where jurisdiction is often based on the "contacts" between a defendant and a forum, a court's decision to exercise jurisdiction often

⁸ See, e.g., the *Al Amoudi* and *Jameel* cases discussed *infra* in Part IV.

⁹ See *infra* Part III.

¹⁰ See John Hooper, *Google Executives Convicted in Italy Over Abuse Video*, THE GUARDIAN (London), Feb. 24, 2010, available at <http://www.guardian.co.uk/technology/2010/feb/24/google-video-italy-privacy-convictions>.

¹¹ See §230 of the Communications Decency Act of 1996, 47 U.S.C. §230. The CDA provides, in relevant part, that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The statute generally protects website operators from suits arising out of user-generated content appearing on their sites. See, e.g., *Zeran v. America Online, Inc.*, 1 ILR 533, 129 F.3d 327 (1997).

¹² EU law generally provides that the host of content provided by a third party should not be subject to liability based on that content if it removes it after being notified of it. See European Union Directive 2000/31/EC on Electronic Commerce (the "E-Commerce Directive"), June 8, 2000 (discussed in more detail *infra* at notes 23-27 and accompanying text). This principle did not appear to be honored by the Italian court that prosecuted Google executives in this case after the content at issue had been removed.

depends upon whether the defendant has targeted his activity toward the forum state.¹³ By contrast, the European Union has enacted codes that dictate where jurisdiction is appropriate that do not rely on the complex, and often unclear, “contacts” analyses used in common law countries like the U.S. and Canada. Such codes have, at least in some areas of the law, made the risks of doing business online more predictable, thereby encouraging growth in realm of e-commerce.¹⁴

II. Distinguishing Between Types of Jurisdiction

In considering how courts and regulators have addressed the problems of international jurisdiction in the internet age, it is useful to distinguish between three broad categories of jurisdiction that often are conflated: legislative jurisdiction (or jurisdiction to prescribe), judicial jurisdiction (or jurisdiction to adjudicate), and executive jurisdiction (or jurisdiction to enforce).¹⁵ These three concepts are closely related, but distinct.

A. Legislative Jurisdiction

Legislative jurisdiction, or jurisdiction to prescribe, refers to a state legislature’s authority to make its substantive laws apply to particular parties or circumstances. In general, a legislature’s authority to proscribe certain behavior within its territory or by its nationals is undisputed. A more controversial but increasingly accepted basis for legislative jurisdiction is the prohibition of actions taken in a foreign state that cause injury or bad “effects” in the home state. The worldwide nature of the internet places great strain on the traditional principles of legislative jurisdiction. For example, it is generally accepted that Germany and France may keep their nationals and people within their territory from viewing Nazi propaganda or other forms of hate speech. When their laws apply to websites that are established in foreign countries, however, as was the case in *Yahoo!*, their legislative jurisdiction is far more controversial.

Some countries have taken steps to limit the problems that arise when a sovereign asserts jurisdiction over entities that are neither citizens nor present in the sovereign’s territory. The object of these measures is to promote trade by providing consistency and predictability in the laws of different sovereigns. One prevalent limitation on legislative jurisdiction within the federal system of the United States is the “dormant commerce clause.” Laws passed by individual U.S. states are invalid under the dormant commerce clause if they unduly burden or discriminate against interstate commerce.¹⁶ A similar principle applies to EU Member State laws that are seen as protectionist and in violation of EU common market efforts. While this is a complex area of the law with few easily predictable results, the practical effect is that laws passed by U.S. states or EU Member States that impose undue burdens on online businesses without a legitimate purpose (such as consumer protection) might be subject to challenge under the dormant commerce clause or the EU common market principle. The doctrinal underpinnings of both provide a useful model for thinking about problems of international jurisdiction and the internet in that they are intended to prevent one sovereign from imposing its laws on the citizens of another in such a way as to impede the free flow of commerce (arguably the outcome of cases such as *Yahoo!* and *Gutnick*).

B. Judicial Jurisdiction

Judicial jurisdiction, or jurisdiction to adjudicate, refers to the authority of a state to subject parties to proceedings in its courts or other tribunals. The exercise of judicial jurisdiction is based on a defendant’s connection to the forum where legal action is commenced.¹⁷ This connection can be the defendant’s continuous and systematic contacts with the forum, which give rise to what U.S. courts call “general jurisdiction.” Where there is general jurisdiction over a defendant, the cause of action need not have any relation to the forum. This concept has very little applicability to cases involving the internet, because the existence of a website that is accessible to forum residents, without more, is insufficient to give rise to general jurisdiction. The only businesses that are subject to such jurisdiction are those that have a real-world presence in the forum and already anticipate being sued there. Specific jurisdiction, on the other hand, allows courts to exercise jurisdiction when there is some minimal relationship between the defendant, the cause of action, and the forum state. The seminal U.S. case, *International Shoe v. Washington*, described “specific jurisdiction” as existing when the plaintiff could show that the defendant had “certain minimum contacts [with the forum] . . . such that the maintenance of the suit does not offend traditional

¹³ See *infra* notes 60 to 66 and accompanying text.

¹⁴ See *infra* Part IV.

¹⁵ See LOUIS HENKIN ET AL., INTERNATIONAL LAW 1046 (3d ed. 1993).

¹⁶ See, e.g., *Granholm v. Heald*, 17 ILR 677, 544 U.S. 460 (2005) (dormant commerce clause violated by state laws discriminating against the direct sales of wine by out-of-state wineries).

¹⁷ See ASHLEY PACKARD, THE BORDERS OF FREE EXPRESSION 13 (2009).

notions of fair play and justice.”¹⁸ Internet jurisdiction cases are most often about whether a defendant may be subject to specific jurisdiction, usually based on the “effects” of the defendant’s conduct in the forum or the defendant’s “targeting” of the forum.¹⁹

C. Executive Jurisdiction

Executive jurisdiction, or jurisdiction to enforce, refers to the authority of a state to use its resources to compel compliance with its law. This authority typically flows from the jurisdiction to adjudicate. International law principles of comity usually require states to assist in the enforcement of judicial decisions of other states. There are, however, limits to such international cooperation. For example, in the U.S., the recently passed SPEECH Act prohibits the enforcement of foreign judgments in U.S. courts unless the court finds that the foreign judgment is consistent with the First Amendment.²⁰ And even before the SPEECH Act,²¹ U.S. courts had typically refused to enforce judgments that were repugnant to the First Amendment, on public policy grounds.²² For example, after the French court’s ruling in the *Yahoo!* case, Yahoo! sought an order from a U.S. court barring enforcement of the French judgment in the U.S. The lower court sided with Yahoo!, although a plurality of an *en banc* panel of the Ninth Circuit Court of Appeals reversed on the grounds that the case was not yet ripe.²³

The following sections discuss the treatment of the issue of jurisdiction and the internet by various courts, regulators, and legislative bodies across the world.

III. The European Union

The issue of whether a publisher will be subject to the jurisdiction of national courts is generally a matter of the internal laws of that nation. The most prominent exception to this principle is the European Union, which has established principles of jurisdiction and choice of law that apply across multiple countries. This section presents a survey of emerging jurisdiction and choice of law principles in the 27-country EU.

Approximately ten years ago, the EU adopted Directive 2000/31/EC on electronic commerce (the “E-Commerce Directive”).²⁴ The E-Commerce Directive establishes basic, harmonized rules in areas such as electronic contracts, electronic commercial communications, and online provision of professional services. The E-Commerce Directive, which applies only to electronic commerce activities (and more particularly, “information society services”²⁵) 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”:

Information society services should be *supervised at the source of the activity*, in order to ensure an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens; in order to improve mutual trust between Member States, it is essential to state clearly where the services originate; moreover, in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of services, *such*

¹⁸ *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945).

¹⁹ See *infra* notes 68 to 70 and accompanying text (discussing the U.S. Supreme Court’s *Calder v. Jones* decision).

²⁰ See *infra* notes 82 to 83 and accompanying text.

²¹ See *id.*

²² *Yahoo! Inc. v. La Ligue Contre le Racisme et l’Antisemitisme*, 9 ILR 171, 169 F. Supp. 2d 1181 (N.D. Cal. 2001), *rev’d on other grounds*, 16 ILR 283, 379 F.3d 1120 (9th Cir. 2004), *rev’d en banc*, 19 ILR 226, 433 F.3d 1199 (9th Cir. 2006); see also *Sarl Louis Feraud Int’l v. Viewfinder, Inc.*, 19 ILR 69, 406 F. Supp. 2d 274 (S.D.N.Y. 2005) (refusing to enforce French intellectual property and unfair competition judgment because judgment was incompatible with the First Amendment), *vacated*, 2007 ILRC 2009, 489 F.3d 474 (2d Cir. 2007) (affirming lower court’s holding that a court can refuse to enforce foreign judgment that conflicted with the First Amendment, but remanding based on insufficient factual record to support lower court’s decision); *Matusевич v. Telnikoff*, 877 F. Supp. 1, 23 Media L. Rep. 1367 (D.D.C. 1995) (refusing to enforce U.K. libel judgment based on speech that would have been protected by the First Amendment); *Bachchan v. India Abroad Publ’ns, Inc.*, 585 N.Y.S 2d. 661 (N.Y. Gen. Term. 1992).

²³ *Yahoo! Inc. v. La Ligue Contre le Racisme et l’Antisemitisme*, 19 ILR 226, 433 F.3d 1199 (9th Cir. 2006).

²⁴ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, 2000 O.J. (L. 178) 1-16.

²⁵ As defined in Directive 98/48/EC, “information society services” are services “normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.”

information society services should in principle be subject to the law of the Member State in which the service provider is established.²⁶

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.

This concept was reaffirmed by the European Union in the adoption of Directive 2007/65/EC, the Audiovisual Media Services Directive (the “AVMS Directive”), which was required to be transposed into national law during 2010.²⁷ 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.²⁸ This principle states that “only one Member State should have jurisdiction over an audiovisual media service provider.”²⁹ 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.”³⁰

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.³¹

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.

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).³² The advocates of the “single point of publication” rule point out that it complements the country of origin rule by ensuring that there is a principal place of publication, and therefore a country of origin, for every article. The proposal also 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 single point of publication rule accounts for these scenarios because “publication” would be deemed to take place at the point at which there is a final opportunity for the publisher to exercise control over content. This rule has not, to date, been adopted.

²⁶ E-Commerce Directive, recital 22 (emphasis added), available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF>.

²⁷ Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:095:0001:0024:EN:PDF>.

²⁸ See *id.* at Whereas clause 33 (“The country of origin approach should be regarded as the core of this Directive”).

²⁹ *Id.* at Whereas clause 34.

³⁰ *Id.* at Whereas clause 33.

³¹ *Id.* at Article 2(3).

³² For a description of this proposal, see Media Law Resource Center’s Comments to the European Commission, http://ec.europa.eu/justice/news/consulting_public/rome_ii/contributions/mlrc_en.pdf.

The E-Commerce Directive states that it “neither aims to establish additional rules on private international law relating to conflicts of law nor does it deal with the jurisdiction of Courts.”³³ With respect to jurisdiction, the seminal EU accord is the Brussels I Regulation.³⁴ Under Brussels I, persons domiciled in a Member State generally may be sued in the courts of that Member State.³⁵ This provision mirrors the U.S. concept of general jurisdiction discussed above. 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.

With respect to choice of law, the 1980 Rome Convention controls in contractual disputes.³⁶ 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.”

Choice of law in non-contractual disputes is, with important exceptions, governed by the Rome II Regulation (“Rome II”).³⁷ 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.” Rome II also contains more specific principles governing choice of law in particular kinds of cases, *e.g.*, cases involving intellectual property and products liability claims.

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

³³ E-Commerce Directive, recital 23; *see also id.* at Article 1 §4. The E-Commerce Directive directs Member States to adopt legislation to aid the free movement of information society services between the Member States, including provisions relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions, and cooperation between Member States. *See id.* at Article 1 §§ 1-2.

³⁴ Brussels I Regulation, superseding the Brussels Convention, Council Regulation (EC) No. 44/2001 of 22 December 2000, on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/1_012/1_01220010116en00010023.pdf. All Member States with the exception of Denmark have adopted the Regulation. A second regulation, referred to as Brussels II, Council Regulation No. 2201/2003, creates EU rules relating to jurisdiction and recognition and enforcement of civil judgments involving parental responsibility, child abduction, and access rights.

³⁵ Brussels I Regulation, Article 2.

³⁶ *Available as amended at* [http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:41998A0126\(02\):EN:HTML](http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:41998A0126(02):EN:HTML).

³⁷ All Member States but Denmark have adopted the Rome II Regulation.

that the law of the place where the act was committed applies to the dispute.³⁸ Such a rule is inadequate to resolve choice of law questions in complex international dealings, however. Dispute-specific facts—including the location of where the damage was sustained, the country with which the case is most closely connected, and the extent to which the courts favor claimants—may all have an effect on the choice of law determination. The result of this is that the law remains unpredictable in this area, and has no doubt chilled certain transnational commercial activity.

It is worth noting in this regard that all Member States of the EU and 21 additional signatories are bound to the Council of Europe’s Convention for the Protection of Human Rights and Fundamental Freedoms (“ECHR”).³⁹ Article 10 of the ECHR protects freedom of expression, although in a manner weaker than that provided by the U.S. First Amendment. Article 6 of the ECHR also provides for fair trials and procedural justice. Other multinational treaties with which internet and media lawyers should familiarize themselves include the United Nations’s International Covenant on Civil and Political Rights (“ICCPR”), the American Convention on Human Rights (“ACHR”), and the African Charter on Human and Peoples’ Rights (“ACHPR”), all of which are international agreements protecting freedom of expression and the free exchange of ideas.

IV. Individual European Countries

As discussed above, Article 4 of the Brussels I Regulation 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.” Consequently, from the perspective of website operators and publishers in the United States or in other non-EU countries, the jurisdictional rules of individual EU nations have not been displaced by a uniform body of law. Such defendants must determine whether jurisdiction is proper under the laws of the forum state. This Part briefly surveys the most important European precedents in this area.

In addition to the *Yahoo!* case discussed above, the first years of the Twenty-First Century witnessed the courts of several European countries asserting jurisdiction over materials posted on websites established by companies or individuals domiciled in other countries. For example, in 2000, Germany’s highest court let stand the conviction of Australian national and well-known Holocaust revisionist, Frederick To’ben, for views expressed on his Australian website.⁴⁰ The court found that laws prohibiting denial of the Holocaust could be applied to internet content on a foreign website that was accessible in Germany.

An Italian case from around the same time as *To’ben* produced a similarly broad ruling. The case involved a “trans-border custodial battle,” in which an Italian man accused his ex-wife, who lived in Israel, of defamation when the latter posted statements online suggesting the man was incapable of caring for his two daughters.⁴¹ Although the statements were posted on websites created and hosted in Israel and other foreign countries, an Italian prosecutor brought defamation charges against the site operators. A lower court dismissed the case for lack of jurisdiction because the websites were not published in Italy, but an appeals court reversed, holding that although the websites were “published abroad,” the offense was within the jurisdiction of the Italian courts because the effects of the publication occurred in Italy. Under the Italian model, consequently, internet publishers would be subject to jurisdiction in Italy in cases where the content causes harm in Italy, even if the content is created and uploaded elsewhere.

Under the reasoning of *Yahoo!*, *To’ben*, and the Italian case, the content of a website would have to be tailored to the standards of every country in the world—from the relatively tolerant standards of the United States’s First Amendment, to the standards in many European countries that make many kinds of hate speech illegal, to perhaps even the indecency standards of countries in the Middle East that are very different from those in Western countries. Because of the universal accessibility of a given website, the effect of this approach would be to require that site to produce content that complies with the most restrictive national laws in the world.

³⁸ Proposal for a European Parliament and Council Regulation on the Law Applicable to Non-Contractual Obligations (“Rome II”), July 22, 2003, Explanatory Memorandum at §2.1, available at http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003_0427en01.pdf.

³⁹ Available online as amended at <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>.

⁴⁰ See Steve Kettman, *German Hate Law: No Denying It*, WIRED, December 15, 2000, <http://www.wired.com/politics/law/news/2000/12/40669>.

⁴¹ See Corte di Cassazione, closed sez., 27 Dec. 2000, n.4741, V; see also ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 190-91 (Robert Deibert et al. eds. 2008). The names of the complainant and the websites that were prosecuted are not published in the court’s decision.

A related, and equally troubling, phenomenon in Europe is the rise of so-called “libel tourism,” the practice of litigants bringing defamation suits in foreign jurisdictions in order to take advantage of plaintiff-friendly defamation laws.⁴² Libel tourism introduces a level of unpredictability in the application of national laws beyond what we have seen in those cases where a business operating online finds itself subject to the jurisdiction of a foreign nation’s courts by virtue of causing harm to a plaintiff that resides in that nation. While in some of the cases discussed thus far, it was at least arguably foreseeable that the defendant would find itself subject to the jurisdiction of a foreign country’s court because the web content at issue affected a resident of that country,⁴³ libel tourism cases feature plaintiffs from one country suing defendants from another country in the courts of a third country. For example, in *Berezovsky v. Michaels*, the House of Lords permitted two Russian citizens to sue Forbes Magazine—an American publication—in the U.K.⁴⁴ Although the issue containing the article in question had a distribution of only 1,915 in the U.K. (compared to 785,710 in the U.S. and Canada), the article was also available online.⁴⁵ The Lords found that because the plaintiffs had extensive business dealings in England and had confined their claim to damages suffered there, jurisdiction over Forbes was appropriate.⁴⁶

Another prominent example of libel tourism in the U.K. is the case of *Bin Mahfouz v. Ehrenfeld*, in which a Saudi billionaire sued U.S. author Rachel Ehrenfeld and her publisher Bonus Books. The suit arose out of Ehrenfeld’s book *Funding Evil: How Terrorism is Financed and How to Stop It*, which documented Sheikh Khalid Bin Mahfouz’s role in financing Al Qaeda and other terrorist organizations.⁴⁷ Ehrenfeld did not appear in the action, and Bin Mahfouz obtained a default judgment against her providing for money damages, an injunction against publishing the statements in the U.K., and a “declaration of falsity,” in which the court declared that the book’s statements were false and defamatory. The court entered the judgment despite the dispute’s having an even weaker connection to the forum than the *Berezovsky* case. Only 23 copies of *Funding Evil* had been purchased in the U.K.—all through U.S. websites (though the court noted that the first chapter of the book had been available on the U.S. news website, abcnews.com). And the court did not even consider Bin Mahfouz’s connection to the U.K.

Although these cases from France, Germany, Italy, and the U.K. continue to represent dangerous precedents for businesses operating online, some recent developments suggest courts and regulators are becoming more sensitive to the problems that expansive approaches to international jurisdiction have created. Interestingly, the most promising developments have come from the U.K., which as the *Berezovsky* and *Ehrenfeld* cases demonstrate, is rightly known as the “libel capital of the world.”⁴⁸ Two U.K. cases are helpful precedents for internet publishers. In *Dow Jones & Co., Inc. v. Jameel*,⁴⁹ a court refused to exercise jurisdiction over the U.S. publisher of the *Wall Street Journal* for an allegedly defamatory article. Although the article did not name the plaintiff, the online version provided readers with a link to a document naming the plaintiff as someone who had provided funds to Al Qaeda. The court held that it would not exercise jurisdiction because only a handful of subscribers to the website had accessed the document and thus there was no “substantial” publication in the jurisdiction. In another promising case, *Al Amoudi v. Brisard*, a website operated by a French national residing in Switzerland published two articles linking the plaintiff businessman to Al Qaeda financing. Although the website was accessible to the general public, the court ruled that the burden was on the plaintiff to demonstrate that the publications were accessed and downloaded by a third party. The judge concluded that he could not “accept that under English law a claimant in a libel action on an internet publication is entitled to rely on a presumption of law that there has been substantial publication.”⁵⁰ In addition to the increasing caution being exercised by U.K. courts in cases implicating

⁴² See generally Emily C. Barbour, *The SPEECH Act: The Federal Response to “Libel Tourism,”* CONGRESSIONAL RESEARCH SERVICE, Sept. 16, 2010.

⁴³ The *Bangoura* case is, of course, a notable exception. As discussed above, the Ontario Court of Appeal focused on the unforeseeability of the *Washington Post*’s having to stand trial in Ontario, where the plaintiff had moved three years after the publication at issue.

⁴⁴ *Berezovsky v. Michaels*, 5 ILR 572, [2000] 1 W.L.R. 1004 (H.L.) (Eng.), available at <http://www.publications.parliament.uk/pa/ld199900/ldjudgmt/jd000511/bere-1.htm>.

⁴⁵ See *id.*; see also PACKARD, *supra* note 16, at 33.

⁴⁶ The Lords have since limited the reach of this principle. See *infra* note 48 and accompanying text.

⁴⁷ *Bin Mahfouz v. Ehrenfeld*, [2005] EWHC 1156 (Q.B.) (Eng.), available at <http://www.bailii.org/ew/cases/EWHC/QB/2005/1156.html>.

⁴⁸ See PACKARD, *supra* note 16 at 33.

⁴⁹ [2005] EWCA Civ. 75, 2005 ILRC 1271 (3 Feb. 2005).

⁵⁰ *Al Amoudi v. Brisard*, 2006 ILRC 1881, [2006] EWHC 1062, para. 37 (Q.B.D.) (5 May 2006).

international jurisdiction and the internet, U.K. legislators are currently putting together libel reform legislation that will be considered by a Joint Select Committee of both Houses of Parliament in the spring of 2011.

Libel reform in the plaintiff-friendly U.K. may usher in a new era of awareness of the dangers to electronic commerce that many European countries' approaches to international jurisdiction pose. For now, though, the courts of many European countries remain unfavorable fora for non-European businesses whose websites are accessible in Europe. In early 2010, a German appellate court held that *New York Times* journalist Raymond Bonner could be subject to suit in Germany, along with the *Times*, for a 2001 article that allegedly defamed a German citizen.⁵¹ Notably, the court appears to have based its jurisdiction not on the fact that the article had been read in Germany but rather that there were more than 14,000 subscribers to the *Times's* website in the country. And nothing illustrates the dangers that publishers may face better than the prosecution of the four Google executives discussed above.

V. Other International Approaches

Countries in Asia, Africa, and South America have also seen an increasing number of cases raising international jurisdictional problems that arise from the internet's global reach. But unlike the cases discussed above, the most noteworthy cases from these countries involve attempts to curtail criticism of the state or of particular government officials. Although many of these cases are deeply troubling in that they involve the prosecutions of, or civil lawsuits against, journalists who are seeking to inform readers about official abuses of power, they are also heartening in that they highlight the democratizing effect of the rise of the internet. Furthermore, these cases illustrate how the borderless nature of cyberspace has transformed matters that would once have been of purely local concern into questions of international importance.

For example, the well-known case of Andrew Meldrum has opened up a debate about some of the more repressive practices of the Mugabe regime in Zimbabwe. Meldrum, an American journalist writing for the *Guardian*, a London newspaper, was prosecuted in Zimbabwe on charges of "abuse of journalistic privileges by publishing falsehoods" on the basis of stories published in the *Guardian* in England and posted on its website, which is published and hosted in England.⁵² The *Guardian* was not available in paper copy in Zimbabwe. Prosecutors took the position that Zimbabwe's criminal courts have jurisdiction over any content published on the internet if that content could be accessed in Zimbabwe.⁵³ On July 15, 2002, Meldrum was acquitted of the charges against him by the district court in Harare. Immediately upon acquittal, however, Meldrum was served with deportation papers. Judge Godfrey Macheyo refused to address Meldrum's argument that the court lacked jurisdiction over him, effectively leaving the door open for future prosecutions against foreign journalists based on internet distribution of their stories.⁵⁴ Local and international criticism of this decision, and others like it, appear to have given some momentum to efforts to repeal the law under which Meldrum was prosecuted, the Access to Information and Protection of Privacy Act ("AIPPA"), though these efforts appear to have stalled for the time being.⁵⁵

A similar case in Senegal involved the prosecution of a French journalist, Christian Costeaux, who ran a website about tourism in Senegal. Costeaux was sentenced in absentia for posting an article from a Senegalese newspaper that accused the mayor of Ziguinchor and two hotel owners of being involved with organized crime.⁵⁶ The court issued an international warrant for Costeaux's arrest.

A more recent case in Brazil against freelance journalist Joe Sharkey recently ended in a rare international victory for a journalist sued abroad for alleged defamation. Sharkey, who reports on air travel for a variety of publications, was involved in a midair collision above the Amazon that resulted in the deaths of 154 people. In an

⁵¹ See *German Court Claims Jurisdiction in Lawsuit Against American Author*, The Reporters Committee for Freedom of the Press, Mar. 18, 2010, <http://www.rcfp.org/newsitems/index.php?i=11326>.

⁵² See "U.S. Citizen Becomes First Journalist Tried Under Zimbabwe's New Press Law," NEWS MEDIA UPDATE (REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS), July 1, 2002. Domestic journalists have been prosecuted under the law as well, and a Zimbabwe journalist stood as a co-defendant with Mr. Meldrum in the prosecution in Harare.

⁵³ See Geoffrey Robertson, *Mugabe Versus the Internet*, THE GUARDIAN, June 17, 2002, available at <http://www.guardian.co.uk/Archive/Article/0,4273,4435071,00.html>.

⁵⁴ See *American Reporter in Zimbabwe Acquitted but Ordered Deported*, MEDIA LAW LETTER (MEDIA LAW RESOURCE CENTER), July 2002, at 55.

⁵⁵ See Raymond Mhaka, *AIPPA and POSA To Be Repealed by End of Year*, ZIMBABWE METRO, Mar. 21, 2010, <http://www.zimbabwemetro.com/politics/aippa-to-be-repealed-by-end-of-year/>.

⁵⁶ See PACKARD, *supra* note 16, at 41; *Frenchman Sentenced in Senegal for Internet Libel*, AGENCE FRANCE-PRESSE, Jan. 7, 2004.

article about the incident that appeared in the *New York Times* and in subsequent entries on his personal blog, Sharkey suggested that errors by Brazilian air traffic control, which is operated by the Brazilian military, caused the collision. Sharkey was sued by the widow of one of the passengers killed in the collision. She sued under a Brazilian law allowing any citizen to claim damages for any insult to the dignity or honor of Brazil in any case involving a crime.⁵⁷ Specifically, the complaint asserted that Sharkey had impugned Brazil's honor by calling the country "archaic" and its citizens "idiots," comments that Sharkey denied having made.⁵⁸ In November 2010, a judge dismissed the suit.

VI. 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, and after some initial confusion, the law is beginning to stabilize. 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.

This principle has evolved much as the internet itself has evolved. One of the first cases to address the issue of jurisdiction and the web was *Inset Systems, Inc. v. Instruction Set, Inc.*⁵⁹ This 1996 case involved a trademark infringement dispute in which the plaintiff relied on the defendant's website for establishing jurisdiction. The court took an expansive view of the effect a website would have on the jurisdiction analysis. Finding that the defendant "directed its advertising activities via the internet . . . not only to Connecticut, but to all states," the court held that the defendant had, through its website, "purposefully availed itself of the privilege of doing business within Connecticut."⁶⁰

This expansive view of jurisdiction did not last. The first case to recognize that not all websites are created equal was *Zippo Manufacturing v. Zippo Dot Com, Inc.*,⁶¹ 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."⁶² 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.⁶³

Courts in the late 1990s and early 2000s used *Zippo*'s sliding scale as a starting point in their analyses and, for the most part, followed its reasoning. This was especially true of cases at either end of the *Zippo* sliding scale. For example, in *Mink v. AAAA Development LLC*,⁶⁴ the Fifth Circuit followed *Zippo* in finding that the defendant's website, which included information about its products and services, was a passive website despite providing users with a printable mail-in order form, postal and e-mail addresses, and a toll-free number. The court noted that the defendant's site was not interactive enough to support a finding of jurisdiction because customers could not actually

⁵⁷ The American pilots of the jet on which Sharkey was traveling were charged with negligent homicide for their role in the collision.

⁵⁸ See *U.S. Reporter Faces 'Insult' Suit in Brazil Air Crash Aftermath*, COMMITTEE TO PROTECT JOURNALISTS, <http://cpj.org/2009/09/us-reporter-faces-insult-suit-in-brazil-air-crash.php>.

⁵⁹ 1 ILR 729, 937 F. Supp. 161 (D. Conn. 1996).

⁶⁰ *Id.* at 165.

⁶¹ 2 ILR 286, 952 F. Supp. 1119 (W.D. Pa 1997).

⁶² *Id.* at 1124.

⁶³ *Id.*

⁶⁴ 3 ILR 515, 190 F.3d 333 (5th Cir 1999).

make purchases online. In another passive website case, *Cybersell, Inc. v. Cybersell, Inc.*,⁶⁵ the Ninth Circuit found that a website that did not specifically target Arizona residents was not sufficient to confer jurisdiction in Arizona. Because the defendant, a Florida company, merely established a passive website and did nothing more to encourage Arizona residents to access its site, the court held that there was no personal jurisdiction. As for cases that fall in the middle of the *Zippo* scale, several subsequent courts followed *Zippo* and engaged in fact-specific inquiries regarding the interactivity and commercial nature of the website.⁶⁶ As the Third Circuit noted, “[m]ere operation of a commercially interactive website should not subject the operator to jurisdiction anywhere in the world. Rather, there must be evidence that the defendant ‘purposefully availed’ itself of conducting activity in the forum state, by directly targeting its website to the state, knowingly interacting with residents of the forum state via its website, or through sufficient other related contacts.”⁶⁷

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.⁶⁸ Courts that apply this targeting analysis have tended to rely on the Supreme Court’s *Calder v. Jones* opinion,⁶⁹ 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*,⁷⁰ 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.”⁷¹ 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.

Calder has been particularly useful in cases involving intentional torts. In *Panavision International, L.P. v. Toeppen*,⁷² the Ninth Circuit found jurisdiction in a case in which a nonresident defendant registered Panavision’s trademark as the domain name for its website and then sought to extort money from the plaintiff. The court applied *Calder*’s “effects” test and held that the defendant’s conduct had the effect of injuring the plaintiff in California, its principal place of business, and that this outcome was foreseeable enough to the defendant as to give him reason to anticipate being haled into court there. Similarly, the Seventh Circuit recently held in *Tamburo v. Dworkin* that defendants were subject to personal jurisdiction in Illinois because they defamed the plaintiff on their websites, knowing that the plaintiff lived in Illinois and would suffer reputational harm there.⁷³

Recently, however, there has emerged a split in authority as to how *Calder* should apply in internet jurisdiction cases. The disagreement concerns whether the due process standard for personal jurisdiction is satisfied where, as in *Tamburo*, a plaintiff shows merely that the defendant posted allegedly defamatory material on a website with knowledge that the defendant lives in the forum state. In addition to the Seventh Circuit, the state supreme courts of New Jersey⁷⁴ and Ohio⁷⁵ have answered this question in the affirmative. On the other hand, the Third,⁷⁶ Fourth,⁷⁷

⁶⁵ 3 ILR 215, 130 F.3d 414 (9th Cir 1997).

⁶⁶ See, e.g., *Edberg v. Neogen*, 1998 ILRC 2403, 17 F. Supp. 2d 104 (D. Conn. 1998); *E-Data Corp. v. Micropatent Corp.*, 1 ILR 377, 989 F. Supp. 173 (D. Conn. 1997); *CD Solutions v. Tooker*, 965 F. Supp. 17 (N.D. Tex. 1997).

⁶⁷ *Toys “R” Us, Inc. v. Step Two*, 12 ILR 764, 318 F.3d 446, 454 (3d Cir. 2003).

⁶⁸ This is perhaps because virtually all websites now have at least some interactive features.

⁶⁹ 465 U.S. 783 (1984).

⁷⁰ *Young v. New Haven Advocate*, 12 ILR 379, 315 F.3d 256 (2002), cert. denied, 538 U.S. 1035 (2003).

⁷¹ *Id.* at 263.

⁷² 1 ILR 699, 141 F.3d 1316 (9th Cir 1998).

⁷³ See *Tamburo v. Dworkin*, 30 ILR 335, 601 F.3d 693 (7th Cir. 2010).

⁷⁴ See *Blakey v. Continental Airlines, Inc.*, 5 ILR 594, 751 A.2d 538 (N.J. 2000).

⁷⁵ See *Kauffman Racing Equipment L.L.C. v. Roberts*, 31 ILR 41, 126 Ohio St.3d 81 (2010).

⁷⁶ See *IMO Indus. v. Kierkert*, 155 F.3d 254 (3d Cir. 1998).

⁷⁷ See *Young*, 315 F.3d 256.

Fifth,⁷⁸ and Eighth⁷⁹ Circuits, as well as the Minnesota Supreme Court⁸⁰ have applied a “knowledge-plus” standard, requiring a plaintiff to prove that a defendant knew of the plaintiff’s residence *and* to present other facts that demonstrate the defendant intentionally targeted the forum state. Petitions for certiorari are pending in both the *Tamburo* and *Roberts* cases, so it is possible that the Supreme Court will step in to provide much-needed guidance in this increasingly important (and increasingly confusing) area of the law.

It should be noted that the above cases discuss jurisdiction to adjudicate. There have also been legal battles over the jurisdiction to prescribe and the jurisdiction to enforce. For example, Minnesota courts permitted Minnesota to enforce its anti-gambling laws against foreign defendants because the defendants solicited Minnesota residents to gamble via the internet.⁸¹ Similarly, a couple maintaining a bulletin board service in California was convicted of obscenity in Tennessee because they knew Tennessee residents subscribed to their service.⁸² However, as noted above in Part II, attempts by individual states to proscribe certain activities on the internet are increasingly being limited by the dormant commerce clause.

Finally, the most significant development in U.S. law in this area is the recent enactment of the Securing the Protection of our Enduring and Established Constitutional Heritage Act (the “SPEECH Act”),⁸³ which prohibits both state and federal courts from recognizing or enforcing foreign judgments for defamation if: (1) the judgment is inconsistent with the First Amendment, (2) the foreign court failed to comport with the due process requirements that are imposed on domestic courts by the U.S. Constitution, or (3) the judgment is inconsistent with section 230 of the Communications Decency Act. The SPEECH Act also provides that a U.S. citizen who opposes the recognition or enforcement of a foreign judgment may sue the judgment holder in federal court for a declaratory judgment that the foreign judgment is invalid.⁸⁴ The Act facilitates these actions by providing for nationwide service of process on foreign judgment holder. Moreover, the Act includes as an additional incentive a provision allowing successful plaintiffs in these actions to recover reasonable attorneys’ fees.

Although the SPEECH Act is an important step toward protecting publishers from liability for online content, it is not a panacea. For instance, because the Act addresses only the enforcement jurisdiction of U.S. courts, it will not prevent a judgment from being enforced against a U.S.-based company that has assets abroad. Because many of the leading media companies have bureaus and other significant resources in countries around globe, they may still face significant judgments for conduct that is protected by the First Amendment. Furthermore, the Act does not address the increasing number of *criminal* cases to have been lodged against U.S. defendants for defamation. Although the defendants in those cases do not face monetary liability, they may be restricted on where they can travel because of international warrants for their arrest.

Still, the Act is certainly a bright spot in an otherwise bleak area of the law. The Act will provide much-needed protection to smaller companies and individuals, such as Ehrenfeld, whose case we discussed above. Perhaps more important than this, though, is the Act’s status as a symbol of U.S. opposition to the troubling practices of those foreign governments that have impeded the free flow of information by allowing U.S. media outlets to face lawsuits merely for reporting the news.

VII. Conclusion

While certain principles relating to jurisdiction in the internet era are becoming clearer, the situation outside the United States suggests that the applicable rules may be murky for some time yet. Uncertainty, particularly coupled with a challenging business environment, can act as a damper on investment and innovation. The uncertainty has never been more problematic for businesses than it is now, as we stand at the brink of a new era in computing. The rise of “cloud computing”—a model of computing in which user files and applications are provided over the internet—promises to make available to businesses, governments, and individuals computing power and efficiency that previously were unimaginable. But because the basis of cloud computing is the provision of services via the internet—and thus accessible from anywhere in world—the companies that provide these services must be prepared to navigate the unpredictable and sometimes hostile legal universe described in this Article.

⁷⁸ See *Revell v. Lidov*, 12 ILR 629, 317 F.3d 467 (5th Cir. 2002).

⁷⁹ See *Johnson v. Arden*, 30 ILR 635, 614 F.3d 785 (8th Cir. 2010).

⁸⁰ See *Griffis v. Luban*, 11 ILR 305, 646 N.W.2d 527 (Minn. 2002).

⁸¹ *Minnesota v. Granite Gate Resorts, Inc.*, 1 ILR 165, 568 N.W.2d 715 (Minn. Ct. App. 1997).

⁸² *United States v. Thomas*, 2 ILR 22, 74 F.3d 701 (6th Cir.), *cert denied*, 519 U.S. 820 (1996).

⁸³ See Pub. L. No. 111-223, 124 Stat. 2380 (to be codified at 28 U.S.C. §§ 4101-4105).

⁸⁴ *Id.* at §4014.

The brightest spots on the horizon are the EU's E-Commerce Directive and the related concepts in the AVMS Directive, with their sensible approach to apportionment of legal responsibility, and the SPEECH Act in the United States, which will provide certain protections for online publishers. Developments in other countries, however, continue to be troubling, with courts outside the United States almost uniformly seizing jurisdiction over disputes that arose away from their territory. This area will demand increasing vigilance in the near term. Online businesses are advised to utilize self-regulatory measures, including appropriate site design, language, and content, to mitigate the effects of uncertain jurisdictional laws. And technology and media lawyers should be alert to the increasing potential for foreign claims and become conversant in the relevant laws that may apply outside of the United States.

This is particularly true as cloud computing becomes more prevalent as a part of the internet ecosystem. As the cloud evolves, and as providers begin to process and store greater amounts of user data, they face a growing dilemma. Governments increasingly are focused on obtaining access to user content and other data held by cloud service providers. Multiple jurisdictions may have an interest in a single matter, each seeking access to user information. There are, however, no universally agreed upon rules governing such access by law enforcement. The result is that service providers are increasingly subject to divergent, and at times conflicting, rules governing jurisdiction over user content and data. In addition, the presence of data in a particular country could be used as a justification for exercising jurisdiction over the owner of that data, frustrating the concept that the rights and obligations of an internet publisher should be governed by the laws of the country of origin.

This global thicket of competing and conflicting laws presents a significant obstacle to the delivery of cloud services that meet users' reasonable expectations of privacy. Where the rules of different nations conflict, a cloud provider's decision to comply with a lawful demand for user data in one jurisdiction may place a provider at risk of violating the privacy or other laws of another jurisdiction. Equally troubling, this situation makes it extremely difficult for providers to give their customers accurate and adequate notice of the conditions under which their data might be accessed by law enforcement. For cloud computing to realize its full potential, significant law reform efforts may be required to provide the consistency and predictability needed to foster confidence in this inevitable extension of technology for data storage and access.
