Cornell Law Review

Volume 99
Issue 6 *September 2014 - Symposium on Extraterritoriality*

Article 5

New Territorialism in the Not-So-New Frontier of Cyberspace

Juliet M. Moringiello

William L. Reynolds

ESSAY

THE NEW TERRITORIALISM IN THE NOT-SO-NEW FRONTIER OF CYBERSPACE

Juliet M. Moringiello† *& William L. Reynolds*††

INTRODUCTION

Who should govern cyberspace? And what rules should apply? When Professor Louise Weinberg invited us to contribute to this symposium, she asked us to write on governance issues in the new frontier of cyberspace. That could have been a daunting task. The electronic world we live in today presents many challenges. Fortunately, cyberspace is no longer new, and many before us have attacked the broad governance questions that arise when persons all over the world communicate and transact business using the global Internet.[1] As a result, we need not tackle those larger questions; rather, we will discuss what the Supreme Court's recent imposition of territorial limits in various

† Professor, Widener University School of Law.

†† Jacob A. France Professor of Judicial Process, University of Maryland Francis King Carey School of Law. Thanks to Wil Marchica, Maryland Law School class of 2014, for research assistance.

1 *See, e.g.*, Dawn C. Nunziato, *Freedom of Expression, Democratic Norms, and Internet Governance*, 52 EMORY L.J. 187, 192–93, 196–214 (2003) (examining the impact of the Internet Corporation for Assigned Names and Numbers' authority over the Internet's infrastructure on free speech); Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 815 (2004) (identifying the fundamental question of Internet governance as "whether and how the architecture of the Internet should affect the shape and content of legal regulation of the global network of networks").

areas of law means to disputes that arise from interactions that take place electronically. Rather than discussing who should govern cyberspace, we will focus on the question of whose rules should apply.

Our assigned task implies that the frontiers of cyberspace differ from the frontiers of the tangible world. In one sense, that is true: the Internet is a global "network of networks," enabled by the Transfer Control Protocol/Internet Protocol (TCP/IP), which allows any computer in the world to communicate with any other computer in the world.[2] On the other hand, however, the interactions conducted over this global network have tangible world effects that are often no different from the pre-Internet era tangible world effects of tangible world activities. This is true regardless of the number of exotic jurisdictions through which electronic information may pass on its journey from point A to point B.

So what insight do we have concerning who should govern cyberspace? We propose a simple framework. At the core of that framework is our recognition that the term "cyberspace" refers to a means of communication. This means of communication allows individuals and entities to engage in the same interactions using electronics in which they engage in the face-to-face world. Cyberspace, as a method of communication, in other words, removes spatial constraints from these interactions. Therefore, persons can interact at no additional cost with others located in far-flung jurisdictions. Does the removal of cost and spatial constraints change the legal nature of the interaction?

Our framework separates the substance of the interaction from the method of communication. Most cyberspace problems are not unique to this century. As Debora Spar wrote in 2001, "[c]yberspace is indeed a brave new world, but it's not the only new world."[3] In past centuries, telegraphy[4] and radio[5] were similarly transformative technologies in that they allowed the instantaneous, or almost instantaneous, transmission of content to geographically far-flung recipients. Courts experienced little or no difficulty—at least as seen from this distance—when dealing with the new technology. Is there anything about cyberspace that makes it different?

We acknowledge that this history of technology and cyberspace is one step in the evolution of communications technology. Therefore,

---

2 Solum & Chung, *supra* note 1, at 821. *See* MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 6 (2004).

3 DEBORA L. SPAR, RULING THE WAVES: CYCLES OF DISCOVERY, CHAOS, AND WEALTH FROM THE COMPASS TO THE INTERNET 3 (2001).

4 *See id.* at 62 (describing telegraphy as a "more dramatic" innovation than today's Internet because it "made irrelevant distances that had once seemed unbreachable, and widened the perspective of nearly all the world's people").

5 *See id.* at 125 (attributing the power of radio to its "inherent capacity . . . to send a single message across a wide and unidentified audience").

in the first instance, we view cyberspace problems as common problems that the law—both statutory and judge-made—has had centuries to deal with, understand, and resolve. Under our framework, that hard-won collective wisdom should be displaced only if the world of cyberspace creates a world different not only in technology but also in concept. In other words, is there something fundamentally different about cyberspace so that it creates qualitatively different legal problems? It is only when that happens that cyberspace-specific solutions should be adopted.

Finally, we have asked if American courts have been "territorial" in their approach to either multistate or international problems. We have then asked, if so, whether that territorial approach makes sense.

The short answer is that American courts have not gone out of their way to assume control over these problems. Rather, the preference has been to use well-established precedents to resolve situations. In other words, American courts have overtly deferred to American law in cyberspace transactions only when fundamental American issues—such as free speech—are at stake. Our courts have shown little appetite for neo-territorialism, unless something vital to our own interests is involved. That is not a complete answer, however, for it does not answer the question whether those precedents lead to overly territorial results. Alas, that too is beyond the scope of this Essay.

In this short Essay, we cannot possibly address all governance problems in cyberspace. In the early days of cyberlaw scholarship, Judge Frank Easterbrook asked whether cyberspace law was just "the law of the horse."[6] His point was that just as any attempt to gather all of the cases involving horses into a law of the horse was "doomed to be shallow and to miss unifying principles,"[7] so too might an attempt to isolate a discipline called cyberspace law. We heed this warning, and in this Essay we reflect on the effect that electronic communications has had on the substantive areas of law about which we teach and write. We have chosen not to consider issues involving governmental eavesdropping—solutions, if any, to those problems can come only at the national, or perhaps, international level. What we do address are issues common to everyday life—contracts, jurisdiction, choice of law, taxation, and some torts, including defamation and privacy. All of these questions raise governance issues; they do not, however, tell us on their face who should control cyberspace.

---

6 Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 208.

7 *Id.* at 207.

I
A Note on the Past

Twenty years ago, many argued that cyberspace presented a different legal environment.[8] One well-known screed by John Perry Barlow, the former Grateful Dead lyricist who cofounded the Electronic Frontier Foundation,[9] put it this way: "[cyberspace] is a world that is both everywhere and nowhere, but it is not where bodies live."[10] Barlow went on to proclaim that the tangible world concepts of "property, expression, identity, movement, and context" do not apply in cyberspace.[11] He was not alone; many proclaimed the dawning of a new age, where different rules—or maybe no rules—would control. The feeling of a new era became compounded when litigation inevitably arose where at least one party would contend that the old rules should no longer apply.[12]

These proclamations were based on the faulty premise that cyberspace was a new world, unlike any other. The word "cyberspace" itself encourages adoption of this premise, strongly implying that this mode of interaction is in fact a place. Although the original author of the term, cyberpunk author William Gibson, denounced it as an "'evocative and essentially meaningless' buzzword,"[13] "cyberspace" became the preferred term for talking about and analyzing all things electronic.[14] As a result, some courts and commentators started to approach issues involving interactions conducted electronically as though the fact of their electronic genesis needed a whole new analysis of the harm or transaction.[15] Other commentators, however, approached Internet regulation not on a transaction or interaction basis

---

8 *See infra* notes 15–17 and accompanying text. *See, e.g.*, Lawrence Lessig, Commentary, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev. 501, 505–11 (1999) (arguing that cyberspace has an "architectural feature" that complicates legal regulation and noting that some scholars believe that regulation is impossible).

9 *See* Barlow Home(stead) Page, https://homes.eff.org/~barlow/ (last visited July 14, 2014).

10 John P. Barlow, *A Declaration of the Independence of Cyberspace*, Barlow Home(stead) Page (Feb. 8, 1996), https://projects.eff.org/~barlow/Declaration-Final.html.

11 *Id.*

12 The new world was full of money-making opportunities; it was not as innocent as Barlow and others thought. Squabbling over money leads to litigation.

13 Scott Thill, *March 17, 1948: William Gibson, Father of Cyberspace*, Wired, Mar. 17, 2009, http://www.wired.com/science/discoveries/news/2009/03/dayintech_0317.

14 *See, e.g.*, *Cyber Glossary*, Nat'l Initiative for Cybersecurity Careers & Studies, U.S. Dep't of Homeland Sec., http://niccs.us-cert.gov/glossary#letter_c (last visited Mar. 15, 2014) (defining "cyberspace" as "[t]he interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers").

15 *See, e.g.*, Danielle K. Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age,* 80 S. Cal. L. Rev. 241, 295 (2007) (arguing that "[o]ur conception of injury must undergo change in the twenty-first century").

but on an architecture basis,[16] and they proposed Internet governance regimes that took the Internet's architecture into account. Probably the most prominent of these commentators was Lawrence Lessig, who argued that the greatest challenge in regulating cyberspace was how to make sense of the "software and hardware that make each cyber-space the way it is."[17]

Things eventually sorted themselves out, however. When faced with questions involving the Internet, the judges did what they have been trained to do and embarked on a search for analogy. To be sure, that took some effort, and it was some time before courts began to feel comfortable in opining on the new world that was opening before them. That is very clear (and understandable). Opinions written fifteen or twenty years ago showed an earnest attempt by judges to understand the Internet and how it works in modern life.[18] Those opinions are quite touching when read in retrospect;[19] although the judges showed their good faith attempts to understand the new technology, they often got it wrong. Eventually, however, both the judges and their clerks came to understand things better, and today the world of electronic interactions has become very well settled.

A number of scholars took somewhat longer to realize these truths. Perhaps that is because novelty has a premium in academic life: status there depends much more on new ideas rather than on clarifying old truths. It is much better for a professor's career to create new concepts, no matter how wrong-headed, than to say that the old law got all of this right.[20] In short, for many professors, novelty trumps analysis. Although that predilection for novelty led to many wrong turns in dealing with problems involving electronic transactions,[21] the courts eventually got it right. Litigation today involving

---

16 An "architecture basis" assumed that the structure of the Internet might by itself require a separate analysis. *But see* Lessig, *supra* note 8, at 505–06 & n.13 (criticizing arguments that the nature of cyberspace eliminates the government's capacity to regulate).

17 *Id.* at 503.

18 For example, consider a line of cases in which various courts attempt to analyze types and levels of Internet activity that are sufficient to establish personal jurisdiction. *See, e.g.*, CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996) (regularly sending electronic files); Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996) (maintaining advertisements on a website); Bensusan Rest. Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996) (posting information on a website); Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328 (E.D. Mo. 1996) (forwarding advertisements and encouraging the use of an electronic mailing list).

19 Perhaps the most touching of all these attempts is *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997), where the judge tries so very hard to understand the Internet and yet manages to mangle the law badly.

20 We discuss this problem in more detail in Juliet M. Moringiello & William L. Reynolds, *From Lord Coke to Internet Privacy: The Past, Present, and Future of Electronic Contracting*, 72 MD. L. REV. 452 (2013).

21 *See* discussion *infra* Part IV.A.

electronic transactions is virtually indistinguishable from that involving old-fashioned paper contracts.[22]

That is not our approach in this Essay. We contend that centuries of legal experience have provided ample guidance to deal with most issues. It is only when the new world provides us with unique problems that new solutions need to be found. In the world of potential cyberspace governance, lines of demarcation of authority have long been laid out and are well understood. That understanding can be traced to the opinion by Justice Curtis in *Cooley v. Board of Wardens*[23] where the Court recognized that some problems required a national solution, some demanded a local solution, and many could be handled at either level.[24]

Similarly, in the electronic world, the real question becomes whether there is something so special about that world that renders the long-settled rules in the area no longer relevant. Basically, that leaves us with two issues: first, those concerning the technical structure of the electronic world, and second, issues involving the permanence and unlimited range of electronic transactions. With regard to the latter, we mean that electronic transactions can occur anyplace in the world and they have the potential to last forever.

II
The New Territorialism and Cyberspace

The topic of this symposium is the "new territorialism" displayed by the Supreme Court in decisions such as *Kiobel v. Royal Dutch Petroleum*[25] and *Morrison v. National Australia Bank*.[26] In those cases, the Court applied a canon of statutory interpretation that provides that a statute has no extraterritorial application unless it gives a clear indication that such an application should be found.[27] The presumption "rests on the perception that Congress ordinarily legislates with respect to domestic, not foreign matters."[28] We were asked to write about cyberspace, so the question we explore is this: Where does activity in cyberspace take place under *Kiobel* and *Morrison*?

Here, it is helpful to refine what we mean when we talk about cyberspace. Despite John Perry Barlow's proclamation that cyber-

---

22 *See* Moringiello & Reynolds, *supra* note 20, at 457–58 & n.31.

23 53 U.S. 299 (1851).

24 *See id.* at 319; *see generally* Ronald D. Rotunda & John E. Nowak, Treatise on Constitutional Law: Substance and Procedure § 11.4 (5th ed. 2012) (explaining the *Cooley* doctrine).

25 133 S. Ct. 1659 (2013).

26 130 S. Ct. 2869 (2010).

27 *See Kiobel*, 133 S. Ct. at 1664; *Morrison*, 130 S. Ct. at 2877–78.

28 *Morrison*, 130 S. Ct. at 2877.

space is "everywhere and nowhere,"[29] cyberspace is not a place. Nor is it a thing. Instead, cyberspace is a collection of networks comprised of physical components such as wires and cables, and digital components such as software and transport protocols, which allow the content generated by persons using computers connected to the Internet to flow through the network.[30]

On the one hand, cyberspace is a method of communication. When we send an e-mail message or post an update to Facebook, our communication is facilitated by cyberspace. When cyberspace functions only as a method of communication between two entities, there may be little reason to treat cyberspace any differently from how we treat the telephone.[31]

Cyberspace, however, is also a method of advertising, both in the traditional sense, as when a company establishes a web page that viewers all over the world can see, and in the informal sense, as when an individual posts an update to Facebook or to Twitter. In the advertising sense, cyberspace gives actors a worldwide presence. Is that worldwide presence enough to invite the reach of the laws of myriad jurisdictions? The answer is "maybe." Below, we discuss the problem of collecting sales tax in online transactions. There, we make an argument that the answer is "yes." But that should not always be the case, and the last paragraph of the *Kiobel* opinion reminds us that cyberspace is not the only facilitator of worldwide transactions.[32]

A corporation, unlike cyberspace, is a defined legal entity. But like cyberspace, and unlike natural persons, a corporation can have a worldwide presence. Corporate presence is more definable than cyberspace presence; in order for a corporation to be "present" in a jurisdiction, it must be doing something there through its agents and physical presence, or someone must register it in the jurisdiction.[33] In *Kiobel*, Chief Justice Roberts reminds us that although corporations can be present in many jurisdictions, "it would reach too far to say that mere corporate presence suffices" to defeat the presumption against extraterritoriality.[34] The same rule should apply to interactions conducted over the Internet. If the interaction truly takes place "everywhere and nowhere," it may need to be regulated in an Internet-

29 Barlow, *supra* note 10.

30 *See* Solum & Chung, *supra* note 1, at 816–17 (explaining the different layers of the Internet "[v]iewed as a system of communication between users").

31 One difference is that e-mail messages can be stored at virtually no cost.

32 *See Kiobel*, 133 S. Ct. at 1669.

33 *See, e.g.*, 28 U.S.C. § 1408 (2012) (allowing an entity to file for bankruptcy in the district in which it has its domicile, principal place of business, or principal assets); U.C.C. § 9-307 (stating that the location of a registered organization is the state in which it is organized).

34 *Kiobel*, 133 S. Ct. at 1669.

unique way. If the interaction is one that would have the same impact if conducted over the phone or by a fax machine, then it probably does not require a unique regulatory mechanism.

On the other hand, the Internet raises several unique questions. Some arise from the architecture of the Internet. We address one of those issues, that of Internet domain names, in the next section. Others arise from the advertising nature of the Internet. The telephone is a communication device, but a telephone conversation transmits information to a finite number of persons in known jurisdictions. The Internet is different because it conveys information to an infinite number of persons across the globe. It is easy to argue that the mere existence of information on a web page gives the effect of that information worldwide ramifications. Certainly that is the approach taken in *Yahoo! Inc. v. La Ligue Contre Le Racisme et l'Antisemitisme (LICRA)*,[35] which we discuss below.

We do not discuss issues where national (or international) treatment is clearly appropriate. The most obvious of such areas involve electronic eavesdropping,[36] but there are many others, which space does not permit us to talk about.

III
How Do I Find You If You Are Everywhere and Nowhere?

Telephones allow persons all over the world to communicate directly with one another. In order to do so, each person connected with a phone must have a phone number. In the days of landlines, the responsibility for distributing phone numbers was easily assigned. Phone numbers had some relationship to physical location. One person could have the number 555-1212 in Washington, D.C., and another could have the same number in New York City, because those two locations had two different area codes. On the other hand, no two persons could have the same number with the same area code. As mobile phones proliferated, the phone numbers, at least in the United States, remained tied to geography.

Just as one can reach a telephone customer only by using her unique identifier, one can find an entity on the Internet by using its unique identifier. On the Internet, this identifier is the domain

---

35 433 F.3d 1199 (9th Cir. 2006) (per curiam) (en banc).

36 Electronic eavesdropping is normally associated with governmental snooping. The resolution of those issues is clearly beyond the authority of national courts applying national territorial-based law. *See* Charlie Savage & James Risen, *Latest Release of Documents on N.S.A. Includes 2004 Ruling on Email Surveillance*, N.Y. Times (Nov. 18, 2013), http://www.nytimes.com/2013/11/19/us/latest-release-of-documents-on-nsa-includes-2004-ruling-on-email-surveillance.html.

name.[37] Many domain names are "everywhere and nowhere." A holder of a domain name in the ".com"-level domain can be located anywhere in the world, but often the name sends no signal about its holder's geographical location.[38] Domain names require an international regime for two reasons, one related to Internet technology and the other related to Internet impact.

The technology reason is this: a domain name is a unique, worldwide identifier. In the physical world people can distinguish United Airlines from United Van Lines. They cannot both be known as "united.com" on the Internet, however.[39] Because every web address must translate to a unique computer, the assignment of web addresses in the Domain Name System (DNS) must be, and is, managed by a central authority.[40]

The Internet Corporation for Assigned Names and Numbers (ICANN) was created in 1998.[41] ICANN replaced the U.S. government as the sole assignor of domain names on the Internet.[42] It should be quite clear that one and only one authority can control the assignment of domain names. Not only has ICANN done that well in the past, but it recently expanded greatly (for better or worse) the galaxy of available top-level domain names.[43]

The Internet technology that led to worldwide domain names created a clash among trademark regimes. Domain names often incorporate trademarks, and because domain name registrars do not vet domain name requests before granting them, it is easy for someone other than a trademark holder to register a mark.[44] In the early days

---

37 Juliet M. Moringiello, *Seizing Domain Names to Enforce Judgments: Looking Back to Look to the Future,* 72 U. CIN. L. REV. 95, 95 (2003) ("A domain name is the identifier used by individuals to find specific web sites.").

38 Of course, many domain names are country specific. *See* Paul Sloan, *Staking A Claim On Domains Beyond Dot-Com*, CNNMoney (Aug. 29, 2006, 10:45 AM), http://money.cnn.com/2006/08/29/technology/nextbigforeign.biz2/.

39 *See* Moringiello, *supra* note 37, at 119.

40 Anupam Chander analogizes the DNS to a worldwide property registry. *See* ANUPAM CHANDER, THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD IN COMMERCE 110 (2013).

41 *Id.*

42 *Registrar Accreditation: History of the Shared Registry System*, ICANN, http://www.icann.org/en/resources/registrars/accreditation/history (last visited July 14, 2014). The U.S. government retained oversight of ICANN but announced in March 2014 that it would relinquish its control of the organization. Gautham Nagesh, *U.S. Plans to Give Up Oversight of Web Domain Manager*, WALL ST. J. (Mar. 14, 2014, 7:01 PM), http://online.wsj.com/news/articles/SB10001424052702303546204579439653103639452.

43 *See New Generic Top-Level Domains*, ICANN, http://newgtlds.icann.org/en/about/program (last visited July 14, 2014) (explaining ICANN's process for introducing new generic top-level domains). Top-level domains include ".com," ".net," and ".edu." Generic top-level domains are those that are not restricted to residents of a particular country. Moringiello, *supra* note 37, at 97–98.

44 *See* Moringiello, *supra* note 37, at 100 ("The registrar does not inquire as to whether anyone else has trademark rights in the name.").

of the Internet, it was common for cybersquatters to register the names of large companies in order to try to coerce those companies into paying for a transfer of the name.[45] Because these problems are felt worldwide, ICANN implemented the Uniform Domain Name Resolution Policy (UDRP), a policy to which all domain name registrants must agree.[46] The UDRP requires that domain name registrants agree to arbitrate any claims that the name infringes on the rights of a trademark holder.[47] By implementing the UDRP, ICANN, an American entity, has regulatory authority over all domain name registrants in the top-level domains in ICANN's control.[48]

Even domain names cannot truly be "everywhere and nowhere," however. Someone in a physical location must have the power to identify and regulate those names. Congress recognized this fact in enacting the Anticybersquatting Consumer Protection Act (ACPA).[49] The birth of the World Wide Web and the Domain Name System gave rise to a form of wrongdoing that was unique to cyberspace: cybersquatting. Cybersquatters reserved high-profile domain names such as "eddiebauer.com" and "neiman-marcus.com," hoping to sell them for a high price to the holders of the trademarks incorporated in the names.[50] Many of these domain name registrants used fictitious names and addresses or registered the domain names in the name of offshore companies, in an attempt to evade jurisdiction.[51]

To address the cybersquatting problem, Congress gave domain names a situs and provided for *in rem* jurisdiction over them.[52] Under the ACPA, an aggrieved trademark holder may bring an *in rem* action against a domain name in the judicial district in which the domain name registrar or registry is located.[53] This makes sense—intangible property should be located at the place in which its controller resides. To some, however, this is a "particularly obnoxious example of expansive U.S. claims to regulate domain names," and it is a poor substitute

---

45 *See id.* at 120–21.

46 *Uniform Domain Name Dispute Resolution Policy*, ICANN, http://www.icann.org/en/help/dndr/udrp/policy (last visited July 14, 2014).

47 *See id.* at ¶ 4 ("You are required to submit to a mandatory administrative proceeding in the event that a third party (a 'complainant') asserts to the applicable Provider, in compliance with the Rules of Procedure, that (i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and (ii) you have no rights or legitimate interests in respect of the domain name; and (iii) your domain name has been registered and is being used in bad faith.").

48 *See* CHANDER, *supra* note 40, at 110.

49 15 U.S.C. § 1125(d) (2012).

50 *See* Thomas R. Lee, *In Rem Jurisdiction in Cyberspace*, 75 WASH. L. REV. 97, 104 (2000).

51 *See id.* at 106.

52 *See* 15 U.S.C. § 1125(d)(2)(A) (providing that "[t]he owner of a mark may file an in rem civil action against a domain name").

53 *See id.*

for international coordination.[54] That criticism is wrong: someone needs to control domain names and the United States stepped into the vacuum. Perhaps the American position as arbiter in some sense of ICANN makes sense, but the United States certainly seems to have foregone the opportunity to regulate in favor of other, more likely sources.[55]

The lesson to be drawn from the domain names story is that sometimes, American neo-imperialism works to satisfy the universal good. In other words, some problems require a system-wide solution. The assignment of domain names was one of those, and the solution has worked out well. We now address questions concerning electronic transactions and specific issues, either procedural or substantive. In that analysis, we address the following issues: electronic contracts, long-arm jurisdiction, interstate defamation, revenge porn, Internet privacy, interstate taxation, and regulatory jurisdiction.

IV
Where the Traditional Rules Work

In this Part, we first discuss topics where the old law provides the proper method of analysis. We then discuss areas where cyberspace might lead us to think about answers to problems that differ from the digital or paper world. Finally, we draw conclusions concerning when "old" or "new" law is appropriate. We apply our analytical framework first to electronic contracting because we have developed our analysis in this area over the course of several years.

Electronic contracts. Electronic contracting provides an example of an Internet interaction that is not "everywhere and nowhere." Like a phone conversation, a contract must affect a finite number of people in that in order to be bound by an agreement, a party must have assented to it. In order to assent, the party must know the identity of the person with whom he is dealing. Internet contracts may raise special issues because the lack of spatial constraints allows vendors to offer more, and perhaps more onerous, terms than they do on paper;[56] however, they do not raise governance issues. Choice-of-law analysis should not depend on the medium of exchange. Rather, the question has to be whether there has been adequate notice to both parties. If

54 Catherine T. Struve & R. Polk Wagner, *Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act*, 17 Berkeley Tech. L.J. 989, 1039 (2002).

55 *See, e.g.*, Gary B. Born, International Civil Litigation in United States Courts: Commentary & Materials, 497–501 (3d ed. 1996) (discussing U.S. attempts to expand jurisdiction and apply its laws extraterritorially).

56 *See* Nancy S. Kim, Wrap Contracts: Foundations and Ramifications 125 (2013) ("Wrap contracts, by their form, permit companies to impose more objectionable terms than paper contracts of adhesion.").

that notice has been given, then the result should be the same under any form of analysis.

In a series of annual surveys published in *The Business Lawyer* from 2005 to 2010[57] we examined the law of electronic contracting. When we began those surveys, many scholars and courts believed that special rules should be adopted for electronic contracting. In particular, concepts such as "clickwrap" and "browsewrap" were thought to require special rules, rules that were separate from the general contract law that we teach students and which can be found in the Contracts Restatements and the Uniform Commercial Code.[58] The push for special rules in the "wrap" area, especially by academics, was so strong that the American Law Institute (ALI) even convened a group to suggest "principles" that might govern software transactions.[59] This project necessarily examined Internet contracting because the rise in computer use by individuals in the waning years of the twentieth century and the early years of the twenty-first century led to two parallel developments: the transfer, by way of standard form terms, of computer programs designed for individual use, and the use of the Internet to enter into bargained-for relationships.[60] As time went on, software vendors delivered their standard terms not in a shrink-wrapped box containing a plastic disk, but over the Internet by a clickwrap agreement accompanying downloaded software. We were dubious of the argument that the ordinary rules of contracting did not control e-contracts.

Events have proven us right. In particular, the ALI *Principles of Software Contracts* have been (overwhelmingly) ignored by the courts,[61] and basic contract principles have won the day. Internet "exceptionalism" lost out to the law of contract that had been hammered out over the centuries. Today, it is quite clear that the vast majority of online agreements present problems that differ little from those presented by paper or oral agreements. Even electronic contracts between parties in two different countries do not raise unique issues. A person negotiating by phone or by fax trusts that the voice, phone number, or signature belongs to a known party. Purely electronic verification is more difficult, but the problem is one of trust, which exists any time two parties negotiate in any environment other than the face-to-face environment. In the paper world, notaries serve a verification pur-

---

57 Juliet M. Moringiello & William L. Reynolds, *Electronic Contracting Cases 2009–2010*, 66 BUS. LAW. 175 (2010); Juliet M. Moringiello & William L. Reynolds, *Electronic Contracting Cases 2008–2009*, 65 BUS. LAW. 317, 317 n.1 (2009) (listing the previous surveys).

58 *See* Moringiello & Reynolds, *supra* note 20, at 454–55.

59 *See id.* at 474.

60 *See id.* at 454.

61 *See id.* at 491 (noting that "the American Law Institute's project, *Principles of Software Contracts*, met with a lackluster response").

pose. They can do so in the electronic world as well, and there are initiatives on the national level[62] to modernize and simplify notarial verification and attestation of signatures. A similar international initiative is desirable. To be sure, occasionally an agreement will present different problems; but those situations are so rare that they deserve no special category.

That is not to say that basic common law concepts control everything.[63] As we pointed out in a recent article, there are many things that those concepts do not adequately address.[64] We gave as examples privacy policies, the application of the Computer Fraud and Abuse Act, and intelligent agents.[65] We believe, however, that eternal verities generally hold true, and that the underlying everyday law that existed before cyberspace was invented controls most everyday transactions, except for those few situations where special rules are necessary because of the unique properties of cyberspace.

Long-arm jurisdiction. The cyber world certainly raises many questions involving multistate problems, problems that American lawyers generally place under the heading of long-arm jurisdiction. For a while it looked as though long-arm jurisdiction involving the Internet also would develop a set of special rules, rules different from those found in electronic transactions. There were two main categories of cases that led to that concern—interstate contracting and Internet defamation. After some fumbling and hesitation, the courts eventually decided that new rules were not necessary to deal with the online world.

Courts seemed befuddled at first with cases involving jurisdictional questions involving contracts concluded over the Internet. The leading case for many years was *Zippo*,[66] a case where the judge was so confused that he chose to ignore long-standing Supreme Court precedent and create a new and separate world of long-arm jurisdiction for

---

62 *See* REVISED UNIFORM LAW ON NOTARIAL ACTS, NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS 2010, *available at* http://www.uniformlaws.org/shared/docs/notarial_acts/rulona_final_10.pdf.

63 *See generally* Moringiello & Reynolds, *supra* note 20, at 457–58, 496 (discussing how efforts to change the common law failed because "contracts for information . . . need[ed] a different law from that applied to all other agreements").

64 *See id.* at 480–87 (discussing how the common law must be creatively used and adapted to meet the changing conditions posed by electronic contracts).

65 *See id.* at 481–87.

66 Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997). *Zippo* adopted a sliding-scale approach to the Internet jurisdiction problem, even though that approach had been soundly rejected years earlier by the Supreme Court in *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408 (1984). Although profoundly wrong on its face, the *Zippo* opinion was routinely cited as authoritative for many years.

the Internet.[67] For some mysterious reason, *Zippo* became a must-cite in long-arm Internet cases, but it quickly became a *de rigeur* cite that was ignored as soon as it was mentioned.[68] *Zippo* was typical of cases involving online transactions fifteen or twenty years ago. The judges did not understand the Internet and groped mightily in their opinions with an effort to understand it (no doubt aided by law clerks who tried to bring their bosses into the modern world).[69] About a dozen years ago, courts began to feel comfortable with the modern world, and the decisions involving the Internet assumed a much more realistic flavor.

There was no good reason for this confusion. Although the Supreme Court has never expressly addressed the question of online jurisdiction, courts had long dealt with problems involving similar transactions in the analog world. Perhaps the most common analogy was to book-catalog sales, a problem that the courts had long ago resolved in a satisfactory doctrinal fashion.[70] Eventually, however, the courts in Internet jurisdiction cases signed off on the analogies that were familiar to them.[71] Long-arm jurisdiction involving the Internet,

---

67 *Zippo* distinguished between passive and active websites, a not-bad analysis, but also adopted a sliding-scale approach which directly conflicted with the Supreme Court's decision in *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408 (1984).

68 Perhaps the leading case rejecting the *Zippo* line of reasoning is *ALS Scan, Inc. v. Digital Serv. Consultants, Inc.*, 293 F.3d 707 (4th Cir. 2002). The *ALS Scan* decision does not reject the framework proposed in *Zippo*; it actually used the *Zippo* framework as a starting point for its own analysis:

> Drawing on the requirements for establishing specific jurisdiction, . . . which requires *purposeful* conduct directed at the State and that the plaintiff's claims arise from the purposeful conduct, we adopt today the model developed in [*Zippo*].
>
> . . . .
>
> Thus, adopting and adapting the *Zippo* model, we conclude that a State may, consistent with due process, exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts.

Id. at 713–14. According to Westlaw, *Zippo* has eighty-one instances of negative treatment, with *Howard v. Missouri Bone and Joint Center, Inc.*, 869 N.E.2d 207 (Ill. App. Ct. 2007), being perhaps the most negative.

69 We sympathize: one of us was a law clerk who tried long ago to educate a judge about modern physics in a patent case.

70 *See, e.g.*, Quill Corp. v. North Dakota, 504 U.S. 298, 308 (1992) (finding that Quill Corp. had a presence in North Dakota where it sold equipment through catalogues and advertisements).

71 *See, e.g.*, Gator.com Corp. v. L.L. Bean, Inc., 341 F.3d 1072, 1079 (9th Cir. 2003) (using a sliding scale approach for Internet-based firms); Neogen Corp. v. Neo Gen Screening, Inc., 282 F.3d 883, 890 (6th Cir. 2002) (holding that a state has personal jurisdiction when a firm's website "specifically intend[s] [to] interact[ ] with residents of the state"); Mink v. AAAA Dev., LLC, 190 F.3d 333, 336 (5th Cir. 1999) (holding that personal jurisdiction is inappropriate where a nonresident defendant merely establishes a passive website that does nothing more than advertise on the Internet).

in short, does not provide problems that differ in substance (and solution) from those encountered in the real world. Some have suggested that both the permanence and worldwide distribution of the World Wide Web might create a need for special jurisdictional rules.[72] That has not been the case, however, and no special rules have been needed for online problems.[73] This does not mean, of course, that similar fact patterns will always be resolved in similar fashion. It does mean, however, that the lines of analysis will be similar.

Interstate defamation. What happens when someone in State A defames someone in State B using the Internet? This too does not present novel legal problems. The worry in the area is that a defendant will be held amenable to personal jurisdiction for a defamatory publication in a jurisdiction that has little contact with the defendant. An early and controversial case where this was the central issue was *Dow Jones & Co. v. Gutnick*.[74] There, Barron's Online, a subsidiary of Dow Jones, had published a story, available online, that led to a defamation action in Australia, where the plaintiff lived. Many commentators thought it unfair that the defendant, an American-based company, could be forced to travel half a world to defend a publication that did not target Australia.[75]

But that problem also has a print analog. After all, the problem of jurisdiction with the publication of a defamatory statement in a state where the defendant had little presence had been recognized as long ago as 1964 in the famous case of *New York Times v. Sullivan*.[76] The problem is the same today. The analog version of the *New York Times* or *The Economist* is distributed all over the world; why should the digital distribution of the paper lead to a different resolution? As the Australian High Court wrote in *Gutnick*:

> [T]he spectre which Dow Jones sought to conjure up in the present appeal, of a publisher forced to consider every article it publishes on the World Wide Web against the defamation laws of every coun-

---

72 *See* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123–24 (W.D. Pa. 1997).

73 *See, e.g.*, *Neogen Corp.*, 282 F.3d at 889 (applying the minimum-contacts test, which asks whether a corporation "purposely avail[ed] itself of the privilege of conducting activities within the forum State") (citing Hanson v. Denckla, 357 U.S. 235, 253 (1958) (internal quotation marks omitted)).

74 (2002) 210 CLR 575 (Austl.).

75 *See id.* at 654.

76 376 U.S. 254 (1964). The *New York Times* had 394 copies of the print edition that contained the alleged libel. SUSAN DUDLEY GOLD, *NEW YORK TIMES CO. V. SULLIVAN*: FREEDOM OF THE PRESS OR LIBEL? 18 (2007). The Supreme Court did not address the jurisdictional issue, but in holding for the defendants on other grounds, it inferentially upheld the propriety of long-arm jurisdiction in situations where jurisdiction was similarly questionable. The Court eventually soundly repudiated that idea in *Keeton v. Hustler Magazine, Inc.*, 465 U.S. 770 (1984). The problem—publication in a distant forum—is closely related to cyberspace jurisdiction.

> try from Afghanistan to Zimbabwe is seen to be unreal when it is recalled that in all except the most unusual of cases, identifying the person about whom material is to be published will readily identify the defamation law to which that person may resort.[77]

Justice Kirby discussed the fact that the Internet presented a new technology.[78]

> Generally speaking, it is undesirable to express a rule of the common law in terms of a particular technology. Doing so presents problems where that technology is itself overtaken by fresh developments. It can scarcely be supposed that the full potential of the Internet has yet been realised. The next phase in the global distribution of information cannot be predicted. A legal rule expressed in terms of the Internet might very soon be out of date.[79]

In short, new technologies must give way to old legal rules unless a good reason appears for not doing so.

The *Gutnick* case created a lot of concern among commentators about liability for allegedly defamatory publications that have been "published" in a remote forum.[80] That leads to the question of why American authors should be concerned about potential liability in those circumstances. There are three reasons. First, the contact with the foreign jurisdiction may be only incidental (that, of course, is the nature of the Internet); but *Sullivan* teaches us that incidental contact does not preclude the assertion of jurisdiction in defamation actions. Second, the foreign jurisdiction may not provide adequate procedural protections for First Amendment claims. Again, cases such as *Sullivan* and *Gutnick* make clear that insignificant contacts with the forum can still lead to a proper assertion of personal jurisdiction, at least if the defendant has been defamed there.

That leaves us with choice-of-law with respect to the enforcement of judgments. Here Congress has acted and acted appropriately. For the last twenty years, American courts have struggled with the question of whether defamation judgments entered abroad should be enforced in this country, even though the courts in the country where the judgment was rendered do not accord the same level of protec-

---

77 *Gutnick*, 210 CLR at 609.

78 *See id.* at 627 ("Viewed in one way, the Internet is not simply an extension of past communications technology. It is a new means of creating continuous relationships in a manner that could not previously have been contemplated.").

79 *Id.* at 631.

80 *See generally* Eric Barendt, *Jurisdiction in Internet Libel Cases*, 110 PENN ST. L. REV. 727, 728–31 (2006) (discussing the *Gutnick* decision); Peter Bartlett, *Gutnick Shows Need for New International Jurisdictional Principles*, 20 COMM. LAW. 16, 16–17 (2003) (discussing the implications of the *Gutnick* decision).

tion to speech that American courts would.[81] Those cases have generally involved print media, and the courts that were asked to enforce the foreign judgments resolutely have refused to do so.[82]

Although the law seemed well settled, Congress in 2012 felt the need to weigh in with the SPEECH Act.[83] That law basically codified the emergent common-law rule that an American court would not enforce a judgment from abroad where the defendant was not accorded free speech protections similar to those that it would have received in an American tribunal.[84] The lower courts have had no problem applying the SPEECH Act to the cyber world. In *Trout Point Lodge, Ltd. v. Handshoe*,[85] for example, the Fifth Circuit applied the SPEECH Act to a defamation action involving an online blog that allegedly injured the plaintiff in Nova Scotia. Plaintiff recovered a judgment for defamation in Nova Scotia and sought to enforce it in Louisiana. The Fifth Circuit applied the SPEECH Act and denied enforcement.[86]

What is interesting here for our purposes is that Congress codified a solution applicable to online problems that had already been reached by courts dealing with print-based questions. But the SPEECH Act was not superfluous. Given our very strong tradition of protecting speech, there is much to be said for federal action to ensure a uniform national (and protective) result. On the other hand, the SPEECH Act is not an Internet-specific solution, for it applies to all defamation actions, online or not. Once again, the digital world had little new to offer the print world.

V
New Problems—Where the Traditional Rules Don't Work

That observation, however, does not solve problems where the common law result ends in less-than-optimal solutions. Or, to put it somewhat differently, there are problems that need a national (or even international) solution. Assuming there is a problem that needs to be resolved, where should the solution lie? In other words, if the

81 *See, e.g.*, Telnikoff v. Matusevitch, 702 A.2d 230, 251 (Md. 1997) (refusing to enforce a libel judgment entered against a British paper which did not comport with American First Amendment protections).

82 *See, e.g., id.* (refusing to enforce a foreign judgment).

83 Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act, 28 U.S.C. § 4102 (2012).

84 *See id.* ("[A] domestic court shall not recognize or enforce a foreign judgment for defamation unless the domestic court determines that (A) the defamation law applied in the foreign court's adjudication provided at least as much protection for freedom of speech and press in that case as would be provided by the first amendment to the Constitution of the United States . . . .").

85 729 F.3d 481 (5th Cir. 2013).

86 *Id.* at 491–94.

traditional rules do not work, who and what should replace them? We discuss three examples—revenge porn, Internet privacy, and interstate taxation.

Revenge porn. "Revenge porn" provides the first example. This has become a distressingly common problem: one partner takes explicit nude photos of another partner.[87] They split up in a messy arrangement; the aggrieved party then posts sexually explicit pictures of the other on the Internet often leading to negative treatment of the other party, including, but not limited to, harassment and lost professional opportunities.[88] Who should regulate that posting and under what standards?

Ordinary tort law does not give a good answer: an action for invasion of privacy or defamation does not solve the problem that the photos can last forever and certainly can be downloaded and redistributed by anyone who sees them. Thus, although the award of damages in a tort action might be satisfying to the plaintiff, she probably would prefer to have the pictures removed from the Internet entirely. Although that could probably be done under section 230 of the Communications Decency Act,[89] in our cyber world, that is a bit like locking the barn door after the horses have left. A better answer would be to make sure the pictures are never posted in the first place.

So what should be the answer? First, if we assume that tort damages are an inadequate remedy, then the logical answer is to make the posting of revenge porn a crime, a classification that carries with it significant deterrent value. But this answer raises the question of legislative jurisdiction. Can State A make criminal the conduct that occurs in State B (the posting of the pictures) and harms a resident of A? And given the ubiquity of the Internet, do we even know where any of this "takes place"? Can we even tell from where the photos were posted?[90] Additionally, what if State B takes a contrary, free speech–protective approach and legislates to ensure that such a posting is legal?

This is a problem that surely needs a national solution, like the SPEECH Act. Only Congress can solve many of the thorny problems

---

87 We leave aside here pictures taken of underage persons.

88 *See generally* Danielle K. Citron, *'Revenge Porn' Should be a Crime in U.S.*, CNN (last updated Jan. 16, 2014, 3:49 PM), http://www.cnn.com/2013/08/29/opinion/citron-revenge-porn/; Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 345–46 (2014).

89 47 U.S.C. § 230 (1996).

90 Although I may type an entry in State B, my server is located in State C. Unless the seller has asked for a mailing or shipping address, how will it determine what state I am "in"? And does the state where the server is located have regulatory jurisdiction over a seller for that reason alone?

raised by our federal system and present us with a uniform national solution that can be enforced everywhere.[91]

Internet privacy. Privacy rights provide another example. Companies like Facebook and Google collect vast amounts of information on each of us.[92] What rights do we have to limit what those businesses can do with that information? Several states have passed some limits on use of such personal data, but that seems to be an unsatisfactory solution.[93] The reasons are much the same as those set forth in the discussion of revenge porn, but again there is a hurdle: does Facebook know what state I am in when I post on Facebook? My IP address only tells Facebook where my server is located. If I am using a large Internet e-mail provider such as Gmail or Hotmail, Google simply cannot tell what state has an interest in protecting my privacy. So, how does my privacy get protected?

Perhaps there are ways for Facebook to learn my protected personal information, but they might well prove unduly burdensome and costly, and therefore trigger the dormant Commerce Clause concerns Justice Curtis worried about so long ago in *Cooley v. Board of Wardens*.[94] Once again, this is the type of problem that demands a national, uniform solution; one that will benefit both the consumer and the company collecting the data.

But what if Congress cannot agree on a solution? Then we have a problem, leading to a hodge podge of state laws that may well conflict with one another and cause recurring dormant Commerce Clause problems. Perhaps a Uniform Act would be more successful, but such things take a long time. Here, pretty clearly, the need is for national legislation.

---

91 A related problem involves the posting of damaging personal information. Due to free speech concerns, both state and federal governments have been hesitant to regulate this behavior. In 2013, however, California took a big step toward such regulation when it passed a bill protecting children in the state from their own online blunders. The California law requires that all websites, online services and mobile applications where a California minor is registered, have an "eraser button" that allows children and teens to remove information that they posted and now regret posting. James Steyer, *Oops! Button Lets Kids Remove Posts They Regret*, CNN (last updated Sept. 26, 2013, 10:44 AM), http://www.cnn.com/2013/09/26/opinion/steyer-california-eraser-button-law/. Although the law allows for removal of information posted by the individual children themselves, it does not extend to information that has been posted by third parties. Still, this is a step in the right direction, and we hope it will lead to action by Congress, the appropriate body to regulate this field.

92 *See* Ashlee Vance, *Facebook's Is Bigger Than Yours*, BLOOMBERG BUS. WK. (Aug. 23, 2012), http://www.businessweek.com/articles/2012-08-23/facebooks-is-bigger-than-yours; Robert Epstein, *Google's Gotcha*, U.S. NEWS & WORLD REP. (May 10, 2013), http://www.usnews.com/opinion/articles/2013/05/10/15-ways-google-monitors-you.

93 *See* Somini Sengupta, *No U.S. Action, So States Move On Privacy Law*, N.Y. TIMES (Oct. 30, 2013), http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html?ref=onlineprivacyregulation.

94 53 U.S. 299 (1851).

Interstate taxation. Tax provides a third example. Today, cities and states are experiencing fiscal distress to a degree unknown since the Great Depression.[95] Sales taxes provide an important source of revenue for cities and states.[96] The proliferation of online commerce has made an enormous dent in sales tax collection, however.[97] The Supreme Court has held that a state can require a retailer to collect and pay a sales tax only if that retailer has a "substantial nexus" with that state.[98] As a result, an Internet retailer has no obligation to collect sales tax on a purchase made by a resident of a state in which the retailer has no physical presence, either in the form of a bricks-and-mortar store or a sales force in the buyer's state.[99] Although state laws require online purchasers (and offline purchasers who buy goods out-of-state) to remit a use tax to the state in which the goods will be used, enforcement of these laws is notably lax.[100]

Reeling from the loss of sales tax revenue, some states have enacted legislation redefining "substantial nexus" for sales tax collection purposes. The most famous example is that of New York, which in 2008 imposed what is widely referred to as an "Amazon Tax."[101] Under New York tax law, an out-of-state seller is required to collect a sales tax if that seller enters into an agreement with a New York resident under which that resident refers potential customers to the seller, "by a link on an internet website or otherwise."[102] The New York Court of Appeals has upheld the tax;[103] and in December 2013,

---

95 Several municipalities, including most notably Detroit, have taken the rare step of filing for bankruptcy in the past few years. *See* Juliet M. Moringiello, *Goals and Governance in Municipal Bankruptcy*, 71 WASH. & LEE L. REV. 403, 406–07 (2014).

96 Timothy R. Hurley, *Curing the Structural Defect in State Tax Systems: Expanding the Tax Base to Include Services*, 61 MERCER L. REV. 491, 492 (2010) ("In 2008 states collected $240.4 billion in general sales tax, which was less than the $279.1 billion states collected in personal income tax.").

97 *See* Robert W. Wood, *10 Remarkable Facts About Online Sales Tax*, FORBES (Apr. 24, 2013, 1:37 AM), http://www.forbes.com/sites/robertwood/2013/04/24/10-remarkable-facts-about-online-sales-tax/ (reporting that state governments rely on sales and use taxes for a third of their revenue, local governments for just over eleven percent of their revenue, and that lost tax revenue from Internet sales was estimated at over $11 billion in 2012).

98 Quill Corp. v. North Dakota, 504 U.S. 298, 311 (1992).

99 *See id.* at 315 (noting that a vendor's use of a "small sales force, plant, or office" in the taxing state often determines whether that state may impose a sales or use tax on a vendor).

100 *See Overview of E-Commerce Selling Issues*, 27 CORP. COUNSEL'S Q. 716, 771–72 (2011).

101 *See* James G.S. Yang, *Amazon Tax Under Challenge*, 27 J. ST. TAX'N 37, 37 (2009); *see also* Adam Liptak, *Justices Pass on Tax Case from Online Merchants*, N.Y. TIMES, Dec. 2, 2013, http://www.nytimes.com/2013/12/03/business/new-york-ruling-on-sales-tax-collection-by-online-retailers-will-stand.html?_r=0 (noting a Supreme Court decision to uphold the levying of New York sales taxes on Internet retailers).

102 N.Y. TAX LAW §§ 1101(b)(8)(vi), 1131(1) (McKinney 2008).

103 Overstock.com, Inc. v. N.Y. State Dep't of Taxation and Fin., 987 N.E.2d 621, 627 (N.Y. 2013).

the U.S. Supreme Court declined to hear Amazon's appeal of that ruling.[104]

Online vendors may truly be "everywhere and nowhere," thus necessitating a fresh look at how they are treated under the tax laws. The history of the sales tax cases reflects the evolutionary nature of technology and illustrates that online sales are just the most recent point on a spectrum whose earlier points included catalog sales made by mail order and telephone order. The Supreme Court saw the substantial nexus test as a Commerce Clause mandate; under the Commerce Clause, a state may not place an undue burden on interstate commerce.[105]

The world today, however, is substantially different from the world that existed in 1992, when the Supreme Court decided *Quill v. North Dakota*. The business environment in 1992 was in turn different from that in 1967, when the Court had held in *National Bellas Hess, Inc. v. Department of Revenue* that a state could not require a vendor to collect a use tax when that vendor's only connection with the state was by mail or common carrier.[106] In 1967, the Court stressed that requiring an out-of-state vendor to keep abreast of the tax rules in the thousands of American taxing jurisdictions was too great a burden to impose on an entity that received no protection from the taxing jurisdiction.[107] By 1992, significant technological changes had occurred, a point noted both by the North Dakota Supreme Court in the opinion taken to the Supreme Court in *Heitkamp v. Quill*[108] and by the dissenting opinion in *Quill v. North Dakota*.[109] By 1992, computers had made it easier both for companies to comply with the myriad state and local tax laws,[110] and for buyers to place orders with sellers.[111] Ultimately, however, the Court in *Quill v. North Dakota* maintained the physical presence requirement and punted the responsibility for changing that rule to Congress.[112] It will shock no one to learn that Congress has maintained a deafening silence on the subject.

The solution. As we stress above, the Internet is a communications platform. In the realm of sales and advertising, the communications medium matters. When *Bellas Hess* and *Quill* were decided, a vendor had to spend time and money in order to advertise in other jurisdic-

---

104 Robert Barnes, *Supreme Court Declines Case On Making Online Retailers Collect Sales Taxes*, WASH. POST, Dec. 2, 2013, at A1.

105 Quill Corp. v. North Dakota, 504 U.S. 298, 312 (1992).

106 Nat'l Bellas Hess, Inc. v. Dep't of Revenue, 386 U.S. 753, 758 (1967).

107 *See id.* at 759–60.

108 *See* Heitkamp v. Quill Corp., 470 N.W.2d 203, 213 (N.D. 1991).

109 Quill Corp. v. North Dakota, 504 U.S. 298, 328, 332 (1992) (White, J., concurring in part and dissenting in part).

110 *See Heitkamp*, 470 N.W.2d at 213.

111 *Quill*, 504 U.S. at 328 (White, J., concurring in part and dissenting in part).

112 *See id.* at 317–18.

tions. A vendor could do so by mailing paper catalogs, by purchasing television advertising time, or by placing an advertisement in newspapers. All of these methods cost money. Today, it costs no more to advertise in fifty states than it costs to advertise in one; the entire Internet-accessed population of the United States (and the world) can be reached by one website.

Although the Court in *Bellas Hess* and *Quill* was reluctant to place burdens on companies that received little benefit from the states in which they made sales, today that burden is minimal due to the sophistication of computer programs that can determine, calculate, and remit taxes, and whose corporate owners benefit from the wonderful ability to reach the entire United States population through one website. Moreover, Internet commerce is limiting state tax revenue in two ways: by reducing the number of taxable sales and by contributing to the death of local business.[113] Does the removal of cost and spatial constraints change the legal nature of the transaction? No, a bricks-and-mortar sale of goods is no more or less a sale of goods than an Internet sale. The removal of these constraints, however, has made physical presence irrelevant to both buyers and sellers. As a result, buyers may be just as likely to order a book from Amazon as they are to drive a mile to the nearest Barnes & Noble. This irrelevance inures to the great benefit of online vendors, rendering the burden of tax compliance less onerous.

There is much commentary to the effect that online sales hurt local bricks-and-mortar stores.[114] There has also been counter commentary to the effect that the suspension of the sales tax on Internet sales is needed to foster the fledgling industry of e-commerce.[115] These are issues that no state can resolve on its own. Neither do they require an international solution. But a national solution addressing all problems can only be handled by Congress. Alas, Congress has failed to address the issue (surprising no one).

---

113 *See* Liptak, *supra* note 101 ("Brick-and-mortar companies often complain that they are put at a competitive disadvantage when they are required to collect sales taxes and online companies are not.").

114 *See* Kathleen McHugh & Oren Teicher, *Yes, Small Business Wants Online Giants to Collect Sales Tax*, BLOOMBERG BUS. WK., Nov. 22, 2013, http://www.businessweek.com/articles/2013-11-22/yes-small-business-wants-online-giants-to-collect-sales-tax; *see also* Liptak, *supra* note 101 (noting bricks-and-mortar companies' objections to the tax-exempt status of online companies).

115 *See, e.g.*, Charles E. McLure, Jr., *Thinking Straight About the Taxation of Electronic Commerce: Tax Principles, Compliance Problems, and Nexus*, 16 TAX POL'Y & ECON. 115, 124 (2002) ("One line of reasoning might be characterized as an 'infant industry' argument: that e-commerce should experience a period of tax exemption in order to allow it to 'get on its feet.'"). Large Internet retailers like Amazon now often support taxes on Internet transactions as a way of entrenching their market power. *See* Tim Worstall, *Amazon's in Favour of the Online Sales Tax Bill Now*, FORBES (Oct. 26, 2013, 10:55 AM), http://www.forbes.com/sites/timworstall/2013/10/26/amazons-in-favour-of-the-online-sales-tax-bill-now/.

VI
Regulatory Jurisdiction

A. From Us to Them

It has been hornbook law, at least since the A*ramco* decision in 1991, that American statutory law is not to be applied extraterritorially unless Congress has made clear its intent that such be done.[116] That precept has been reinforced strongly in recent years, especially in the *Kiobel* case, where the Court refused to apply the Alien Tort Statute (ATS) extraterritorially.[117] *Kiobel* is of foremost importance because the ATS had been routinely applied by lower courts and because it involved human rights.

We know of no attempt by Congress to regulate the foreign effects of electronic transactions. *Aramco* and *Kiobel* make clear, however, that Congress will have to provide in no uncertain terms for such a law to have extraterritorial effect. They also make clear that normal choice-of-law rules will apply to all transactions.

That in turn raises the question of so-called "f-cubed" litigation, where a foreign plaintiff sues a foreign defendant in a U.S. court over matters that happened in a foreign country. (Get it? Foreign, foreign, foreign.) The Supreme Court will hear argument this Term in two cases raising those issues.[118] If the Court should restrict the extraterritorial reach of American courts in such situations, it will help to reinforce the lesson from *Kiobel* and *Morrison* that the courts of this country follow Justice Story's dictum—that "[n]o nation has ever yet pretended to be the custos morum of the whole world."[119] That is particularly important in the world of online transactions, given the possibility that the universality of the e-commerce world will permit the exercise of personal jurisdiction over many matters that have no "real" basis for being heard in an American court. If we are correct in that prediction, then the Supreme Court will have stepped back from its apparent ability to assert jurisdiction over most of the cyber world.[120] In other words, although the cyber world permits widespread assertions of jurisdiction under traditional notions of long-arm jurisdiction, we believe that it is likely that the Court will step back and say that it has no business here.

---

116 EEOC v. Arabian Am. Oil Co. (Aramco), 499 U.S. 244, 248 (1991).

117 Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659, 1664 (2013).

118 Those cases are *Daimler AG v. Bauman*, 134 S. Ct. 746 (2014), and *Firoe v. Walden*, 688 F.3d 558 (9th Cir. 2012), *rev'd*, 134 S. Ct. 1115 (2014).

119 United States v. La Jeune Eugenie, 26 F. Cas. 832, 847 (C.C.D. Mass. 1822). Or, as the Court of Appeals of New York wrote in *Neumeier v. Kuehner*, 31 N.Y.2d. 121, 130 (1972), "Was the New York rule really intended to be manna for the entire world?"

120 This is not the place to venture into choice of law in detail. But the Supreme Court has exercised very little control over state choice-of-law decisions, be they on or offline.

Finally, we get to international assertions of jurisdiction by American courts. Although the recent trend has been to limit the broad reach of American personal jurisdiction—both long-arm and general,[121] that jurisdiction may be exercised so as to limit overbroad judgments of a foreign court. In *Yahoo! Inc. v. La Ligue Contre Le Racisme et l'Antisemitisme*, the court was faced with a French judicial decision that forbade Yahoo! from publishing ads for Nazi memorabilia.[122] Those ads were illegal in France but not in the United States. The decision was to be enforced by potentially ruinous fines.

Yahoo! then filed suit in federal court—seeking a declaratory judgment that the orders of the French court could not be enforced in an American court because it could not comply fully with those orders, due to technical problems. The District Court granted the injunction, but a badly divided Ninth Circuit, sitting en banc, held that the case should be dismissed.[123] There was not a majority for any reason behind the dismissal—three of the judges found that personal jurisdiction over the defendant was lacking, and three more—constituting a bare majority—believed the case was not yet ripe for adjudication. The division on the Ninth Circuit illustrates the immense difficulty of resolving a close-to-intractable problem, a problem made all the more acute due to the immense importance the French (and other European) governments place on restricting racist propaganda.

The problem *Yahoo!* raises is a perplexing one indeed: How can an American company determine whether it is complying with an order of a foreign court to refrain from acting in that country in a certain way? There is no easy answer to this quandary. The ideal solution would be an international agreement, but the contours of that agreement do not leap readily to mind.

B. From Them to Us

The *Yahoo!* litigation also raises the reverse question: Can a foreign country regulate the American electronic world?[124] The answer, of course, is that the foreign country can *try* to do so, but can it enforce its orders here? As we discussed earlier, American courts have been reluctant to enforce foreign libel judgments.[125] The reason is

---

121 *See* Linda S. Mullenix, Personal Jurisdiction Stops Here: Cabining the Extraterritorial Reach of American Courts, Public Law and Legal Theory Research Paper Series No. 530, at 12, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2348233.

122 433 F.3d 1199 (9th Cir. 2006) (per curiam) (en banc).

123 *Id.* at 1224.

124 We have already touched on this question in our discussion of the *Gutnick* litigation. *See supra* notes 74–79 and accompanying text.

125 *See supra* notes 75–77.

that most of those judgments do not provide enough procedural safeguards for First Amendment rights. In other words, American courts will assert control over problems that involve significant American interests—here, free speech—and deny recognition if those rights are not sufficiently protected.

A much more likely form of regulation by external authorities, however, involves the substance of an ordinary commercial transaction. Here, our courts are more likely to take a hands-off approach and defer to the regulatory regime of other jurisdictions. The European community has long been a leader here. In 2008, the EU adopted comprehensive regulations concerning consumer contracts, regulations which are much more protective of consumers than most similar American rules.[126] By adopting choice-of-law rules that implement substantive consumer protections that protect both paper and electronic transactions, the European Union has assumed control of all consumer transactions in the EU, regardless of what form they assume. In this respect, the EU tracks the United States: no special rules are needed for online transactions; rather, the traditional rules (here legislative) protect all consumers.[127]

Conclusion

This symposium focuses on neo-territorialism in various aspects of American law. Our journey through the law that has been applied to cyber transactions makes quite clear that neither the Supreme Court nor other U.S. courts have been particularly territorial in their approach to electronic transactions. Rather, our courts have focused on what they know and do best—drawing analogies to well-known existing law. Judges have not treated cyber problems as *sui generis*, a view that has led them away from expressions of Internet "exceptionalism." Nor have Congress or state legislatures become especially territorial in their approach to the law.[128]

That does not mean that there are no issues involving electronic transactions that need to be resolved. We have discussed revenge porn and consumer privacy as areas where many believe action is needed. Action in either area should take the form of uniform na-

---

126 *See* Council Regulation 593/2008, On the Law Applicable to Contractual Obligations, art. 6, 2008 O.J. (L 177) (specifying that the choice of law in a consumer contract dispute in the EU will be the law of the country in which the consumer resides).

127 There is a big difference, of course, in the fact that consumer transactions in the EU are subject to substantive protections; and here they are not protected nearly as well.

128 That the old laws work even in a modern age is vividly demonstrated in Professor Louise Weinberg's Essay in this symposium where she shows how the application of traditional jurisdictional rules would have reached more just results in very recent human rights litigation. *See* Louise Weinberg, *What We Don't Talk About When We Talk About Extraterritoriality:* Kiobel *and the Conflict of Laws*, 99 Cornell. L. Rev. 1471 (2014).

tional rules; that there has been no legislation suggests that no consensus sufficient to spur that action has been developed. We are comfortable with that result.