2020

Conflicts of Law and Transnational Data Flows

Paul S. Berman

10

Conflicts of Law and the Challenge of Transnational Data Flows*

PAUL SCHIFF BERMAN

A INTRODUCTION

Phillip Jessup's *Transnational Law*,[1] though generally phrased in the reassuring tones of a treatise, presented a bold vision for law in the twentieth century and beyond. In his very first paragraph, Jessup asserted the existence of a "complex interrelated world community" and a set of legal problems that involve more than just state-to-state relations.[2] Thus, his vision was both cosmopolitan and pluralist from the get-go, recognizing that human community affiliations cut across traditional territorial lines and that states are not the only relevant actors on the world stage of law. Jessup then spent the remainder of the book identifying both conflict-of-law principles and possible alternative legal and political forums where what he called transnational law was being made.

In this chapter, I wish to update Jessup's vision for the twenty-first century. Jessup correctly observed sixty years ago that multinational corporate activity created new challenges for nation states and their territorially based rules for jurisdiction, choice of law, and recognition of judgments. Those challenges are exponentially more difficult in the twenty-first century because electronic data – everything from emails and text messages to Facebook and Instagram posts to Twitter pronouncements to drone warfare data to search algorithms to financial transactions to cloud data storage – travels around the globe with

* Special thanks to Samuel Wenzel for helpful research assistance in the preparation of this chapter. Some material in this chapter is derived from Paul Schiff Berman, Global Legal Pluralism: A Jurisprudence of Law beyond Borders (2012) and Paul Schiff Berman, *Legal Jurisdiction and the Deterritorialization of Social Life*, *in* Research Handbook on the Law of Virtual and Augmented Reality (Woodrow Barfield et al. eds., 2019).

[1] Phillip Jessup, Transnational Law (1956).

[2] *Id.* at 1.

little relationship to physical territory. In addition, this data is often in the custody and control of data intermediaries such as Google, Facebook, Twitter, Apple, Microsoft, Amazon, private military contractors, and so on.

Three important consequences flow from this ubiquitous technology-enabled, data-driven global societal activity. First, the territorial location of data becomes increasingly arbitrary and substantively unimportant. If I, as a US citizen based in Maryland, have a Gmail account and Google, a US corporation, decides to store my archived emails in Ireland or France or Indonesia (or indeed to split up the data fragments that make up each email message among data warehouses in all three countries), that decision seems irrelevant to any question of whether I have somehow affiliated myself with any of those communities or governments for purposes of jurisdictional or choice-of-law analysis. Second, because of this deterritorialization of data, it will often be the case that territorially based courts (or law enforcement authorities generally) are unable to easily enforce their decisions because those decisions require cooperation from relevant actors in far-flung communities. Third, as a direct result of the first two problems, governmental and judicial authorities are increasingly turning to multinational corporate data intermediaries to carry out and enforce their orders because only those companies have sufficient global reach to make legal rulings effective. But deputizing these intermediaries to become enforcement agents, while logical and possibly effective, raises new problems regarding the scope of governmental authority and the distortions involved in privatizing law enforcement.

These are the sorts of concerns that surely would have occupied Phillip Jessup were he still alive today. Interestingly, even though scholars first began raising these issues at the dawn of the commercial internet era as far back as 1995, the jurisprudential solutions we see so far are still largely unsatisfying, both conceptually and practically. Indeed, as with many conflicts-of-law problems that have bedeviled courts and commentators for hundreds of years, there *may not be* a fully satisfactory solution. Moreover, even if there were a single unifying theory for conflicts of law in the information age, it's not at all clear that everyone would agree on what that theory should be. Thus, as legal pluralist scholars have long realized, there is never a stable "solution" to the reality of legal pluralism. Instead, legal pluralism is an inevitable (and perhaps not even an undesirable) result of a world with multiple communities and multiple legal and quasi-legal systems.

Yet, even if there is no single unifying theory that could put an end to legal conflicts, we can still survey the types of cases that are arising and analyze the efforts of courts and others to navigate the problems that arise from the deterritorialization of information. This chapter aims to do that, providing a

series of real-life case studies that any consideration of twenty-first-century conflicts of law (and transnational law) must face.

What is perhaps most striking about all of these cases, taken together, is that we see in the legal decisions very little serious engagement with the doctrines, principles, values, and policies that historically underlie the conflicts-of-law doctrines of jurisdiction, choice of law, or recognition of judgments. Instead, courts simply tend to assume that because something is arguably located within a territorial boundary, that is enough to assert jurisdiction or apply local law. Or they assume that because local application of a legal regime is appropriate, worldwide application of that same regime is also appropriate. Or they assume that in recognizing a foreign judgment, local public policies automatically apply and trump any other concerns. And even in the rare case of a court refraining from applying its local law, such a decision not to apply norms extraterritorially may still be based on an arbitrary territorial localization, not on a sustained grappling with the core values underlying conflicts-of-law doctrines.

But conflicts-of-law doctrines are not just mechanical rules based on territorial location or raw power. They implicate fundamental questions about community affiliation, membership, and effects, as well as governmental sovereignty, relative authority, and cosmopolitan cooperation. The conundrums raised by the deterritorialization of data and the rise of data intermediaries afford a useful opportunity to ask these fundamental questions and begin to forge new conceptions of conflicts of law for the new information age that is already transforming our world.

B INTERNET CONFLICTS-OF-LAW CASES: 2000–03

1 *LICRA v. Yahoo!*

It is perhaps fitting that the most famous legal dispute of the early internet era implicated all three conflicts doctrines: jurisdiction, choice of law, and judgment recognition. On May 22, 2000, the Tribunal de Grande Instance de Paris issued a preliminary injunction against Yahoo.com, ordering the site to take all possible measures to dissuade and prevent access in France to Yahoo! auction sites that sell Nazi memorabilia or other items that are sympathetic to Nazism or constitute Holocaust denial.[3] Undisputedly, selling such

[3] UEJF & LICRA v. Yahoo!, Inc. & Yahoo France, Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, May 22, 2000, 00/05308, https://perma.cc/738B-V9BM.

merchandise in France would violate French law,[4] and there would be no jurisdictional dispute had the French authorities limited their prosecution to the French end users who were downloading the illegal materials from Yahoo!'s auction sites. But even in this early internet era, legal authorities were already realizing that it is often far more effective to proceed against an intermediary such as Yahoo!, both because the intermediary is usually a larger corporate actor and therefore easier to find and because one legal action can address a broader problem rather than requiring separate enforcement actions against each end user. In effect, the intermediary becomes the enforcement agent of whatever legal authority issues the order.

In this case, the intermediary question had two parts, however. Certainly the French court had undisputed jurisdictional authority over Yahoo.fr, Yahoo!'s French subsidiary, and Yahoo.fr complied with requests that access to such sites be blocked.[5] What made this action noteworthy was that the suit was brought not only against Yahoo.fr but against Yahoo.com, an American corporation, and the court sought to enjoin access to non-French websites stored on Yahoo.com's non-French servers.

Of course, one can easily see why the court and the complainants in this action would have taken this additional step. Shutting down access to web pages on Yahoo.fr does no good at all if French citizens can, by entering a slightly different URL in their search box, simply go to Yahoo.com and access those same pages. On the other hand, Yahoo! argued that the French assertion of jurisdiction was impermissibly extraterritorial in scope.[6] According to Yahoo!, in order to comply with the injunction, it would need to remove the pages from its servers altogether (not just for the French audience), thereby denying such material to non-French citizens, many of whom have the right to access the materials under the laws of their countries.[7] Most importantly, Yahoo! argued that such extraterritorial censoring of American web content would run afoul of the First Amendment of the US

[4] *See* Code Pénal [C. Pén] [Penal Code] art. R.645-1 (Fr.) (prohibiting the public display of Nazi memorabilia except for the purposes of a historical film, show, or exhibit), https://perma.cc/BL8T-4J3A.

[5] *See* LICRA & UEJF v. Yahoo!, Inc. & Yahoo France, TGI Paris, Nov. 20, 2000, 00/05308 (noting that Yahoo! France had posted warnings on its site that the user could access revisionist sites through Yahoo! U.S. and that the visiting of such sites is prohibited and punishable by French law), https://perma.cc/ALK9-XM6A.

[6] *Id.*

[7] *Id.*

Constitution.[8] Thus, Yahoo! and others[9] contended that the French assertion of jurisdiction was an impermissible attempt by France to impose global rules for internet expression. As Greg Wrenn, associate general counsel for Yahoo!'s international division, put it at the time, "We are not going to acquiesce in the notion that foreign countries have unlimited jurisdiction to regulate the content of U.S.-based sites."[10]

Yet, it is easy to see that the extraterritoriality charge runs in both directions. If France is *not* able to block the access of French citizens to proscribed material, then the United States will effectively be imposing First Amendment norms on the entire world. And though geographical tracking software might seem to solve the problem by allowing websites to offer different content to different users, such a solution would still require the sites to analyze the laws of all jurisdictions to determine what material to filter for which users.

The arguments in the *Yahoo!* case therefore establish the basic dichotomy that we then see repeated in case after case subsequently. On the one hand, legal authorities wish to assert jurisdiction anywhere a community is affected by web-based content. This tends to push in the direction of universal jurisdiction because content uploaded anywhere in the world can potentially cause harmful effects anywhere else in the world. In response, defendants argue for jurisdiction only where content is uploaded or only where their servers are located or only in their home jurisdiction. This theory of jurisdiction tends to result either in arbitrary or easily manipulable jurisdictional principles (such as where a server is located) or a system where actors impacting communities across the globe can only be sued or regulated in their home jurisdiction. Both of these solutions seem unsatisfying. And finding some other non-web-based territorial nexus to bolster an assertion of jurisdiction can also be problematic. For example, regardless of how one resolves the jurisdictional question in the Yahoo! case, it seems clear that where in the world the actual paper share certificate by which Yahoo! owned Yahoo.fr seems irrelevant to the underlying jurisdictional issues at stake.

In the end, rather than filter out French users, Yahoo! chose a two-pronged strategy. First, it decided to remove the auction sites from its servers altogether,

[8] *Id.*

[9] *See, e.g.*, Carl S. Kaplan, *Experts See Online Speech Case as Bellwether*, N.Y. TIMES (Jan. 5, 2001), http://www.nytimes.com/2001/01/05/technology/05CYBERLAW.html (quoting the warning of Barry Steinhardt, associate director of the American Civil Liberties Union, that if "litigants and governments in other countries . . . go after American service providers . . . we could easily wind up with a lowest common denominator standard for protected speech on the Net").

[10] *Id.*

but it claimed that such a decision was "voluntary" and unrelated to the French court ruling.[11] Second, it filed suit in US District Court in the Northern District of California, seeking a declaratory judgment that the French court's orders were not enforceable in the United States pursuant to the First Amendment.[12] Accordingly, what had started as a jurisdictional dispute was transformed into its flip side: a question of recognition of judgments.

Faced with the question of whether or not to enforce the French court's order, the district court started from the assumption that US law (and US constitutional norms) must apply. Thus, the court framed the issue for decision solely in US constitutional terms: "What is at issue here is whether it is consistent with the Constitution and laws of the United States for another nation to regulate speech by a United States resident within the United States on the basis that such speech can be accessed by Internet users in that nation."[13]

Conceptualized in this way, the district court had little difficulty determining that enforcement of the French court order would violate the First Amendment, concluding both that the French judgment constituted impermissible viewpoint discrimination and that it was unconstitutionally vague. The court therefore concluded that a US court could not have issued such an order in the first instance without violating constitutional free speech norms.[14] But of course, in a judgment recognition case, that is not the appropriate inquiry. Indeed, in the domestic context, the Full Faith and Credit Clause *requires* recognition of judgments that might be completely unavailable or even potentially illegal in the state where recognition is sought.[15] Thus, the

[11] *See* Press Release, Yahoo!, Yahoo! Enhances Commerce Sites for Higher Quality Online Experience (Jan. 2, 2001), https://perma.cc/H9RS-QGTN (announcing new product guidelines for its auction sites that prohibit "items that are associated with groups which promote or glorify hatred and violence"). *But cf.* Troy Wolverton & Jeff Pelline, *Yahoo to Charge Auction Fees, Ban Hate Materials*, CNET (Jan. 2, 2001), https://perma.cc/LGE4-RDMX (noting that Yahoo!'s new policy regarding hate-related materials followed action by the French court).

[12] Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisémitisme, 169 F. Supp. 2d 1181, 1186 (N.D. Cal. 2001), *rev'd on other grounds*, 433 F.3d 1199 (9th Cir. 2006) (en banc).

[13] *Id.* at 1186 (emphasis omitted).

[14] *Id.* at 1189–90, 1192–93.

[15] *See, e.g.*, Estin v. Estin, 334 U.S. 541, 546 (1948) (finding that the Full Faith and Credit Clause "ordered submission . . . even to hostile policies reflected in the judgment of another State, because the practical operation of the federal system, which the Constitution designed, demanded it"); Milwaukee County v. M.E. White Co., 296 U.S. 268, 277 (1935) ("In numerous cases this Court has held that credit must be given to the judgment of another state, although the forum would not be required to entertain the suit on which the judgment was founded . . . ."); Fauntleroy v. Lum, 210 U.S. 230, 237 (1908) (holding that the judgment of a

real question is whether this is the type of judgment that should be *recognized*, not whether the court could have issued the ruling *as an original matter*.

To its credit, the district court did include a brief discussion of the judgment recognition issue in a section titled "Comity."[16] And the court acknowledged that "United States courts generally recognize foreign judgments and decrees unless enforcement would be prejudicial or contrary to the country's interests."[17] Yet, after reiterating that the French judgment "clearly would be inconsistent with the First Amendment if mandated by a court in the United States,"[18] the district court judge concluded that because the foreign order would unconstitutionally chill speech occurring within US borders, "the principle of comity is outweighed by the Court's obligation to uphold the First Amendment."[19]

Thus, while ostensibly addressing principles of judgment recognition, the court ultimately returned to the idea that if a judgment would be unconstitutional if issued in the United States, enforcing that judgment also would be unconstitutional, or at least sufficiently contrary to state interests as to overwhelm any principles of comity. By eliding the difference between *issuing* a judgment and *enforcing* a judgment, however, the court neglected to apply in more detail the various principles of judgment recognition or to consider more carefully those circumstances in which US interests might *not* truly be threatened by the application of a foreign norm.

An en banc panel of the Ninth Circuit ultimately reversed, on other grounds, by a six-to-five vote.[20] Three judges in the majority determined that the District Court did not have personal jurisdiction over the French defendants until those defendants actually came to the United States seeking to enforce the French judgment. The other three judges making up the majority also dismissed, but they did so on ripeness grounds, similarly concluding that the enforcement issue should not be decided until the French defendants actually sought enforcement. Thus, the Court of Appeals majority never addressed the judgment recognition issues upon which the district court had relied.

Missouri court was entitled to full faith and credit in Mississippi even if the Missouri judgment rested on a misapprehension of Mississippi law).

[16] *Yahoo!*, 169 F. Supp. 2d at 1192–93.

[17] *Id.* at 1192.

[18] *Id.*

[19] *Id.* at 1193.

[20] *Yahoo!*, 433 F.3d 1199 (9th Cir. 2006) (en banc).

II *GlobalSantaFe Corp.* v. *Globalsantafe.com*

Transnational data flows also impact choice of law. For example, historically, the boundaries of trademark law have been delineated in part by reference to physical geography.[21] Thus, if I own a store in New York City called Berman's, I will not, as a general matter, be able to prevent a person in Australia from opening a store that is also called Berman's, even if I have previously established a trademark in my name. The idea is that customers would be unlikely to confuse the two stores because they are in markets that are spatially distinct.[22] In the online world, such clear spatial boundaries are collapsed because, as the domain name system is currently organized, there can be only one bermans.com domain name, and it can only point to one "location."[23]

In the early to mid-1990s, as corporations and entrepreneurs began to understand the potential value of a recognizable domain name, pressure increased to create trademark rights in such names. In response, Congress first passed the Federal Trademark Dilution Act[24] and then the Anticybersquatting Consumer Protection Act (ACPA), which provides an explicit federal remedy to combat so-called cybersquatting.[25] According to the congressional reports, the ACPA is meant to address cases where non–trademark holders

[21] *See* Graeme B. Dinwoodie, *Trademarks and Territory: Detaching Trademark Law from the Nation-State*, 41 HOUS. L. REV. 885, 887 (2004) ("[I]t is an axiomatic principle of domestic and international trademark law that trademarks and trademark law are territorial.").

[22] *See* Stone Creek, Inc. v. Omnia Italian Design, Inc., 875 F.3d 426, 438 (9th Cir. 2017), *petition for cert. filed* ("[W]here two parties independently are employing the same mark upon goods of the same class, but in separate markets wholly remote the one from the other, the question of prior appropriation is legally insignificant . . . [except in cases of bad faith].") (quoting Hanover Milling Co. v. Metcalf, 240 U.S. 403, 415 (1916)). This is not an absolute rule, of course, because "famous or well-known marks may well leap oceans and rivers, cross national borders, and span language barriers to achieve international recognition." Dan L. Burk, *Trademark Doctrines for Global Electronic Commerce*, 49 S. C. L. REV. 695, 720 (1998). *See also* Vaudable v. Montmartre, Inc., 193 N.Y.S.2d 332, 332 (N.Y. Sup. Ct. 1959) (enjoining the use by a restaurant in New York of the name and decor of Maxim's Restaurant in Paris). Nevertheless, the likelihood-of-confusion standard historically has tended to imbed a geographical limitation.

[23] Of course, users going to www.bermans.com could be shown an introductory screen that provides a choice of which Berman's site they wish to access.

[24] Federal Trademark Dilution Act of 1995, Pub. L. No. 104-98, 109 Stat. 985 (codified at 15 U.S.C. §§ 1125, 1127 (Supp. 1996)).

[25] Anticybersquatting Consumer Protection Act, Pub. L. No. 106-113, § 3002, 113 Stat. 1501A-545 (1999) (codified at 15 U.S.C. § 1125(d) (2000)); *see* H.R. REP. NO. 106-412 (1999) (detailing the act).

register well-known trademarks as domain names and then try to "ransom" the names back to the trademark owners.[26]

This application of trademark law to domain names means that trademark law has become unmoored from physical geography and is now more likely to operate extraterritorially. Potentially, even those who are legitimately using a website that happens to bear the name of a famous mark held by an entity across the globe could be forced to relinquish the name. In addition, this unmooring of trademarks from territory creates the possibility that individual countries will interpret their trademark laws expansively, thereby reducing trademark rights "to their most destructive form": the mutual ability to block (or at least interfere with) the online use of marks recognized in other countries. Moreover, each of the parties claiming ownership in a trademark could sue in a different country, and because of differences in substantive law, each party could win.[27]

This is the backdrop for *GlobalSantaFe Corp. v. Globalsantafe.com*.[28] On September 3, 2001, Global Marine Inc. and Santa Fe International Corp. announced their agreement to merge into an entity to be known as Global-SantaFe Corp. Less than a day later, Jongsun Park, a citizen of South Korea, registered the domain name globalsantafe.com with the Korean domain name registrar Hangang. In response, Global Marine and Santa Fe filed an in rem action in the Eastern District of Virginia under the ACPA. The ACPA provides in rem jurisdiction over a domain name wherever that name is registered.[29] Thus, for example, if people register domain names online via a website owned by Network Solutions, a domain name registrar[30] corporation located in Virginia, they potentially can be forced, under the ACPA, to defend a trademark action in Virginia whether or not they have ever set foot in Virginia or knew Network Solutions was a Virginia corporation.

[26] *See* H.R. Rep. No. 106-412, at 5–7 (1999) (noting that "[s]ometimes these pirates put pornographic materials on theses sights [*sic*] in an effort to increase the likelihood of collecting ransom by damaging the integrity of a [trade]mark"); S. Rep. No. 106–140, at 4–7 (1999) (highlighting testimony regarding attempts to ransom domain names to the highest bidder).

[27] *See, e.g.*, Mecklermedia Corp. v. D.C. Cong. GmbH, 1998 Ch. 40, 53 (Eng.) (noting that the cause of action for using trademarked language is different in Germany and England and, thus, simultaneous proceedings could continue).

[28] GlobalSantaFe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610 (E.D. Va. 2003).

[29] 15 U.S.C. § 1125(d)(2)(C) (2000) ("In an *in rem* action . . . a domain name shall be deemed to have its situs in the judicial district in which . . . the domain name registrar, registry, or other domain name authority that registered or assigned the domain name is located . . .").

[30] A registrar is one of several entities for a given top-level domain (such as .com, .edu, .gov, .uk, etc.) that is authorized by the Internet Corporation for Assigned Names and Numbers to grant registration of domain names. David Bender, Computer Law § 3D.05[3], at 3D-104 (2002).

In this case, however, jurisdiction was further complicated by the fact that Park had not even registered the domain name with a US registrar but with a South Korean one. Nevertheless, the ACPA also authorizes in rem jurisdiction in the judicial district where the overall domain name *registry* is located.[31] Based on this provision, the district court determined that it could exercise jurisdiction because VeriSign, which administers the entire ".com" registry, is located in Virginia.[32] And having determined that the substantive provisions of the ACPA had been met, the court therefore ordered both Hangang and VeriSign to "take all appropriate steps to transfer the domain name" to GlobalSantaFe.[33]

Approximately a week later, Park filed an application for an injunction in the District Court of Seoul, South Korea, seeking an order preventing Hangang from transferring the domain name.[34] Ruling that the Virginia court did not have proper jurisdiction, the Korean court provisionally granted the injunction, and Hangang, presumably responding to the Korean court's injunction, subsequently refused to transfer the domain name.[35] In an effort to resolve this transnational stalemate, GlobalSantaFe returned to the court in Virginia seeking an additional order directing VeriSign to cancel the infringing domain name from the ".com" registry.[36]

The district court reaffirmed that it had proper in rem jurisdiction over the case pursuant to the ACPA because VeriSign is located in Virginia.[37] The court also reiterated that Park had violated the substantive provisions of the ACPA.[38] And after a lengthy discussion of the mechanics concerning how a registry company would effectively cancel or transfer a domain name,[39] the court concluded that such a remedy was both available under the ACPA and appropriate given the unwillingness of Hangang to act in violation of the Korean court's order.[40]

[31] For each top-level domain (such as ".com," ".gov," ".edu," ".uk," etc.), a single registry company is responsible for keeping the records and a directory of all the domain names within that domain. When an individual or corporation company wants the rights to a new domain name, it contacts a registrar. The registrar submits the domain name to the registry, which enters the assigned domain name into a database. At the time, VeriSign Global Registry Services was the sole registry for ".com" domain names.

[32] *GlobalSantaFe*, 250 F. Supp. 2d at 614–15.

[33] *Id.* at 614.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.* at 614–15.

[38] *Id.* at 615–16.

[39] *Id.* at 617–24.

[40] *Id.* at 623.

From a conflicts perspective, what is most striking about the decision is that the court focuses almost exclusively on its jurisdiction to hear the case but never questions that the ACPA is the only possibly relevant legal regime. Indeed, the court seems to assume that the ACPA's legal reach is limited solely by the scope of the court's jurisdiction, not by any choice-of-law considerations. Thus, in the court's view, the only significant gap in the ACPA's trademark enforcement regime is for domain names registered under top-level domains whose registry is located outside the United States. Never does it seem to occur to the court that even if it had jurisdiction over the action, it might nevertheless choose South Korean (or some other) law as providing the operative legal norms for resolving the dispute.

This single-minded focus on jurisdiction (and therefore the physical location of registry companies) poses potential problems for ACPA enforcement in the future. As the court recognizes, if jurisdiction is all, then the ACPA can only provide a broad-based remedy in domain name trademark cases so long as the registries of the most popular top-level domains remain in the United States.[41] Thus, if the registries for generic domains such as ".com" and ".net" were relocated outside the physical territory of the United States, then US trademark rights in domain names would face serious enforcement challenges.

Such difficulties are a natural consequence of laws that are deemed to apply to the full extent of their territorially based jurisdictional reach. But, of course, as choice-of-law scholars have long recognized, laws need *not* be applied to the full extent of their jurisdictional reach, and concerns about the establishment of competing or conflicting trademark systems on the internet are precisely the sorts of concerns that might animate a more restrained application of forum law.

In any event, having concluded that the case was within its jurisdiction and that, therefore, US law necessarily applied, the court only at the very end of its opinion asked whether "concerns of international comity" might dictate deference to the injunction issued by the Korean court.[42] Even here, however, the court did not ask about the *content* of South Korean trademark law; it only asked whether deference was owed to the court decision granting the actual injunction.[43] Having framed the issue in this way, the court resolved it by reference to a principle that in rem cases should generally be decided by the

[41] *Id.*
[42] *Id.* at 624.
[43] *Id.*

first court to exercise jurisdiction over the property in question.[44] And since the original Virginia court order preceded the Korean court injunction, the Virginia court found deference inappropriate.[45]

The vision of choice of law that emerges from the decision, therefore, is founded solely on jurisdictional power and a race to the courthouse. A state can enact legal norms with extremely broad extraterritorial reach, and courts within that state are bound to apply those norms to a multinational dispute so long as the case was commenced there first. Needless to say, this is not a particularly thoughtful or nuanced choice-of-law regime,[46] nor does it take into account the possible long-term benefits that might accrue from adopting a more restrained application of forum law or from considering the forum's own interest in harmonious international adjudicatory processes.

III *Barcelona.com, Inc.* v. *Excelentisimo Ayuntamiento de Barcelona*

Whereas the choice-of-law issues in *GlobalSantaFe* were made more complicated by the fact that the parties were from different countries, in *Barcelona.com*, all of the principal actors in the dispute were from Spain.[47] Yet even here the Fourth Circuit, reversing a contrary ruling of the district court,[48] eschewed Spanish law and insisted on applying the ACPA.[49] Moreover, this decision was again reached without significant consideration of choice-of-law issues.

The case involved the right to the domain name barcelona.com. In 1996, Mr. Joan Nogueras Cobo ("Nogueras"), a Spanish citizen, registered barcelona.com with the Virginia-based domain name registrar Network Solutions.[50]

[44] *See id.* at 624–26 (referring to the first-in-time rule known as the *Princess Lida* doctrine.)

[45] *Id.* at 625.

[46] It should be noted that this first-in-time principal, also known as *lis pendens*, is used in many civil law jurisdictions around the world.

[47] Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona, 330 F.3d 617 (4th Cir. 2003).

[48] Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona, 189 F. Supp. 2d 367 (E.D. Va. 2002), *rev'd* 330 F.3d 617 (4th Cir. 2003).

[49] *Barcelona.com*, 330 F.3d at 630. To be sure, because the claim at issue sought only a declaratory judgment as to the plaintiff's rights under the Lanham Act, it is possible to construe the Fourth Circuit decision as merely clarifying US law without requiring that this law be the ultimate rule of decision in the case. However, nowhere does the court state that it is rendering such a limited ruling and instead explicitly reverses the district court's application of Spanish law and remands so that the district court can "grant the appropriate relief under [the Lanham Act]." *Id.* at 630. In addition, the appellate opinion states that the ACPA can be used specifically to reverse arbitration decisions "grounded on principles foreign or hostile to American law." *Id.* at 626. Both of these statements strongly imply that the Fourth Circuit considered its application of US law to be dispositive.

[50] *Id.* at 620.

Subsequently, Nogueras formed a corporation under US law, called Bcom, Inc.[51] Despite the US incorporation, however, the company had no offices, employees, or even a telephone listing in the United States.[52] Nogueras (and the Bcom servers) remained in Spain.[53]

The Barcelona City Council asserted that Nogueras had no right to use barcelona.com under Spanish trademark law and demanded that he transfer the domain name registration to the city council.[54] When Nogueras refused, the city council filed a complaint with the World Intellectual Property Organization (WIPO).[55] Several months later, the WIPO panelist ruled in favor of the city council.[56] Instead of transferring the domain name, however, Bcom filed suit in federal court, again in Virginia, seeking a declaratory judgment that the registration of barcelona.com was not unlawful.[57]

Having decided that the WIPO administrative proceedings would be given "no weight,"[58] the district court then turned to the elements of the ACPA, first considering whether either party possessed a valid trademark for the name *Barcelona*. Significantly, the district court sought to answer this question by reference to *both* US and Spanish law.[59] And although the court concluded that neither party possessed a US trademark in the name *Barcelona*, it did find that the city council possessed multiple Spanish trademarks containing the term *Barcelona*, such as *Barcelona Teatre*, *Barcelona Canal*, and *Barcelona Television*.[60] The court also noted that under Spanish law, if a trademark consists of two or more words, the operative issue is which word creates the dominant impression in the mind of the consumer. Here, that word obviously would be *Barcelona*.[61] Finally, the court determined that under Spanish law, the names of communities, municipalities, and provinces cannot be registered as trademarks without authorization by municipal officials, and neither

[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.* at 621. Every domain name issued by Network Solutions is issued under a contract, the terms of which include a provision requiring resolution of disputes through the Uniform Domain Name Dispute Resolution Policy (UDRP) promulgated by the Internet Corporation for Assigned Names and Numbers. *Id.* The WIPO complaint was filed in accordance with the terms of the UDRP. *Id.*
[56] *Id.*
[57] *See id.*
[58] *See* Barcelona.com, 189 F. Supp. 2d at 371.
[59] *See id.* at 371–72.
[60] *See id.* at 371–72 & n.3.
[61] *See id.* at 372.

Nogueras and Bcom had received such authorization.[62] Thus, the court ruled that the city council possessed a "legally valid Spanish trademark" for the word *Barcelona*.[63] The district court then turned to the other elements of the ACPA, finding both likelihood of consumer confusion and the requisite bad-faith intent to profit from the domain name registration.[64] Accordingly, the district court ruled in favor of the city council and refused to issue the declaratory judgment Bcom had sought.[65]

The Fourth Circuit reversed.[66] Significantly, the major issue on which the appellate court disagreed with the trial court was the use of Spanish law to determine whether the city council had a valid trademark. Citing section 1114 (2)(D)(v) of the ACPA, the Fourth Circuit emphasized that the principal issue to be decided is whether "plaintiff's registration or use of the domain name is not unlawful *under the Lanham Act*."[67] According to the appellate panel, this language makes clear that only US law may be used to determine the existence of a valid trademark or its possible infringement.[68] Having decided to apply US trademark law, the court then concluded that *Barcelona* is "a purely descriptive geographical term entitled to no trademark protection" under the ACPA.[69] Accordingly, the court found nothing unlawful in Nogueras's registration of barcelona.com and therefore reversed the district court's ruling.[70]

Thus, the Fourth Circuit, like the court in *GlobalSantaFe Corp.*, applied US law to an international trademark dispute, invoking principles of territoriality. Indeed, despite the fact that the principal actors in the dispute were all in Spain, the appellate court opined that the ACPA, "by requiring application of United States trademark law to this action brought in a United States court by a United States corporation involving a domain name

[62] *See id.*
[63] *See id.*
[64] *See id.* at 372–73.
[65] *See id.* at 373. The court also ruled in favor of the city council on an ACPA counterclaim against Nogueras, finding that Nogueras had engaged in bad-faith intent to profit from the city council's valid trademark. *See id.* at 373–77.
[66] *Barcelona.com*, 330 F.3d 617 at 619–20.
[67] *Id.* at 626 (emphasis added).
[68] *See id.* at 627–28.
[69] *Id.* at 629.
[70] *Id.* The Fourth Circuit also vacated the district court's decision concerning the city council's counterclaim (without reaching the merits) because the appellate panel concluded that no counterclaim had actually been filed. *See id.*

administered by a United States registrar" was consistent with "the fundamental doctrine of territoriality upon which our trademark law is presently based."[71]

This doctrine of territoriality likely derives from the 1883 Paris Convention for the Protection of Industrial Property[72] (upon which the Fourth Circuit relied[73]). Indeed, the concern animating the convention was that absent a doctrine of territoriality, a country could create a "world mark" simply by granting a trademark under its local law and thereby prevent anyone anywhere in the world from using that name.[74] Such an extraterritorial encroachment was unacceptable in an era when it was presumed that trademarks could easily operate locally because the use of a trade name in one country would have no significant impact on the use of the same name by a different entity in another country.

When considering trademarks in domain names, however, a single-minded emphasis on territoriality may itself create law with substantial *extra*territorial effects. For example, by applying the ACPA in *GlobalSantaFe*, the US District Court necessarily imposed US trademark law on a South Korean domain name registrant and a South Korean domain name registrar, even though neither had any significant contact with the United States. Likewise, in *Barcelona.com*, the Fourth Circuit applied US trademark law to a dispute where all the principal actors were Spanish and where the issue concerned a domain name associated with the name of a major city in Spain. Both of these cases demonstrate that, by applying a rigid conception of territoriality to international trademark disputes (at least in the context of domain names), courts run the risk of imposing US law extraterritorially and creating precisely the sort of world mark that the principle of territoriality was originally designed to avoid.

Accordingly, we need to reconsider the traditional assumption that trademark disputes must always be resolved by applying the law of the forum country. Instead, cases involving international actors require courts to use choice-of-law principles in order to determine the appropriate legal norms. Moreover, such cases may help suggest choice-of-law frameworks that take

[71] *Id.* at 628.

[72] *See* Convention Revising the Paris Convention of March 20, 1883, as Revised, for the Protection of Industrial Property, July 14, 1967, art. 10bis, 21 U.S.T. 1583, 828 U.N.T.S. 305.

[73] *See Barcelona.com*, 330 F.3d at 628.

[74] *See, e.g.*, Tortsten Bettinger & Dorothee Thum, *Territorial Trademark Rights in the Global Village – International Jurisdiction, Choice of Law and Substantive Law for Trademark Disputes on the Internet (Part Two)*, 31 Int'l Rev. Intell. Prop. & Competition L. 285, 286 (2000) (explaining the basis of the doctrine of territoriality with regard to trademarks).

proper account of the actual community affiliations of the parties, as well as the interests nation states have in being a functioning part of an interlocking international network of domestic trademark regimes.

C INTERNET CONFLICTS-OF-LAW CASES: 2013–17

Lest we think that these three cases from the early years of the twenty-first century represent simply the growing pains associated with applying law to a new technology, it is worth considering the following group of cases. Although they each arose a decade or more later, the issues they raise will immediately be familiar based on the paradigm cases discussed so far.

Indeed, more and more of our social identity is now stored remotely by third parties, far from our physical location. Whether it be our emails, our social media posts, our musical preferences, our virtual world activities, our online search histories, or our banking and health data, very little of our data identity actually remains tied to our person anymore. This increasing deterritorialization of data and identity is resurfacing many of the same conundrums for jurisdiction, choice of law, and judgment recognition that were identified in the early days of the commercial internet.

1 *United States* v. *Microsoft*

In 2013 US officers conducting a criminal drug investigation sought a search warrant under federal law to seize the emails of a Microsoft customer. This is usually a relatively routine process, and as long as the search warrant is valid, then data storage companies such as Microsoft generally comply. And in fact Microsoft did turn over all account information it had that was being stored in the United States. However, in this case the actual emails and their contents were stored overseas in Dublin, Ireland. Microsoft refused to turn over this content, arguing that the federal law pursuant to which the search warrant was issued, the Stored Communications Act, could not be applied extraterritorially.

The US Court of Appeals for the Second Circuit agreed, albeit reluctantly.[75] Applying the presumption against extraterritoriality, the court determined that because Congress had not, in the Stored Communications Act,[76] contemplated cloud-based data storage, it had made no provision for warrants to apply beyond US borders. Significantly, the physical location or the

[75] Microsoft v. United States, 829 F.3d 197 (2d Cir. 2016).
[76] 18 U.S.C. §§ 2701–12 (2012).

nationality of the underlying *person* who was the subject of the investigation was irrelevant. Thus, as interpreted by the Second Circuit, the Stored Communications Act might not permit authorities to obtain a search warrant and seize email records of a US citizen located in the United States who sent emails to other US citizens from a computer located in the United States. The only relevant territorial nexus is where the email data happens to be stored. And significantly, this storage decision is entirely within the control of the storage provider, leaving open the possibility of manipulation in order to avoid the law of a particular sovereign.

In contrast, a district court in Pennsylvania subsequently ruled the opposite way on a similar warrant involving Google.[77] Here, the data question was in some ways even more difficult because Google does not store customers' data in one location, such as Ireland. Instead, Google uses an algorithm that divides an individual's user data across data centers and even splinters the data such that an email is not stored as a "cohesive digital file" but in "multiple data 'shards,'" each in a separate location around the world. Accordingly, even if US law enforcement sought the data through a government-to-government treaty, there would be no one government to whom to address the request.

Unlike the Second Circuit, the court in the *Google* case reasoned that if the Stored Communications Act is meant to protect Fourth Amendment privacy interests, then the relevant question is where the potential invasion of privacy takes place, not where the data is located. And given that Google can move customers' data at will around the globe, the court reasoned that forcing Google to reterritorialize the data in the United States does not violate any privacy interest. Then, once the data is repatriated, the warrant can issue just as it would in any other domestic situation.

In order to resolve this ambiguity, the US Congress in 2018 enacted the CLOUD Act.[78] Under this statute US data and communication companies must provide stored data for US citizens on any server they own and operate when requested by warrant, regardless of where in the world that data happens to be stored. Thus, the statute sensibly looks at the underlying community affiliation of the *user* rather than the arbitrary territorial location of the *data*. On the other hand, the act does provide mechanisms for the communications companies or the courts to challenge or reject warrants if they believe the request violates the privacy rights of the foreign country where the data is stored. This caveat still seems to unduly reify the physical location of data even

[77] *In re* Search Warrant No. 16-960-M-01 to Google, *In re* Search Warrant No. 16-1061-M to Google, 232 F. Supp. 3d 708 (E.D. Pa. 2017).
[78] CLOUD Act, H.R. 4943, 115th Cong. (2018).

though that physical location may be arbitrary and completely unrelated to the social reality of the person whose data is at issue.

II *Google Spain SL* v. *Agencia Española de Protección de Datos*

As with data, online searches are part of our social identity. And, as with data, searches are fundamentally deterritorialized, linking searchers anywhere in the world with websites located anywhere in the world. But what if a territorially based sovereign wants to block certain search results because the sovereign objects in some way to the underlying website that would otherwise be retrieved in the search? In such circumstances, as in the *Yahoo!* case, regulators may focus on the intermediary – here the search company – rather than the offending website because it is far easier to find the search company and deputize it to leverage the regulation.

In 2014 the European Court of Justice (ECJ) took this approach in a case involving Google.[79] A 1995 European Council data privacy directive[80] had recognized that individuals possess privacy rights in data. As interpreted by the ECJ, such a right allows individuals to object to old reputation-damaging online information about them that is no longer relevant and not of sufficient public concern to continue to be searchable.

Significantly, rather than apply the directive against the website operator, the court ruled that it was Google, as the search operator, who bore responsibility for ensuring that websites containing this sort of obsolete private information be blocked from search results. Moreover, again as with the *Yahoo!* case, the court deemed it insufficient only to apply its ruling to google.es, the Spanish subsidiary, instead ruling that google.com must also block offending websites from its search results.

By making Google responsible for enforcing this right to be forgotten, the ECJ effectively deputized Google as a sort of administrative agency. Henceforth, any individual seeking to have a website blocked from Google search must first file a notice with Google. Then, it will be Google's legal team that will apply the ECJ's balancing test to see if the elements of the right to be forgotten are satisfied and there is insufficient countervailing public interest in the information remaining accessible. If the individual disagrees with Google's decision, then that decision can be challenged in court. Given that Google is constantly altering its search algorithms anyway, one can understand

[79] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R. 317 (May 13, 2014), https://perma.cc/2367-44E8.

[80] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

why the court would view this as an effective division of labor. Moreover, Google is not jurisdictionally constrained regarding the websites it blocks from its search algorithms, as a government regulator would be if it sought to have a website taken down. Nevertheless, the fact is that a European court has required Google, a US corporation, to perform a quasi-governmental adjudicatory function on a worldwide basis (albeit only at the request of EU citizens).

This case, therefore, not only illustrates issues of jurisdiction but also the increased importance of intermediaries such as virtual world operators, online service providers, social media companies, and search engines. Given that our social lives are conducted through or stored with such intermediary companies, it is increasingly clear that those companies are likely to become the brokers that territorially based governments use to pursue regulation. And, of course, as the ubiquitous power of those companies over data grows, we can expect that they will often be the target of complaints by individuals and governments.

III *Procureur-General* v. *Yahoo! Inc.*; *Procureur-General* v. *Skype*

Meanwhile, Belgian authorities in 2009 reprised the French efforts against Yahoo! from 2000, requiring Yahoo! to disclose subscriber information about Yahoo! users as part of a fraud investigation. Yahoo! once again argued that the application of the Belgium statute to a company without a physical presence in Belgium was impermissibly extraterritorial.[81] And Yahoo!'s argument was perhaps even more compelling than in the French case because, although there was a country-specific yahoo.be website, unlike in the French case, it does not appear that Yahoo! even had a Belgium subsidiary operating locally.

Nevertheless, the Supreme Court of Belgium rejected Yahoo!'s argument.[82] Significantly, the court took an extremely broad view both regarding the scope of the statute and Belgian law enforcement authority more generally. First, according to the court, the Belgian law at issue covered "any operator or provider that actively aims its economic activities on [Belgium] consumers," regardless of whether or not the operator or provider has a physical presence in Belgium.[83] And the court reasoned that enforcing the law would not require

[81] Procureur-Général v. Yahoo! Inc., Hof van Cassatie [Cass.] [Court of Cassation], Dec. 1, 2015, No. P.13.2082.N (Belg.), *translated in* 13 Digital Evidence & Electronic Signature L. Rev. 156 (2016).
[82] *Id.* at 157.
[83] *Id.*

Belgian authorities to act extraterritorially because the statute at issue did not "require the performance of any physical act abroad." From this perspective, the authorities were simply staying in Belgium asking for data to be provided by Yahoo![84] Interestingly, whereas the Second Circuit had ruled that US law enforcement authorities could not collect information held abroad because it was akin to traveling beyond their territorial boundaries, the Belgian court emphasized that the Belgian authorities were simply remaining in the jurisdiction receiving data from elsewhere.

Subsequently, a lower court in Belgium has applied the logic of the *Yahoo!* case to assert jurisdiction over Skype in a case where Belgian authorities sought not only subscriber information but the content of communications as well.[85] Skype complied with regard to registration information, but argued that because Skype is a Luxembourg company, there was no jurisdiction in Belgium. Instead, according to Skype, any request for communications content must proceed via a mutual legal assistance request of the Luxembourg government.

The Belgian court rejected this argument. The court ruled that even though Skype was based in Luxembourg, it was "actively participating in the economic life in Belgium" by offering services there and was therefore subject to Belgian jurisdiction.[86] Echoing the Belgian Supreme Court's decision in *Yahoo!*, the court characterized the enforcement action as occurring within Belgium because presumably the requested data would be handed over there, regardless of where that data might have been collected or stored and regardless of whether or not the underlying target of the investigation was a Belgian citizen.

Thus, the two Belgian cases go far beyond what even the US government argued in the *Microsoft* case, because at least with Microsoft, the government clearly had jurisdiction over the intermediary, which was indisputably based in Washington state. In contrast, neither Yahoo! nor Skype had either a physical presence in Belgium or even a subsidiary there. And if the test is merely whether a company "participates in the economic life of Belgium" by offering services to Belgian customers, then jurisdiction may potentially extend to any web page viewed in Belgium regardless of where the content originated. Such a position mirrors early internet jurisdiction cases in the United States that

[84] *Id.*

[85] Procureur Général v. Skype, Tribunal de Première Instance [Civ.] [Tribunal of First Instance], Mechelen, Oct. 27, 2016, No. ME 20.4.1 105151-12, ¶¶ 1.2–1.5 (Belg.), https://perma.cc/C5Z7-EZ9Y.

[86] *Id.*

asserted jurisdiction over websites wherever they were viewed or viewable, conceptualizing a website as a twenty-four-hour-a-day advertisement "entering" every jurisdiction where the website was accessible.[87]

IV *Google* v. *Equustek*

Finally, we turn to a 2017 Canadian Supreme Court decision that in many respects reprises elements of both the *Google Spain* case and the original *Yahoo! France* case with which we began.

In this case, Equustek, a small Canadian technology company, brought a trademark suit in Canada against another company, Datalink, which had been distributing its products. Equustek claimed that Datalink had begun to relabel one of Equustek's products in order to sell the product as its own. Ultimately, Datalink left Canada, and although Equustek was able to secure Canadian court orders enjoining Datalink from continuing to sell Equustek's products on its websites, those orders were ineffectual because Datalink no longer had any presence or assets in Canada and simply ignored the orders.

Thus, we see an inherent difficulty a territorially based sovereign has in enforcing its judgment. If the relevant party has insufficient presence in the jurisdiction, there will be limited means of enforcing any order. In such a circumstance, as we have seen already, a global data intermediary becomes a useful way to leverage power. Accordingly, it is not surprising that the Canadian courts would turn to Google, just as the ECJ did in the "right to be forgotten" context. As in that case, the courts recognized that if a website exists but can't be found in a Google search, the utility of that website will be reduced to almost zero. Thus, following the court order against Datalink and a request from Equustek, Google agreed to deindex some but not all of Datalink's web pages so that they would not be found if they were being searched for on Google's Canadian site, google.ca. However, those same pages could still be found by searching on google.com or other countries' Google search sites. Thus, as with blocking Nazi memorabilia on yahoo.fr, the Canada-specific remedy was insufficient.

Accordingly, Equustek sought a preliminary injunction against Google requiring the company to deindex Datalink's websites through any of its search portals worldwide. Google argued in response that such an injunction

[87] Bochan v. La Fontaine, 68 F. Supp. 2d 692, 701 (E.D. Va. 1999) ("Federal courts in Virginia in particular have generally found that Internet advertising accessible to Virginia residents 24 hours a day constitutes solicitation of business in Virginia sufficient to satisfy the requirements of § 8.01–328.1(A)(4)" (personal jurisdiction)).

would be improperly extraterritorial as it would mean that Canada's judgment would dictate search results around the world.

The Canadian Supreme Court rejected Google's argument. According to the court,

> [w]here it is necessary to ensure the injunction's effectiveness, a court can grant an injunction enjoining conduct anywhere in the world. The problem in this case is occurring online and globally. The Internet has no borders – its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates – globally.

Accordingly, the court took a purely functionalist approach. Because there was no other way to make its injunction against Datalink effective, it must require Google, a nonparty to the suit, to act as its global enforcement mechanism, just as the European court had in the *Google Spain* case.

Significantly, unlike the *Yahoo! France* case, the concerns about chilling free speech in this case were far less strong because the websites in question were sales sites, and though commercial speech receives First Amendment protection under US Constitutional law, that protection is arguably less stringent.[88] Moreover, if the websites to be deindexed were in fact infringing trademark, deindexing them would be unlikely to be the basis for a successful First Amendment claim. And, of course, since Datalink is not a US corporation, it is not clear it would have valid First Amendment rights to assert in any event. As to Google, it is an open question whether search results count as speech for First Amendment purposes.

Nevertheless, despite the lessened First Amendment concerns at stake, Google took the same path that Yahoo! had sixteen years earlier, filing for a declaratory judgment in a US court that would declare the Canadian judgment unenforceable under US law. This time, however, the law in question was section 230 of the Communications Decency Act, which generally immunizes internet service providers against liability arising from content created by third parties.[89] And as in the *Yahoo!* case, the district court granted the declaratory judgment.[90]

[88] *See* Central Hudson Gas & Elec. Corp. v. Public Svc. Comm'n of New York, 447 U.S. 557 (1980) ("Because 'commercial speech' is afforded less constitutional protection than other forms of speech, it is important that the commercial speech concept not be defined too broadly lest speech deserving of greater constitutional protection be inadvertently suppressed.").

[89] 47 U.S.C. § 230 (2012).

[90] Google v. Equustek Solutions, No. 5:17-cv-04207, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017).

The US District Court's declaratory judgment decision is questionable on a number of grounds. First, because no real liability was being imposed on Google, it is possible section 230 would not apply. Moreover, no party was yet seeking to enforce the Canadian court judgment in the United States, arguably rendering Google's suit unripe or requiring dismissal for lack of personal jurisdiction over the defendant, Equustek. It was on those grounds, after all, that the Ninth Circuit had ultimately overruled the district court order in the *Yahoo!* case.[91] Finally, as noted previously, even if the Canadian Supreme Court order would violate US federal law if the order had been issued by a US court, that does not answer the question of whether it would likewise violate federal law to enforce another court's judgment to the same effect. After all, the judgment recognition decision is based on different considerations from those that are involved in issuing an order in the first instance.

In the end, although the district court's declaratory judgment order seems to create a jurisdictional stalemate, the reality is that Equustek need not ever seek enforcement of the Canadian Supreme Court judgment in the United States anyway because Google presumably wants to continue to do business in Canada as an ongoing commercial enterprise there, and so it is highly likely that Google will comply with the order just as Yahoo! did in France. Thus, the declaratory judgment action may be more a public relations ploy than a serious effort to thwart extraterritorial enforcement.

V *Global Electronic Currencies and Transactions*

Search engines are, of course, not the only piece of deterritorialized infrastructure that operates in online interaction. Consider the general ledger technology known as blockchain. Although the global alternative currency Bitcoin has generated the most attention, it is only one instantiation of this technology. Blockchains store data in distributed computers and chain them together to form an unbroken record of that information.[92] The information stored could be currency transactions, but it could also be any automated executable set of instructions, such as an insurance contract that pays out automatically if a given event occurs. Two features make blockchain technology valuable. First, identical copies of the particular blockchain (or ledger) are stored on and accessed from potentially thousands of computers around the

[91] *Yahoo!*, 433 F.3d at 1253.

[92] Clyde & Co., Blockchain and the Law: An Uncharted Landscape 1 (2016), https://perma.cc/7D7A-DHV4.

world. Any changes to information on one is immediately and automatically authenticated by the others, and any authenticated change immediately updates on all computers in the chain. Second, the information is encrypted so that, in combination with its decentralization, it is difficult to hack.

On the other hand, those same features make blockchains potentially difficult to regulate. Not only do blockchain transactions cross borders, but it will often to be difficult to identify a particular computer or entity that is responsible if there is a dispute or problem. As one commenter has described it, "the infrastructure does not fall under any traditional jurisdiction, but the users of the infrastructure also naturally evade any sense of traditional jurisdiction. All parties may transact entirely anonymously on a public blockchain."[93]

So far, blockchain technology has not been deployed sufficiently for us to know precisely how legal challenges are likely to be resolved. And the assumption that blockchain transactions completely lack connection to a territorially based entity may be overstated. That is because the parties to a blockchain transaction are still physically located somewhere on Earth. And to the extent that money changes hands, that money is in some form sent from one physical place to another, creating a territorial nexus.

For example, in *Greene* v. *Mizuho Bank, Ltd.*,[94] the plaintiff wired money from a Wells Fargo branch account in California to a bank in Japan, which then held the funds in an account used by a Bitcoin exchange. So although the Bitcoin transactions themselves might not have a location, the exchange interacted with a bank chartered in Japan, and that bank in turn interacted with a bank in California, making all of the defendants potentially subject to jurisdiction in California.

Of course, when we say that money was "sent from California to Japan," we are really talking about metaphysical electronic signals crossing borders, and so we are in a sense using what is already a fictional connection to the physical world to territorially ground a Bitcoin transaction, which is an even more fictional connection to the physical world. It remains to be seen at what point all that is solid will melt into air and legal jurisdiction based on territory will cease to be meaningful as a way to describe and regulate electronic transactions at all.

[93] Wulf A. Kaal & Craig Calcaterra, *Blockchain Technology's Distributed Jurisdiction*, MEDIUM, June 20, 2017, https://perma.cc/3PMT-T98E.

[94] Green v. Mizuho Bank, Ltd., 169 F. Supp. 3d 855 (N.D. Ill. 2016).

D THE NEED FOR A COSMOPOLITAN PLURALIST APPROACH TO CONFLICT OF LAWS

As difficult as the cases discussed above may be to resolve, if anything, the future holds issues that may be tougher still. Similar questions can, and almost certainly will, be raised by automation in vehicles and by machine-learning-based robotics and drones for commercial, consumer, and military use. These new deployments will likely reshape legal rules regarding product liability, insurance, contract, jurisdiction, criminal law, and other areas. Indeed, the movement of our social activity into various forms of the virtual is a major trend that is not likely to reverse, and it is a trend that is bound to unsettle previously settled legal principles. Yet, a time of flux is also a time of opportunity. As judges, legislators, and scholars struggle to apply old legal principles to new contexts, they are – in a far more self-conscious way than usual – questioning whether those old legal principles really work in the brave new world they are encountering. Such a time of self-conscious inquiry opens the conceptual space to allow one to go back to first principles and ask important jurisprudential and sociologically charged questions that run throughout all of law.

With regard to conflicts of law, rather than simply adapt existing jurisdictional models to the new social context in order to "solve" tensions in particular situations, we need to reflect on the conflicts principles we are seeking to adapt. By doing so, we can perhaps lay the groundwork for a theoretical model that will allow us better to understand and evaluate the increasing transnationalization of data flows.

To construct such a model, we first need to remind ourselves that conceptions of legal jurisdiction (by which I mean to include both the jurisdiction to decide a dispute and the determination that a jurisdiction's law will apply) are more than simply ideas about the appropriate boundaries for state regulation or the efficient allocation of governing authority. Jurisdiction is also the locus for debates about community definition, sovereignty, and legitimacy. Moreover, the idea of legal jurisdiction both reflects and reinforces social conceptions of space, distance, and identity. Too often, however, contemporary frameworks for thinking about jurisdictional authority unreflectively accept the assumption that nation states defined by fixed territorial borders are the only relevant jurisdictional entities, without examining how people actually experience allegiance to community or understand their relationship to geographical distance and territorial borders. Moreover, by sidestepping these questions of community definition, borders, and the experience of place, legal thinkers are ignoring a

voluminous literature in anthropology, cultural studies, and the social sciences concerning such issues.[95]

Indeed, even a cursory examination reveals that our current territorially based rules for jurisdiction (and conflicts of law) were developed in an era when physical geography was more meaningful than it is today and during a brief historical moment when the ideas of nation and state were being joined by a hyphen to create a historically contingent Westphalian order. Yet if the ideas of geographical territory and the nation state are no longer treated as givens for defining community,[96] an entirely new set of questions can be asked. How are communities appropriately defined in today's world? In what ways might we say that the nation state is an *imagined* community,[97] and what other imaginings are possible? How do people actually experience the idea of membership in multiple overlapping communities? Should citizenship be theorized as one of the many subject positions occupied by people as members of diverse, sometimes nonterritorial, collectivities? In what ways are our sense of place and community membership constructed through social forces? And if ideas such as "place," "community," "member," "nation," "citizen," "boundary," and "stranger"[98] are not natural and inevitable but are instead constructed, imagined, and (sometimes) imposed, what does that say about the presumed "naturalness" of our geographically based jurisdiction and choice-of-law rules?

We need to ask these questions, drawing on humanities and social science literature that complicates many of the premises most lawmakers and legal scholars take for granted concerning jurisdiction. This literature insists that we recognize the constructed nature of our ideas about boundaries and

[95] For a more detailed discussion of this literature as applied to issues of legal jurisdiction, see generally Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. Pa. L. Rev. 311 (2002).

[96] *See* Akhil Gupta, *The Song of the Nonaligned World: Transnational Identities and the Reinscription of Space in Late Capitalism*, *in* Culture Power Place: Explorations in Critical Anthropology 179 (Akhil Gupta & James Ferguson eds., 1997) ("The nation is so deeply implicated in the texture of everyday life and so thoroughly presupposed in academic discourses on 'culture' and 'society' [and jurisdiction] that it becomes difficult to remember that it is only one, relatively recent, historically contingent form of organizing space in the world.").

[97] *See generally* Benedict Anderson, Imagined Communities (Rev. ed. 2006) (analyzing the nation state as an imagined community).

[98] *See, e.g.*, Georg Simmel, *The Stranger*, *in* The Sociology of Georg Simmel 402, 402 (Kurt H. Wolff ed., 1964) (arguing that the stranger "is fixed within a particular spatial group, or within a group whose boundaries are similar to spatial boundaries," but that "his position in this group is determined, essentially, by the fact that he has not belonged to it from the beginning, that he imports qualities into it, which do not and cannot stem from the group itself").

community definition and that we acknowledge the historical contingency of the nation state. Moreover, by analyzing the social meaning of our affiliations across space, we can think about alternative conceptions of community that are subnational, transnational, supranational, or cosmopolitan. Such an analysis provides a better understanding of the world of experience on which the legal world is mapped and is therefore essential in order to develop a richer descriptive account of what it means for a juridical body to assert jurisdiction over a controversy.

In addition, moving from the descriptive to the normative, can we conceptualize the idea of jurisdiction in a way that might take into consideration the contested and constantly shifting process by which people imagine communities and their membership in them? Just as Phillip Jessup noted many of the ways a rigidly territorial conception of jurisdiction eventually gave way in the first part of the twentieth century to the idea of jurisdiction based on contacts with a sovereign entity, so too a contacts-based approach must now yield to a conception of jurisdiction based on community affiliation. In the past, I have offered one such conception, which I have termed a cosmopolitan pluralist conception of jurisdiction.[99]

A *cosmopolitan*[100] approach allows us to think of community not as a geographically determined territory circumscribed by fixed boundaries, but as "articulated moments in networks of social relations and understandings."[101] This dynamic understanding of the relationship between the "local" community and other forms of community affiliation (regional, national, transnational, international, cosmopolitan) permits us to conceptualize legal jurisdiction in terms of social interactions that are fluid processes, not motionless demarcations frozen in time and space.

In addition, if nation states are imagined, historically contingent communities defined by admittedly arbitrary geographical boundaries, and if those

[99] *See* Paul Schiff Berman, Global Legal Pluralism: A Jurisprudence of Law Beyond Borders (2012).

[100] By "cosmopolitan," I refer to a multivalent perspective that recognizes the wide variety of affiliations people feel toward a range of communities, from the most local to the most global. I therefore distinguish cosmopolitanism from a universalist vision (often associated with cosmopolitanism), which sees people solely, or primarily, as members of one world community. Cosmopolitanism, as I use the term, involves an ideal of multiple attachments; it does not necessarily entail the erasure of nonglobal community affiliations. *See, e.g.*, Bruce Robbins, *Introduction Part I: Actually Existing Cosmopolitanism*, *in* Cosmopolitics: Thinking and Feeling beyond the Nation 1, 3 (Pheng Cheah & Bruce Robbins eds., 1998) ("[I]nstead of an ideal of detachment, actually existing cosmopolitanism is a reality of (re) attachment, multiple attachment, or attachment at a distance.").

[101] Doreen Massey, Space, Place, and Gender 154 (1994).

nation states – because of transnational flows of information, capital, and people – no longer define unified communities (if they ever did), then there is no conceptual justification for conceiving of nation states as possessing a monopoly on the assertion of jurisdiction. Instead, any comprehensive theory of conflicts of law must acknowledge that *nonstate* communities also assert various claims to jurisdictional authority and articulate alternative norms that are often incorporated into more "official" legal regimes. This *pluralist*[102] understanding of jurisdiction helps us to see that law is not merely the coercive command of a sovereign power but a language for imagining alternative future worlds. Moreover, various norm-generating communities (not just the sovereign) are always contesting the shape of such worlds.

Finally, as this survey of cases makes clear, in a world of deterritorialized data, the role of intermediaries as lawmakers and law enforcers has radically increased. When Facebook enforces terms of service, or Twitter is asked (or required) to police hate speech, or Google implements an ECJ ruling, we can call these acts of intermediaries law or not, but a pluralist would argue that it doesn't matter how you define it; the fact is that it affects the behavior of real people in the real world. Indeed, the actions of intermediaries can have more impact than the sometimes empty commands of a sovereign. A pluralist perspective has the advantage of not getting caught up in definitions of law but instead recognizing that the quasi-law created, imposed, and/or applied by nongovernmental entities should always remain within our legal analytical purview.

E CONCLUSION

No fixed conflicts-of-law principles will ever completely solve the conflicts problems raised by increasing transnational data flows. Indeed, there are no perfect solutions, and the factual settings whereby these sorts of problems may arise are so multifaceted and unpredictable that trying to develop a comprehensive set of rules to govern all eventualities strikes me as a fool's errand. Moreover, even if we could discover a grand scheme for handling these questions, it is unlikely that all communities in the world (or their judicial bodies) would agree. Therefore, no amount of analysis will ever wipe out the reality of legal pluralism and its attendant uncertainties.

Nevertheless, just as Phillip Jessup did sixty years ago when he sketched out a set of conflicts-of-law problems under the rubric he called transnational law,

[102] *See* Paul Schiff Berman, *The New Legal Pluralism*, 2009 ANN. REV. L. & SOC. SCIENCES 225 (providing an overview of the trajectory of legal pluralism scholarship).

so too it is incumbent on legal scholars today to recognize the new challenges arising in this increasingly data-driven world and to build new cosmopolitan pluralist legal models that may, over time, become simply the way we conceptualize law in the twenty-first century. After all, law and society are forever like a Mobius strip, each turning into the other, and what seems unsettled and new to us now may become the commonplace assumptions of future generations. In that regard, Jessup's bold proposal of sixty years ago seems largely uncontroversial and even obvious to most scholars today; that is the force of Jessup's ideas. But neither law nor society ever stop moving, and to do justice to Jessup's vision, we must push forward to develop new models to respond to new practices in new contexts.