

2018

## Legal Jurisdiction and the Deterritorialization of Data

Paul Schiff Berman

Follow this and additional works at: <https://scholarship.law.vanderbilt.edu/vlr>

---

### Recommended Citation

Paul Schiff Berman, Legal Jurisdiction and the Deterritorialization of Data, 71 *Vanderbilt Law Review* (2024)

Available at: <https://scholarship.law.vanderbilt.edu/vlr/vol71/iss7/2>

This Article is brought to you for free and open access by Scholarship@Vanderbilt Law. It has been accepted for inclusion in Vanderbilt Law Review by an authorized editor of Scholarship@Vanderbilt Law. For more information, please contact [mark.j.williams@vanderbilt.edu](mailto:mark.j.williams@vanderbilt.edu).

# Legal Jurisdiction and the Deterritorialization of Data

*Paul Schiff Berman\**

INTRODUCTION.....	12
I. PLUS ÇA CHANGE...	13
II. A COSMOPOLITAN PLURALIST VISION OF CONFLICT OF LAWS.....	20
III. BUILDING JURISDICTIONAL RULES IN A DETERRITORIALIZED, DATA-DRIVEN WORLD.....	22
A. <i>The territorial location of data or servers is irrelevant.</i> .....	23
B. <i>The place of incorporation of a corporation is potentially relevant to the jurisdictional calculus, but should not be determinative.</i> .....	24
C. <i>Community affiliation is a more plausible basis for legal jurisdiction than contacts with a territorially based sovereign.</i> .....	24
D. <i>Trying to serve a market is a more relevant jurisdictional hook than targeting a territory.</i> .....	25
E. <i>The size, sophistication, and economic breadth of an actor is relevant to the jurisdictional inquiry.</i> .....	26
F. <i>The effects of activities can provide a plausible basis for the assertion of jurisdiction, even without a territorial nexus.</i> .....	27
G. <i>Enforcing a judgment through a powerful intermediary is not inherently illegitimate, but the resulting intermediary enforcement must be regulated, not simply delegated.</i> .....	27
H. <i>Terms of Service agreements will not necessarily resolve jurisdictional and choice-of-law decisions.</i> ...	29

---

\* Walter S. Cox Professor of Law, The George Washington University Law School. Special thanks to Samuel Wenzel for helpful research assistance in the preparation of this Response article. Some material derived from PAUL SCHIFF BERMAN, GLOBAL LEGAL PLURALISM: A JURISPRUDENCE OF LAW BEYOND BORDERS (2012).

I. <i>The decision regarding whether to enforce another jurisdiction's judgment is not the same as the decision regarding whether to issue that judgment in the first instance</i> .....	30
CONCLUSION.....	31

## INTRODUCTION

Jennifer Daskal's *Borders and Bits*<sup>1</sup> accurately describes one of the core challenges regarding jurisdictional law in the twenty-first century: electronic data—everything from e-mails 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 little relationship to physical territory. In addition, all of 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 U.S. citizen based in Maryland, have a g-mail account and Google, a U.S. corporation, decides to store my archived e-mails in Ireland or France or Indonesia (or indeed to split up the data fragments that make up each e-mail 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.

---

1. Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018).

Daskal's article does an excellent job of summarizing recent cases that raise these issues and effectively teasing out the conundrums that data poses for thinking about jurisdiction. In this Response article, therefore, I want to focus on two aspects of the jurisdictional question that are largely beyond the scope of her article. First, I think it is useful to provide more historical context than her article does both regarding early internet cases that pre-date the ones Daskal discusses by fifteen years or so, as well as the scholarly literature that arose in the late 1990s and early 2000s in response to precisely the problems that Daskal describes. This context is important, I think, because it suggests that the issues Daskal seeks to address are not new, though they may be accelerating. Further, the earlier scholarship may actually have more to offer than her article acknowledges. Second, and relatedly, although Daskal effectively lays out the problems raised by the deterritorialization of data, she does not offer much of a roadmap regarding new jurisdictional principles that might be developed to respond to this changing social reality. And ironically, it may be that some of the earlier scholarship on internet jurisdiction might point usefully towards such principles.

Thus, this Response offers both a "look back" and a "look forward": back to the early days of the commercial internet when courts and scholars first began wrestling with the problems of data's deterritorialization; and forward to a set of principles that might guide legal regimes considering jurisdictional dilemmas in the data-driven era in which we find ourselves.

#### I. PLUS ÇA CHANGE...

Reading Daskal's article, one might reasonably conclude that the issues she raises are new or have only arisen in the past few years. Indeed, all of the cases Daskal describes are of relatively recent vintage, and though Daskal briefly references early scholarly debate about internet jurisdiction, she does so only in passing and essentially dismisses that early work as outmoded. However, I think it might be useful to go back to some of that early scholarship in order to help frame more precisely what it is about data that is or is not different.

To the extent Daskal references past scholarship on internet jurisdiction, she focuses on the seminal 1996 article by David G. Post & David Johnson, *Law and Borders—The Rise of Law in Cyberspace*.<sup>2</sup> And there is a reason for that. This article was the first really to make the

---

2. David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

“data is different” argument in order to surface core legal questions about jurisdiction, sovereignty, and legitimacy. Crucially, the article made two fundamental points, one descriptive and one normative.

Descriptively, Johnson & Post argued that online interaction increased the likelihood that activity initiated in one location would create effects in another location, without regard to territory. As the authors put it, information “can be transmitted from one physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another.”<sup>3</sup> This was and remains the essence of the “data is different” argument: that physical location may no longer be as relevant with regard to electronic data, rendering problematic a world of legal jurisdictions based on territorially delimited authority.

Turning from the descriptive to the normative, Johnson & Post argued that, because territorially based sovereigns would inevitably face challenges of sovereignty and legitimacy in regulating online interaction, we might better think of the online world as its own world for jurisdictional purposes. Thus, they argued for the creation of an indigenous law of cyberspace, where different service providers and websites would compete with each other to offer different rule-sets, and users would “vote” for the rule-sets they prefer simply by making decisions as to which rule-sets to use.<sup>4</sup>

Unfortunately, because this normative claim was relatively easy to refute as unrealistic cyber-utopianism, scholars tended to ignore the important descriptive claim as well. Daskal falls into this trap. She confusingly labels the Johnson & Post position “unterritorialism” and then quickly dispatches it to the dustbin as a relic of the early internet era.

But the Johnson & Post argument is neither “unterritorialism” nor irrelevant. Indeed, for better or worse, Johnson & Post, far from being “unterritorialists,” started from the assumption that control over territory was the core principle underlying jurisdiction and sovereignty. Indeed, it was precisely this territorialism that, to them, made online interaction such a difficult problem for jurisdictional analysis.

It would therefore be more accurate to call Johnson & Post cyberspace exceptionalists.<sup>5</sup> They believed that the rise of online interaction required new rules for legal jurisdiction by upsetting old

---

3. *Id.* at 1370–71.

4. *Id.* at 1398–99.

5. This moniker has the added benefit of being the one Post himself adopted. See David G. Post, *Against Cyberanarchy*, 17 BERKELEY TECH. L.J. 1365 (2002).

assumptions about the general tie between legal effects and territorial location. And once we view them simply as exceptionalists, there is actually a straight line from their work to Patricia Bellia's 2001 *Chasing Bits Across Borders*<sup>6</sup> (which even has an almost identical title to Daskal's) to my 2002 article on *The Globalization of Jurisdiction*<sup>7</sup> to Daskal's contention that data is different.

Of course, even as a descriptive matter one could debate the exceptionalist position. For example, Jack Goldsmith argued that online activity created no fundamentally new legal problem and that "well-settled" principles in existing conflict-of-laws doctrines were adequate to address any issues to be resolved.<sup>8</sup> As Daskal notes in her article, Goldsmith's successor in advancing the unexceptionalist position is Andrew K. Woods, who has made strikingly similar arguments to the ones Goldsmith made in the late 1990s.<sup>9</sup>

To my mind, however, this dichotomy between exceptionalist and unexceptionalist visions was a false one from the start. First, one's perspective on whether the online medium creates a new problem depends in large part on what the legal question is. For example, if our focus turned from jurisdiction to simply the substantive law of defamation, we would note that defamation is generally defined as the communication of a false statement about someone with the requisite degree of intent. This communication can be written or oral, and if it is written, there does not seem to be much of a legal difference whether the written defamation is communicated by postal mail, fax, or e-mail. It is still defamation, and the online context doesn't change the legal liability question. Thus, unexceptionalism seems to apply to defamation law. But when we turn to the question of *intermediary* liability regarding that same defamatory content and ask whether (and under what circumstances) various types of internet service providers should be held liable for defamatory content accessible through their portals, then we have a question that is not easily answered without some conceptual understanding of what an internet service provider is or should be. Or, if we ask a jurisdictional question about where the defamatory act took place or whose discovery rules would govern the defamatory e-mail at issue, then again we face core questions about the nature of jurisdiction. So, online defamation issues require either an exceptionalist or an unexceptionalist approach, depending on what aspect of the case one is discussing.

---

6. Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35.

7. Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311 (2002).

8. See Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

9. See Andrew K. Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729 (2016).

The second reason the dichotomy was unhelpful from the beginning is that the unexceptionalist position assumes that there actually *are* well-settled “general” principles of law that can simply be applied to new legal settings without alteration. And yet it is the nature of law that it changes over time. Thus, what is “well-settled” for one generation (or in one century) is apt to be very different from what is well-settled for the next. Even more importantly, new technologies that alter the culture are precisely the sorts of changes that tend to result in shifts to well-settled legal principles.<sup>10</sup>

For example, in the nineteenth century, “well-settled” U.S. principles of legal jurisdiction and choice of law saw jurisdiction as rooted almost exclusively in the territorial power of the sovereign.<sup>11</sup> Each sovereign was deemed to have jurisdiction, exclusive of all other sovereigns, to bind persons and things present within its territorial boundaries. By the early twentieth century, growth of interstate commerce, transportation, and cross-border corporate activity put pressure on the idea that a state’s judicial power extended only to its territorial boundary. In particular, the invention of the automobile and the development of the modern corporation meant that far-away entities could inflict harm within a state without actually being present there at the time of a lawsuit. Not surprisingly, by the end of the twentieth century, it had become “well-settled” in U.S. jurisdiction jurisprudence that a state may at least sometimes assert jurisdiction over a defendant if the effects of the defendant’s activities are felt within the state’s borders, even if the defendant has not literally set foot there.<sup>12</sup> Likewise, it had become “well-settled” that choice-of-law rules could be based on governmental interests or relationships as well as territorial connections.<sup>13</sup> And, of course, these new “well-settled” rules felt as commonsensical and obvious to most judges, lawyers, and observers as the more territorialist view felt in the nineteenth century.

Now, it seems safe to say that jurisdictional, choice-of-law, and judgment recognition rules are in flux again, at least in part because of online interaction. Indeed, as many of the cases described by Daskal suggest, the idea of basing jurisdiction on where effects are felt is difficult to apply to online interaction because our social lives are increasingly spread out in many different locations, anywhere our data

---

10. I discuss such cultural shifts in more detail in PAUL SCHIFF BERMAN, *GLOBAL LEGAL PLURALISM: A JURISPRUDENCE OF LAW BEYOND BORDERS* (2012).

11. *See, e.g.*, *Pennoyer v. Neff*, 95 U.S. 714 (1877); RESTATEMENT (FIRST) OF CONFLICT OF LAW (1934).

12. *See, e.g.*, *International Shoe v. Washington*, 326 U.S. 310 (1945).

13. *See, e.g.*, RESTATEMENT (SECOND) OF CONFLICT OF LAW (1971).

is stored, used, or viewed, and we are potentially affected by activity taking place anywhere, without regard to physical territory.

The answers that law will ultimately evolve to address these sorts of problems are difficult to predict, and scholars and judges will no doubt have differing approaches to specific questions of jurisdiction, choice of law, and judgment recognition regarding online interaction, virtual worlds, data storage, digital currencies, autonomous entities, and the like. Suffice to say that however one resolves the issues, “well-settled” principles of law are unlikely to be very helpful because such principles are themselves always in flux, often precisely because of the pressures placed on such principles by new communications technologies such as the internet and new ways in which social lives become deterritorialized. Thus, in some sense, a pure unexceptionalist position is difficult to maintain. But if unexceptionalists relied too much on the application of mythical well-settled principles, the exceptionalists, at times, tended to the opposite extreme, assuming that the rise of online interaction, data storage and the like upend nearly all extant ideas about law and the role of the state. As we have seen in the two decades since Johnson & Post wrote their article, state regulation of online activity remains a potent force, even allowing for all the jurisdictional conundrums they correctly predicted.

Finally, it is worth noting that, although the cyber-libertarian idea of a world of independent rule-sets created by websites has not come to pass, even that prediction was not altogether wrong. As Daskal’s article makes clear, ubiquitous platforms such as Yahoo!, Microsoft, Skype, and Google are frequently being commandeered by territorially based sovereign entities to operate as a worldwide nonterritorial enforcement mechanism. So the idea that territorially based sovereigns would be unable to effectively regulate and would therefore need web-based assertions of jurisdiction is now in many respects the way things have evolved, for better or worse. And, of course, the ongoing battles about the enforceability of online “Terms of Service” agreements make clear that online rule-sets still matter.

Thus, instead of labeling the early scholarship “unterritorialism” and then dismissing it as a relic of an earlier cyber-utopian era, we might more profitably view it as a debate between exceptionalists and unexceptionalists about the degree to which settled conflict-of-law principles would provide stable solutions to jurisdictional issues related to online interaction. Viewed in this way, Daskal’s argument for data’s difference looks a little less like a new theory for online regulation and a little more like simply the most recent in a line of exceptionalist arguments.



And it is not just the current scholarly debates that echo the debates of two decades ago, but the legal cases as well. Indeed, the recent cases Daskal describes reprise many of the dilemmas and arguments from the first decade of commercial online activity. As early as 1995, a federal district court in Connecticut ruled that it had proper jurisdiction over the defendant Instruction Set, a Massachusetts-based provider of computer technology, even though Instruction Set maintained no offices in Connecticut and did not conduct regular business there.<sup>14</sup> The court ruled that the defendant's promotional website, because it was *accessible* in Connecticut, supported the exercise of jurisdiction in the state. According to the court, the website advertisements were directed to all states within the United States. Therefore, Instruction Set had "purposely availed itself of the privilege of doing business within Connecticut."<sup>15</sup> This vision looks quite a bit like the Belgian assertions of jurisdiction over Yahoo! and Skype that Daskal describes.<sup>16</sup>

Similarly, we can see that efforts to limit the jurisdictional reach of legal decisions over online activity tend to be unsatisfactory. Back in 2000, a French court asserted jurisdiction over Yahoo! and ordered 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.<sup>17</sup> Undisputedly, selling such merchandise in France would violate French law,<sup>18</sup> and there would have been 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.

---

14. See *Inset Sys. Inc. v. Instruction Set, Inc.*, 937 F. Supp. 161 (D. Conn. 1966).

15. See *id.* at 164.

16. See Daskal, *supra* note 1, at 192–95.

17. See *LICRA v. Yahoo!, Inc.*, Tribunal de Grande Instance de Paris [hereinafter TGI] [High Court of Paris], May 22, 2000, <http://lthoumyre.chez.com/txt/jurisfr/cti/yauctions20000522.htm>, [<https://perma.cc/738B-V9BM>].

18. See CODE PÉNAL [C. PÉN] [PENAL CODE], art. R.645-1 (prohibiting the public display of Nazi memorabilia except for the purposes of an historical film, show, or exhibit), <https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006419560&cidTexte=LEGITEXT000006070719>, [<https://perma.cc/BL8T-4J3A>].

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.<sup>19</sup> 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.

The *Google Spain* right-to-be-forgotten case that Daskal describes follows a similar pattern.<sup>20</sup> Google was willing to de-index websites for users using Google's Spanish portal, google.es, but the European Court of Justice ("ECJ") understandably found that solution inadequate because google.com is so easy for Spaniards to access. But, as in the *Yahoo!* case fifteen years earlier, the concern is that de-indexing for all users, regardless of location, effectively means that the ECJ decision is a worldwide injunction, perhaps taking us all the way back to the 1995 *Instruction Set* case discussed above. On the other hand, it is easy to see that the extraterritoriality charge runs in both directions. If France or Spain is *not* able to block the access of its 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 or search engines 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!* and *Google Spain* cases therefore are simply reiterations of the basic dichotomy that has been repeated over twenty years of jurisdictional jurisprudence. On the one hand, legal authorities wish to assert jurisdiction anywhere a community is effected 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

---

19. See *LICRA v. Yahoo!, Inc.*, TGI, Nov. 20, 2000, <http://www.lapres.net/yahen11.html>, [<https://perma.cc/ALK9-XM6A>].

20. See *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, May 13, 2014, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131>, [<https://perma.cc/2367-44E8>].

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.

## II. A COSMOPOLITAN PLURALIST VISION OF CONFLICT OF LAWS

So, if Daskal is right (and I believe she is) that data is different and is inexorably and inevitably changing settled expectations about conflict-of-law rules, what are some of the principles that might help us make sense of this brave new world in which we find ourselves? This is beyond the scope of Daskal's article, but again it seems to me that a look back might allow us to look forward. In my 2002 article, *The Globalization of Jurisdiction*,<sup>21</sup> and my 2005 article *Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era*,<sup>22</sup> I argued for a cosmopolitan pluralist conception of conflict of laws. I noted that the movement of our social activity into various forms of the virtual is a real trend, and it is one 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 anymore. 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.

In addition, moving from the descriptive to the normative, we can 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 a rigidly territorial conception of jurisdiction eventually gave way in the

---

21. See Berman, *supra* note 7.

22. See Paul Schiff Berman, *Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era*, 153 U. PA. L. REV. 1819 (2005).

first part of the twentieth century to the idea of jurisdiction based on contacts with a sovereign entity, so too a contacts-based approach might now yield to a conception of jurisdiction based on community affiliation.

A *cosmopolitan*<sup>23</sup> approach allows us to think of community not as a geographically determined territory circumscribed by fixed boundaries, but as a set of multiple affiliations held simultaneously.<sup>24</sup> This dynamic understanding of the relationship between the “local” community and other forms of community affiliation permits us to conceptualize legal jurisdiction in terms of social interactions that are fluid processes, not motionless demarcations frozen in time and space. A court in one country might therefore appropriately assert community dominion over a legal dispute even if the court’s territorially based contacts with the dispute are minimal. Conversely, a country that has certain “contacts” with a dispute might nevertheless be unable to establish a tie between a local community and a distant defendant sufficient to justify asserting its dominion.

A cosmopolitan interrogation of conceptions of community, therefore, might rein in some assertions of jurisdiction over distant acts while permitting other extraterritorial assertions of jurisdiction that are currently unrecognized. Accordingly, the cosmopolitan pluralist conception of jurisdiction I have proposed seeks to capture a middle ground between strict territorialism on the one hand and a system of complete universal jurisdiction on the other. In any event, the jurisdictional inquiry would no longer be based on a reified counting of contacts with, effects on, or interests of a territorially bounded population. Rather, courts would take seriously the multiple definitions of community that might be available, the symbolic significance of asserting jurisdiction over an actor, and the normative desirability of conceptualizing the parties before the court as members of the same legal jurisdiction.

In addition, if nation-states are imagined, historically contingent communities defined by admittedly arbitrary geographical boundaries, and if those nation-states—because of transnational flows

---

23. 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.”).

24. See DOREEN MASSEY, *SPACE, PLACE, AND GENDER*, 154 (1994).

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 jurisdiction 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*<sup>25</sup> 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 the 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 agreements, 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 remain within our legal analytical purview whether we call it law or not.

### III. BUILDING JURISDICTIONAL RULES IN A DETERRITORIALIZED, DATA-DRIVEN WORLD

So, how might we build a conflict-of-laws jurisprudence that reflects a world of deterritorialized data? How can we create a cosmopolitan pluralist vision that takes account of changing social reality without either starting from scratch and throwing out all extant conflicts principles on the one hand, or simply assuming current doctrine will suffice on the other hand? In short, how can we meld exceptionalist and unexceptionalist positions to develop workable provisional compromises to govern the ubiquitous virtual worlds of the twenty-first century?

As a true believer in common law case-by-case adjudication, I cannot provide a comprehensive code that anticipates all permutations

---

25. For a more detailed application of the insights of legal pluralism to conflict-of-laws questions, see BERMAN, *supra* note 10.

of human activity and provides a definitive answer. Indeed, one of the important lessons of conflict of laws, it seems to me, is that there is no single unifying grand theory that can provide an authoritative answer to every possible dilemma or account for the infinite variety of human activity that may arise. And even if we could, such a grand theory would instantly become obsolete as new advances in technology, science, communications, and transportation keep galloping on ahead of the lumbering efforts of law to catch up.

Thus, all I can offer is a set of provisional principles that might guide the development of conflict-of-laws doctrines. These principles, at most, provide a framework for analyzing the knotty conflicts problems that deterritorialized data creates:

*A. The territorial location of data or servers is irrelevant.*

In an era of cloud computing, data can be anywhere. As the *Microsoft Ireland* case<sup>26</sup> makes clear, even a simple e-mail message can be stored in a location completely unrelated to the sender or recipient or even the home of the company that controls the storage. Further, the message might not even be stored in one location; its component data parts could be split among data warehouses within multiple territorial sovereignties. And not only is the location arbitrary, but it is malleable. The data can easily be shifted from place to place instantly and algorithmically, with no human being even making a conscious decision to relocate. Finally, it is the service provider, not the end-user, that ultimately controls the data location. Even if an individual lives all her life in one territorial location and deposits money in her local branch of a multinational financial institution, data related to that account could move anywhere, all based on the data storage scheme of the financial institution.

The arbitrary and malleable nature of data storage wreaks havoc on jurisdictional systems that rely on territorial location. In response, some countries are pursuing legislation that would require the localization of data.<sup>27</sup> Under these statutes, data related to an individual must remain stored within the home country of that individual. This strikes me as precisely the wrong way to go about solving the problem. It seems to me that, if jurisdictional rules do not map well onto the reality of human activity, it's a sign that

---

26. *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016), *cert. granted*, 138 S. Ct. 356 (2017).

27. See Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. J. 677 (2015) (surveying data localization implementation and its effects across various countries).

jurisdictional rules need to change, not that we need to squelch or limit that human activity.

*B. The place of incorporation of a corporation is potentially relevant to the jurisdictional calculus, but should not be determinative.*

Even those who accept that data and server location should not determine jurisdiction may balk at the idea that place of incorporation should similarly not be determinative. After all, we may think that a corporation should be free to choose the state or country by which it is regulated. And certainly sometimes the place of incorporation signals both a substantive affiliation with that jurisdiction and a willingness to submit to that jurisdiction's laws.

Yet, sometimes, place of incorporation is just as arbitrary and manipulated as data or server location. Individuals with no connection with the United States can easily create a U.S. company and then claim protection of U.S. law (and U.S. courts) even though nothing about the dispute at issue really evinces a connection with the United States. Likewise, in the internet taxation context, corporations can choose to incorporate in a foreign jurisdiction and potentially skirt local tax laws even if most of the corporation's revenue derives from that local jurisdiction. Creating a subsidiary can also shield a corporation from liability. For example, the U.S. Supreme Court has refused to permit a state to assert jurisdiction over a foreign parent company selling products locally solely because the sale passed through a third corporation that acted as the U.S. distributor.<sup>28</sup> But the third-party corporation in this case wasn't truly independent; it was essentially just a subsidiary corporation with an exclusive arrangement to distribute the foreign corporation's products in the United States.<sup>29</sup> Thus, if jurisdiction is automatically tied to place of incorporation without any further analysis of the underlying social or economic reality, distortions may result.

*C. Community affiliation is a more plausible basis for legal jurisdiction than contacts with a territorially based sovereign.*

Instead of relying on arbitrary, manipulable, and nonsubstantive connections to a forum, such as data location, server location, or place of incorporation, community affiliation provides a

---

28. See *J. McIntyre Mach., Ltd. v. Nicastro*, 564 U.S. 873 (2011).

29. *Id.* at 896–98 (Ginsburg, J., dissenting).

potentially more appropriate test for jurisdiction and choice of law in the twenty-first century. The question then becomes to what extent have the parties taken steps to associate themselves with a particular community, and to what extent is the lawsuit in question related to the concerns of a particular community?

A community affiliation test provides a more satisfactory way of analyzing cases such as *Microsoft Ireland*. Rather than looking at where the underlying data happens to be located, the relevant question would be the location and/or nationality of the actual user whose information the government wants to search or the corporation from which the government is seeking the information.

*D. Trying to serve a market is a more relevant jurisdictional hook than targeting a territory.*

In a world of deterritorialized data and multinational corporate activity, it can be difficult to determine when a corporation has targeted a particular jurisdiction. For example, were the Yahoo! auction sites that were selling Holocaust denial and Nazi memorabilia material targeting French customers? Or, to ask a different question, was Yahoo.com explicitly targeting French customers? After all, many websites are simply accessible in many different jurisdictions without particularly targeting any one of them. Accordingly, it seems odd if a desire to access a global market would allow a company to avoid jurisdiction in any particular jurisdiction just because no one jurisdiction was explicitly targeted. Yet, that is precisely what a plurality of United States Supreme Court justices would have ruled in the recent case of *J. McIntyre Machinery Ltd. v. Nicaastro*.<sup>30</sup> In that case, the Court overturned the jurisdictional assertion of a state over a corporation. The plurality did so on the ground that the corporation had not explicitly targeted that particular state.<sup>31</sup> But, as the dissent pointed out, the company was aiming to exploit a national market and so the fact that it wasn't targeting any particular state should not deny the state a basis for asserting jurisdiction.<sup>32</sup> Indeed, for a global product offered on an undifferentiated basis to multiple markets, it can be difficult to determine whether the product is truly being targeted anywhere.

In contrast, a community affiliation analysis would allow an inquiry into whether a party is attempting to serve a particular

---

30. See 564 U.S. 873 (2011).

31. *Id.* at 884–85 (Kennedy J., plurality opinion).

32. *Id.* at 893–94 (Ginsburg J., dissenting).



community or market its products there. Thus, community affiliation would provide a more satisfying way of justifying the Belgian assertion of jurisdiction over Yahoo!<sup>33</sup> and Skype<sup>34</sup> or the ECJ<sup>35</sup> or Canadian<sup>36</sup> assertions of jurisdiction over Google. In all of those cases, the service provider is making a sustained effort to access a major commercial market as part of the companies' continuous and systematic global business strategy. Thus, those companies are purposely affiliating themselves with the foreign markets, and regulation by those communities is potentially justifiable.

*E. The size, sophistication, and economic breadth of an actor is relevant to the jurisdictional inquiry.*

As noted previously, since the very first internet jurisdiction cases in the mid-1990s, courts and commentators have struggled with what seem to be two unpalatable jurisdictional options: either jurisdiction is only legitimate where the operator of the website is located or jurisdiction is potentially appropriate wherever the website is viewable. The first option allows for regulatory evasion and the second pushes towards a form of universal jurisdiction. Indeed, part of what concerns commentators about the Belgian court decisions in the Yahoo! and Skype cases is that, as articulated by the courts, the rationale seems to sweep so broadly.<sup>37</sup>

But there is no necessary reason that the hypothetical case of an individual posting on a personal website or Facebook page needs to be treated the same as Yahoo! posting on its homepage. Indeed, as Justice Breyer has recognized, the possible types of internet transaction are so varied that it is difficult to create one overarching rule.<sup>38</sup> He posits a coffee farmer in Kenya selling artisanal coffee online in small quantities and contrasts that with a large multinational industrialist selling thousands of units per year.<sup>39</sup> Even if both products cause harm abroad,

---

33. Public Prosecutor v. Yahoo!, Inc., Hof van Cassatie [Cass.] [Court of Cassation] [Supreme Court of Belgium], Dec. 1, 2015, No. P.13.2082.N (Belg.), *translated in* 13 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 156 (2016).

34. Public Prosecutor 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.), [http://www.wolterskluwer.be/files/communities/legalworld/rechtspraak/2016/Corr.%20Mechelen%2027%20oktober%202016%20\(Skype\).pdf](http://www.wolterskluwer.be/files/communities/legalworld/rechtspraak/2016/Corr.%20Mechelen%2027%20oktober%202016%20(Skype).pdf) [https://perma.cc/C5Z7-EZ9Y].

35. See *Google Spain*, *supra* note 20.

36. Google Inc. v. Equustek Solutions, Inc., [2017] S.C.R. 34 (Can.), <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do> [https://perma.cc/6JE4-GBSU].

37. Daskal, *supra* note 1, at 195.

38. See *J. McIntyre Mach., Ltd. v. Nicastro*, 564 U.S. 873, 891–92 (2011) (Breyer, J., concurring).

39. See *id.*

there is no reason that both defendants need to be treated identically for jurisdictional purposes.

Community affiliation analysis provides a way out of this seeming conundrum. A large industrialist seeking to sell multiple units on a regular basis as part of a global business plan and earning substantial revenue in the process is trying to access a community in a way that is very different from me as a professor posting my thoughts on a personal webpage. Certainly my thoughts may constitute hate speech or libel or copyright infringement in some foreign jurisdiction. But that does not mean that I have affiliated myself with that distant community or in any way sought to access it.

*F. The effects of activities can provide a plausible basis for the assertion of jurisdiction, even without a territorial nexus.*

Notwithstanding community affiliation (or the lack of it), there might be some extreme cases where a community might justifiably wish to assert jurisdiction over a distant act or actor based on the egregious impact of the act on that community. Harm from pollution is the example that immediately springs to mind. It is easy to imagine a company in one country dumping toxic waste into a river, which then flows downstream and causes harm to communities in a different country. In such a circumstance, one can readily imagine the downstream community wishing to assert jurisdiction.

The tricky question is how far to extend this sort of jurisdictional rationale that is based on effects. Taken to an extreme, it could swallow up all the other rules and lead to universal jurisdiction because an act in one place could always potentially cause harm somewhere else. So, as noted above, any assertion of purely effects-based jurisdiction should also consider all the other factors described: community affiliation, effort to exploit a market, size of company, and so on. And although it is impossible to predict all the potential factual settings in which this question may arise, the point is that these factors should at least temper the potential problems associated with jurisdiction based only on effects.

*G. Enforcing a judgment through a powerful intermediary is not inherently illegitimate, but the resulting intermediary enforcement must be regulated, not simply delegated.*

Governments have always enacted regulation through powerful intermediaries. For example, if regulatory authorities want passengers in automobiles to use seat belts, they can regulate seatbelt use directly,

but they can also require automobile manufacturers to have the car make annoying chiming sounds if the car is moving with the seatbelt unbuckled. Such intermediary regulation is likely to be far more effective because it does not require constant surveillance by state actors.

On the other hand, in the context of data intermediaries, the regulation can, as we see in the *Google Spain* case, turn the intermediary into a quasi-adjudicative administrative agency.<sup>40</sup> Such a move solves enforcement issues, because Google can apply the ECJ legal order effectively around the globe without constant monitoring or jurisdictional difficulties. But it leads to two interrelated questions. First, is the burden placed on intermediaries appropriate? And second, might intermediary enforcement regimes lead to overenforcement?

As to the first question, the burden is surely great. In the first two years or so after the ruling was issued, Google reportedly received 528,756 requests and evaluated 1,634,370 URLs for removal.<sup>41</sup> And of course, it's not as if the ECJ criteria provided clear bright lines to apply. Many decisions will therefore require interpretation and careful legal analysis. And parties unhappy with Google's decision can then challenge the decision in court, leading to more expense for Google.

Yet, I am inclined to think that this is simply the cost of doing business when one has essentially become a monopoly common carrier for online search. Certainly, if Google wants to withdraw from the European commercial scene, it could extricate itself from the ECJ judgment, but undoubtedly the company has performed a cost-benefit analysis and decided that it's worth it to continue providing search services to European end-users.

The second question is more troubling. After all, if someone contacts Google to request de-indexing under the ECJ decision, it is surely far easier for Google to err on the side of granting the de-indexing request rather than risk the aggrieved party challenging Google in court. Thus, although the ECJ decision tries to balance individual privacy concerns with the need to maintain free access to truthful information, it is highly likely that, over time, enforcing that balance through Google will tend to err on the privacy side and de-emphasize the countervailing value of protecting public informational access.

---

40. See *Google Spain*, *supra* note 20.

41. Guy Vassall-Adams & Jacob P. Goldstein, Presentation at the MLRC Media Law Conference September 2016: *Google Spain* and the Right to Be Forgotten Two Years Later, 3 (July 2016) (outline available at <http://www.medialaw.org/component/k2/item/3538-google-spain-and-the-right-to-be-forgotten-two-years-later?tmpl=component&print=1>) [<https://perma.cc/U4W2-YQAK>].

For this reason, a decision like the one the Canadian Supreme Court reached in *Equustek*,<sup>42</sup> though structurally similar to the ECJ decision, is less problematic. In that case, the court ordered Google to de-index a defined and limited set of web pages, which Google can do quickly and mechanically without requiring teams of attorneys making interpretive judgments. Moreover, the pages to be de-indexed were sales sites, not principally sites providing public information. Thus, if the ECJ or other courts are going to ask large data intermediaries to have common-carrier-like responsibilities, they must either define the scope of the enforcement order narrowly or provide ongoing oversight, monitoring, and guidance so that the intermediary is not making too many discretionary legal decisions on behalf of government.

*H. Terms of Service agreements will not necessarily resolve jurisdiction and choice-of-law decisions.*

One way of trying to solve knotty online jurisdictional or choice-of-law problems is to fall back on contractual forum selection or choice-of-law clauses. This is a tempting solution, particularly because most interactions between end-users and intermediaries are at least nominally governed by Terms of Service agreements, those “click through” contracts that most users never read, but simply agree to in order to gain entrance to the site they are accessing. If such Terms of Service agreements are enforced, they can solve many potential jurisdictional and choice-of-law problems. But *should* they be enforced? And who gets to make the enforcement decision? It turns out that both of these questions can prove problematic.

To begin, there are many reasons that Terms of Service agreements might not be enforced. First, the agreements are not true bargained-for exchanges. Rather, they are so-called “contracts of adhesion” that are more accurately analyzed as part of the product itself and therefore perhaps subject to a kind of implied warranty of merchantability or a general consumer protection law governing deception.<sup>43</sup> Thus, substantively unfair terms in such a Terms of Service agreement might be deemed unconscionable.<sup>44</sup> Second, some courts will not allow parties to bargain around local law by choosing a foreign forum or foreign law to adjudicate their dispute.<sup>45</sup> Third, courts might recast a jurisdictional dispute as a disagreement about the validity of

---

42. See *Google v. Equustek Solutions*, *supra* note 36.

43. For an argument along these lines, see generally MARGARET JANE RADIN, *BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW* (2014).

44. See, e.g., *Comb v. Paypal, Inc.*, 218 F. Supp. 2d 1165 (N.D. Ca. 2002).

45. See, e.g., RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 187(2)(a).

the Terms of Service agreement itself, which is a disagreement that can be decided based on forum law, not the law called for in the agreement.<sup>46</sup> After all, if the contract is invalid, then so is that contract's forum selection or choice-of-law clause. And fourth, courts might recast the dispute in the case as a tort or an issue of criminal law or evidence or some other noncontractual regime.<sup>47</sup> Once recharacterized in this way, the dispute becomes one that can be decided without reference to any contractual agreement.

Beyond the question of whether the contract will be enforced is the additional uncertainty regarding which court is even making the enforcement decision in the first place. After all, the four inquiries summarized above concerning the validity of the Terms of Service agreement are all likely to be made by the forum court using local law (that is, the court and law the plaintiff chose) regardless of what the forum selection or choice-of-law clauses say. This is because, again, the initial determination of contract validity cannot be made using the contract's own forum selection or choice-of-law clause; that would require assuming the validity of the contract, the very issue that is being questioned.

*I. The decision regarding whether to enforce another jurisdiction's judgment is not the same as the decision regarding whether to issue that judgment in the first instance.*

When faced with an enforcement decision regarding a foreign judgment, courts should not necessarily assume that their own local public policies trump the dictates of the foreign judgment. Instead, courts must undertake a nuanced inquiry concerning whether the affiliations of the parties render the original court judgment legitimate. Although the local policies of the forum country are not irrelevant, those policies should be weighed against the overall systemic interest in creating an interlocking system of international adjudication.

This is not so different from what courts within federal-style systems already do in domestic cases raising judgment recognition issues. For example, the United States Supreme Court has long held that states cannot refuse to enforce sister-state judgments on the ground that doing so would violate the rendering state's public policy.<sup>48</sup>

---

46. See, e.g., Kevin M. Clermont, *Governing Law on Forum-Selection Agreements*, 66 HASTINGS L.J. 643 (2015) (discussing this issue).

47. See, e.g., *Melia v. Zenhire, Inc.*, 462 Ma. 164 (2012) (using state Wage Act law to govern employment contract rather than the law specified in the contract).

48. See *Baker v. Gen. Motors Corp.*, 522 U.S. 222, 233 (1998) (making clear that there is no public policy exception to the full faith and credit due judgments).

Likewise, the ECJ has attempted to lay down a strong rule of judgment recognition that allows courts to interpose only *European* public policies to avoid recognizing the judgment of another member state, not their own parochial public policies.<sup>49</sup>

Of course, within a single, relatively homogenous country, the idea of one state enforcing another state's judgment does not seem quite so significant because the variations from state to state are likely to be relatively minor. Yet, while the decision to enforce a judgment surely will be less automatic when the judgment at issue was rendered by a court of a different nation-state, many of the same principles still are relevant. Most importantly, what we might call "conflicts values" should be part of the judgment recognition calculus. Thus, courts should acknowledge the importance of participating in an interlocking international legal system, where litigants cannot simply avoid unpleasant judgments by relocating. Indeed, there is no need for inherent suspicion of foreign judgments. Certainly deference to other courts will have long-term reciprocal benefits. And, particularly when the parties have no significant affiliation with the forum state, there is little reason for a court to insist on following domestic public policies in the face of such competing conflicts values.

This is not to say, of course, that foreign judgments should always be enforced. Indeed, even in a cosmopolitan system, one would expect that judges might sometimes interpose local public policies where they would not in the domestic state-to-state setting. But if we acknowledge the importance of the conflicts values effectuated by strong judgment recognition, we will necessarily reject the idea that a court is simply *unable* to enforce a judgment just because such a judgment could not have been issued by the court in the first instance. Instead, we will appreciate that enforcing a foreign judgment is fundamentally different from issuing an original judgment; indeed, judgment recognition implicates an entirely distinct set of concerns about the role of courts in a multijurisdictional world.

#### CONCLUSION

Of course, these nine principles, neither taken on their own nor in combination, will completely solve the conflicts problems raised by the increasing deterritorialization of data. Indeed, there are no perfect

---

49. See *Joined Cases C-404/15 & C-659/15 PPU, Pál Aranyosi & Robert Caldaru v. Generalstaatsanwaltschaft Bremen*, 2016 E.C.R. 198, <http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d0f130d57f798913232b45cabe6aab2cf36bb51b.e34KaxiLc3eQc40LaxqMbN4PaNqRe0?text=&docid=175547&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=253357> [https://perma.cc/2H7U-7BT4].

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, 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. As Daskal's article makes clear, the deterritorialization of data requires us to think differently about law's attachment to physical objects in physical space as the basis for legal jurisdiction. And as we enter the next two decades of legal scholarship surrounding the internet, it is clear that the fundamental challenges identified in the late 1990s are still in flux. Thus, the new settled expectations that may ultimately emerge are at this moment still contested and uncertain. Creative scholars such as Daskal and others will therefore need to keep pushing for new approaches that bring our system of law into better dialogue with our ever-changing social reality.