Catholic University Journal of Law and Technology

Volume 27
Issue 2 *Spring 2019*

Article 5

2019

Legal Jurisdiction and Virtual Social Life

Paul Schiff Berman
George Washington University Law School

LEGAL JURISDICTION AND VIRTUAL SOCIAL LIFE

Paul Schiff Berman[*]

I. INTRODUCTION

Social lives are increasingly unmoored from physical location. This "virtualization" arises in part from successive waves of technological innovation that have repeatedly transformed human conceptions of space, place, and proximity. In the 19th and 20th centuries, new developments in rail, automobile, and airplane travel shrank the sense of physical distance.[1] Communications technologies such as the telegraph, the telephone, and the Internet allowed data to move across territorial boundaries with increasing ease. And 21st century

[*] Walter S. Cox Professor of Law, The George Washington University. Some material in this Essay is derived from Paul Schiff Berman, *Legal Jurisdiction and the Deterritorialization of Social Life*, *in* RESEARCH HANDBOOK ON THE LAW OF VIRTUAL AND AUGMENTED REALITY (2019), and Paul Schiff Berman, Yahoo! v. LICRA, *Private International Law, and the Deterritorialization of Data*, *in* GLOBAL PRIVATE INTERNATIONAL LAW: ADJUDICATION WITHOUT FRONTIERS (Horatia Muir Watt et al. eds., 2019).

1 *See generally* Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 425-32 (2002) (discussing legal jurisdiction and changing social conceptions of space, place, and distance).

developments in social media, virtual worlds, augmented reality, electronic financial transactions, drones, robotics, and artificial intelligence allow human beings to interact in more and more robust ways at a physical remove from their location. Meanwhile, the ubiquity of multinational corporations, global supply chains, and cloud-based data all mean that our lives are more likely to be affected by activity that is spatially distant. Virtual effects often replace direct territorial effects.

As a thought experiment, one can imagine an "effects map," in which one identifies a territorial locality and plots on a map every action that has an effect on that locality.[2] Five hundred years ago, such effects would almost surely have been clustered around the territory, with perhaps some additional effects located in a particular distant imperial location. One hundred years ago, those effects might have begun spreading out. But today, while locality is surely not irrelevant, the effects would likely be diffused over many corporate, governmental, technological, and migratory centers.

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.[3] As a result, our virtual lives are often controlled less by governments and more by private corporations that own the platforms upon which our virtual lives are based.[4]

Three important consequences flow from this ubiquitous technology-enabled, data-driven virtual global societal activity. First, the territorial location of data becomes increasingly arbitrary and substantively unimportant. If I, as a United States 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 virtualization of social life and

---

2 David G. Post, *"Against Cyberanarchy,"* 17 BERKELEY TECH. L.J. 1365, 1381-83 (2002) (articulating this thought experiment).

3 *See infra* Section 3.

4 *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTION OF INFORMATIONAL CAPITALISM (forthcoming, 2019); MOLLY K. LAND, THE PROBLEM OF PLATFORM LAW: LEGAL PLURALISM ON SOCIAL MEDIA PLATFORMS, THE OXFORD RESEARCH HANDBOOK ON GLOBAL LEGAL PLURALISM (Paul Schiff Berman ed., 2019, forthcoming).

deterritorialization of data, territorially based courts (or law enforcement authorities generally) will sometimes be less able to enforce their decisions because those decisions require cooperation from relevant actors in far-flung communities.[5] 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.[6] 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.

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 private international 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 private international law in the Information Age, it's not at all clear that everyone would agree on what that theory should be. "Thus, as legal pluralists have long realized, there is never a stable 'solution' to the reality of legal pluralism."[7] 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."[8]

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 increasing virtualization of social life. This Essay aims to do that, providing a series of real-life case studies that any consideration of 21st century conflict-of-laws jurisprudence must face.

---

5 For example, if a Canadian court issues an order against a company for trademark infringement, but that company has no presence in Canada, that Court order will either need to be enforced by the courts in the company's home country or by some third party, such as Google. *See* Google Inc. v. Equustek Solutions, Inc., [2017] 1 S.C.R. 824 at 829-30 (Can.).

6 Paul Schiff Berman, Yahoo! v. LICRA, *Private International Law, and the Deterritorialization of Data*, *in* GLOBAL PRIVATE INTERNATIONAL LAW, ADJUDICATION WITHOUT FRONTIERS 392 (Horatia Muir Watt et al. eds., 2019).

7 *Id*.; *see generally* Paul Schiff Berman, *The New Legal Pluralism*, 5 ANN. REV. OF L. & SOC. SCI. 225, 226 (2009) (discussing the history of legal pluralism).

8 Berman, Yahoo! v. LICRA, *Private International Law, and the Deterritorialization of Data*, *supra* note 6; *see generally* PAUL SCHIFF BERMAN, GLOBAL LEGAL PLURALISM: A JURISPRUDENCE OF LAW BEYOND BORDERS (2012) (discussing legal pluralism from both a descriptive and normative perspective).

II. ONLINE SPEECH[9]

Many of the earliest debates about jurisdiction and online virtual interaction involved issues of speech, where the speech in question was legal in one location, but illegal in another.[10] The paradigmatic case involved Yahoo.com. Indeed, it is fitting that this most famous legal dispute of the early internet era implicated all three conflict-of-law 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 prevent access in France to Yahoo! auction sites that sell Nazi memorabilia or other items that are sympathetic to Nazism or constitute Holocaust denial.[11] Undisputedly, selling such merchandise in France would violate French law, 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 the late 1990s 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.[12] 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.[13]

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

---

9 Material in this section was published in *Legal Jurisdiction and the Deterritorialization of Data*, 71 VAND. L. REV. en banc 11, 18-19 (2018); *see also* Berman, Yahoo! v. LICRA, *Private International Law, and the Deterritorialization of Data*, *supra* note 6, at 394-96.

10 The *Yahoo!* Case was one of many. *See* Paul Schiff Berman, *The Globalization of Jurisdiction*, *supra* note 1, at 412-20 (2002) (discussing the early internet cases).

11 LICRA v. Yahoo!, Inc., Tribunal de Grande Instance de Paris [TGI] [High Court of Paris] France, Paris, May 22, 2000, J. Gomez (Fr.), https://perma.cc/738B-V9BM (Richard Salis, trans.).

12 *Id*.

13 *Id*.

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 over yahoo.com was impermissibly extraterritorial in scope.[14]

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 had the right to access the materials under the laws of their countries.[15] Most importantly, Yahoo! argued that such extraterritorial censoring of American web content would run afoul of the First Amendment of the U.S. Constitution.[16] Thus, Yahoo! and others contended that the French assertion of jurisdiction was an impermissible attempt by France to impose global rules for internet expression.[17] 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."[18]

Yet, it is easy to see that the extraterritoriality charge runs in both directions. If France were *not* able to block the access of French citizens to proscribed material, then the United States would 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 have subsequently seen repeated in case after case. 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

---

14 *Id*.

15 *Id*.

16 *Id*.

17 Carl S. Kaplan, *Experts See Online Speech Case as Bellweather*, N.Y. TIMES (Jan. 5, 2001), http://www.nytimes.com/2001/01/05/technology/experts-see-online-speech-case-as-bellwether.html.

18 *Id*.

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 is irrelevant to the underlying jurisdictional issues at stake.

In the end, Yahoo! "voluntarily" complied with the French court order,[19] but simultaneously filed suit in United States 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.[20] 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 United States law (and United States constitutional norms) must apply.[21] Thus, the court framed the issue for decision solely in U.S. 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."[22]

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.[23] The court therefore concluded that a United States court could not have issued such an order in the first instance without violating constitutional free speech norms.[24] But of course, in a judgment recognition case, that is not the appropriate inquiry. Indeed, in the domestic context the US Constitution's 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.[25] Thus, the real question should have been whether this was the type of judgment that should have been *recognized*, not whether the court could have issued the ruling *as an*

---

19 Lisa Guernsey, *Yahoo to Try Harder to Rid Postings of Hateful Material*, N.Y. TIMES (Jan. 3, 2001), https://www.nytimes.com/2001/01/03/business/technology-yahoo-to-try-harder-to-rid-postings-of-hateful-material.html.

20 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).

21 *Id*. at 1187.

22 *Id*. at 1186.

23 *Id*. at 1189-90.

24 *Id*.

25 *See, e.g.*, Fauntleroy v. Lum, 210 U.S. 230, 237 (1908) (holding that the judgment of a Missouri court was entitled to full faith and credit in Mississippi even if the Missouri judgment rested on a misapprehension of Mississippi law).

original matter.

To its credit, the district court did include a brief discussion of the judgment recognition issue in a section titled "Comity."[26] 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."[27] Yet, after reiterating that the French judgment "clearly would be inconsistent with the First Amendment if mandated by a court in the United States,"[28] the district court judge concluded that, because the foreign order would unconstitutionally chill speech occurring within U.S. borders, "the principle of comity is outweighed by the Court's obligation to uphold the First Amendment."[29]

Thus, while ostensibly addressing principles of judgment recognition, the court ultimately returned to the idea that whenever 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 U.S. interests might *not* truly be threatened by the application of a foreign norm.[30]

An en banc panel of the Ninth Circuit ultimately reversed, on other grounds, by a 6-5 vote.[31] 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.[32] The other three judges making up the majority also dismissed, but did so on ripeness grounds, similarly concluding that the enforcement issue should not be decided until the French defendants actually sought enforcement.[33] Thus, the Court of Appeals majority never addressed the judgment recognition issues upon which the district court had relied.

Lest we think that this case from the early years of the 21st century represents simply the growing pains associated with applying law to a new technology, it is worth considering the following group of more recent cases. Indeed, because

---

26 La Ligue Contre Le Racisme et L'Antisémitisme, 169 F.Supp.2d at 1192-93.

27 *Id*. at 1192.

28 *Id*.

29 *Id*. at 1193.

30 *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) (discussing further various issues of judgment recognition).

31 Yahoo!, Inc., v. La Ligue Contre Le Racisme et L'Antisémitisme, 433 F.3d 1199, 1201 (9th Cir. 2006).

32 *Id*.

33 *Id*.

more and more of our social identity is now stored remotely by third parties, far from our physical location, very little of our data identity actually remains tied to our person anymore. This increasing virtualization of social life 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.

III. VIRTUAL WORLDS

Where is a virtual world for jurisdictional purposes? The answer depends in part on your perspective.[34] From within the world itself, it feels like one is somewhere else. Think of the spatial set of metaphors. This is a "world." One "goes to it" or "enters it." From this perspective, a virtual world is a new community of individuals unbound by their literal physical location, "meeting" and forming a set of community bonds that could be stronger than the bonds they feel with their physically-oriented communities.

On the other hand, for one external to the virtual world watching the participants, there is no world at all, just a large number of people located somewhere in physical space, looking at computer screens. Regardless of what sort of interactions they are having online, from this perspective these people are always bound to hundreds of separate territorially-based communities and therefore subject to the legal jurisdiction of those communities.

Given the relationship between the social experience of community and the legal definition of community, this difference of perspective matters. If one sees the relevant community affiliation as the in-game community, then the law of that community is established through the software code built into the world by the designer, the rules of behavior dictated by the game itself, the end-user license agreement (or EULA), and the social norms of that virtual world. In contrast, if the relevant community affiliation is the territorial location of its users, then a slew of national laws governing speech, depictions of violence, gambling, sexualized imagery, and so on might apply.

Or, one could try to divide up the jurisdictional pie. Virtual world designers and distributors could be subject to the law of their corporate headquarters, while users could be subject to the jurisdiction of their home countries. However, experience shows that governments are unlikely to be satisfied going after only end-users. The larger corporate actor profiting from the activity makes for a much more palatable (and easier to find) target.

For example, consider the Yahoo! case discussed above. Undeniably, the

---

34 *See* James Grimmelmann, *Virtual Borders: The Interdependence of Real and Virtual Worlds*, 11 FIRST MONDAY 1, 3 (2006); Orin Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 357 (2003).

French end users were violating French hate speech law and could be prosecuted. But those individuals were difficult to find, and prosecuting a few might well be futile because more would likely take their places. Thus, it is not surprising that French prosecutors focused on Yahoo! itself. And while today's technology makes it far easier for websites to track the physical location of users than in 2000, the essential problem for virtual world designers remains: will they potentially face liability for content of their virtual spaces based on the laws in the jurisdiction of each end-user? And even if they can track where those end-users are, altering the elements of the virtual world to accord with each jurisdiction's laws may be difficult.

The EULA could, in theory, solve such jurisdictional and choice-of-law problems by imposing a uniform set of rules on all end-users, regardless of where they are in the world. Yet, EULAs have three possible shortcomings. First, because the EULA is a contract, it is potentially subject to local contract law. And even if the EULA contains a choice-of-law clause, it is possible that a court would override that clause by invalidating the contract itself as unconscionable or a violation of local public policy. Second, because the EULA is a contract between the game designer/distributor and each user, it might not cover torts one user suffers in a virtual world due to the acts of another user. And third, the EULA similarly would not apply if a local regulatory authority claimed that criminal behavior was taking place in the virtual world, which of course could include acts criminal in one jurisdiction but not necessarily in others.

Virtual worlds and territorially-based sovereignties also potentially are forced to interact because objects and attributes in virtual worlds may have market value outside of the virtual world, setting up the possibility of transactions that territorially-based authorities (and game designers themselves) may wish to regulate.[35] For example, in many virtual worlds, avatars that possess certain objects or territory or have acquired certain experience can gain access to parts of the world others cannot, or they can do tasks or perform feats that others cannot.[36] As such, these objects or territories or attributes have value to those immersed in the world. And of course, markets will almost inevitably arise to allow the buying and selling of nearly anything human beings value.

As long as that market operates only within the virtual world itself, exchanges are likely to be governed by in-world code, rules, and the EULA. But as soon as two people exchange virtual items in-world while paying each other using PayPal or Bitcoin or a credit card or a check, then territorially-based authorities may well see the transaction as similar to any other and therefore within their regulatory jurisdiction. If the parties are from different countries, we might have

---

35 *See* Grimmelmann, *supra* note 34, at 2.

36 *Id*. at 3.

a choice-of-law or jurisdictional problem, just as we would with any other cross-border commercial transaction. But perhaps the law of the virtual world could be deployed by a court as a touchstone for adjudicating the dispute. For example, we might see courts using some idea of comity to defer to the norms of the virtual world, just as courts sometimes use comity to defer to norms of other jurisdictions even when not literally obligated to do so.

Of course, the dispute may not only be between two end-users. What if the designer of the virtual world objects to the creation of this market, or demands to have some power over the transaction, or a financial cut?[37] We might then see claims based on property rights in the servers on which virtual worlds run.[38] Or perhaps the designer could argue that the players are accessing the designer's computer systems without authorization for a non-permitted use.[39] The trade could also violate the EULA, spurring a contract claim. Or the market in virtual goods could be violating the designer's trademark or copyright. Each of these claims would likely be pursued in a territorially-based court, invoking territorially-based law.

Finally, an end-user might bring suit against a game designer/operator. In *Bragg v. Linden Research*, for example, a user sued the operator of Second Life because the operator nullified a transaction involving virtual property.[40] The federal district court determined that Pennsylvania could assert jurisdiction even though the defendants were not from the state because a nationwide advertising campaign had explicitly encouraged people to join Second Life in part by promising them the ability to take ownership of virtual property.[41] In addition, Second Life had accepted payment from the plaintiff knowing the plaintiff was in Pennsylvania.[42] If such contacts are sufficient than it is not at all far-fetched to think that suits against operators of virtual worlds could well be brought anywhere a user is located. Moreover, it is worth noting that the court also did not honor the Terms of Service governing Second Life—which dictated mandatory arbitration and other provisions—because the contract was ruled to

---

37 *Id*. at 4.

38 *See, e.g.*, Intel Corp. v. Hamidi, 1 Cal. Rptr. 3d 32, 67 (2003) (recognizing a trespass theory for unauthorized use of computer system).

39 *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C) (2012) (establishing criminal and civil liability for "knowingly access[ing] a protected computer without authorization, or exceed[ing] authorized access"); *see also, e.g.*, Orin Kerr, *Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1598-99 (2003).

40 Bragg v. Linden, 487 F.Supp.2d 593, 595 (E.D. Pa. 2007).

41 *Id*. at 600.

42 *See id*. at 599 (noting Circuit precedent that if the defendant knowingly conducts business with forum state residents via a website, then the ''purposeful availment'' requirement is satisfied).

be unconscionable and therefore invalid.[43] This case therefore illustrates both the potential for broad assertions of jurisdiction against virtual world operators and the possibility that local law could be deployed to displace EULAs.

In contrast, in *Mason v. Machine Zone, Inc.*, a court refused to find a cognizable claim regarding in-game property.[44] In *Mason*, the plaintiff tried to bring a class action lawsuit against a game operator who sold in-game "gold" for real dollars and then allowed players to gamble the gold at an in-game casino.[45] The plaintiff alleged that the algorithms controlling the games of chance in the online casino were deliberately rigged against users, making it more likely that they would squander the gold that they had purchased (and presumably make them more likely to purchase yet more in-game gold to replace what they lost).[46]

Interestingly, the court did not take seriously the idea that being deprived of virtual currency could be a valid legal claim even if that currency were purchased with real dollars. According to the court, "Perceived unfairness in the operation and outcome *of a game*, where there are no real-world losses, harms, or injuries, does not and cannot give rise to the award of a private monetary remedy *by a real-world court*."[47] As formulated by the court, this statement seems potentially plausible, but the whole point of the claim in *Mason* rested on the fact that there *were* "real-world losses, harms, or injuries," namely the dollars the plaintiffs spent on the in-game gold that was then allegedly stolen from them through a rigged algorithm. To take it out of a game context, if an individual purchases Bitcoins using dollars and then is swindled out of the Bitcoins by a Bitcoin exchange vendor, it seems unlikely that a court would dismiss such a claim as not alleging any real-world harm. Indeed, as we will see, in a case presenting just such an issue, a court did in fact find a potentially valid cause of action.

Thus, the "where" question in disputes involving virtual worlds remains contested. Users could be deemed in the world or outside of it, and if outside then we need to answer the further question of which community affiliation is the most salient for jurisdictional and choice-of-law purposes.

IV. CLOUD-BASED DATA

In a sense, of course, many people live at least part of their lives in virtual worlds whether they choose to or not. This is because more and more of our

---

43 *Id*. at 607.

44 Mason v. Mach. Zone, Inc., 140 F.Supp.3d 457, 459 (D. Md. 2015), *aff'd*, 851 F.3d 315 (4th Cir. 2017).

45 *Id*. at 458-59.

46 *Id*. at 460.

47 *Id*. at 459.

social identity is stored remotely, far from our physical location. Whether it be our e-mails, our social media posts, our musical preferences, our virtual world activities, our online search histories, our photographs, 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 virtualization of identity create conundrums for jurisdiction and choice of law.

For example, in 2013 US officers conducting a criminal drug investigation sought a search warrant under federal law to seize the e-mails of a Microsoft customer.[48] 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.[49] And in fact Microsoft did turn over all account information it had that was being stored in the United States.[50] However, the actual emails, and their contents, were stored overseas in Dublin, Ireland.[51] 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.[52]

The U.S. Court of Appeals for the Second Circuit agreed,[53] albeit reluctantly.[54] Applying the presumption against extraterritoriality, the court determined that because Congress had not, in the Stored Communications Act,[55] contemplated cloud-based data storage and because it had used the word "warrant" instead of "subpoena," the Act had made no provision for subpoenas

---

48 Microsoft v. United States, 829 F.3d 197, 200 (2d Cir. 2016), *vacated as moot and remanded*, 138 S. Ct. 1186 (2018).

49 See *Developments in the Law — More Data, More Problems*, 131 HARV. L. REV. 1715, 1722 (2018) ("Facebook received 32,716 requests for information from U.S. law enforcement between January 2017 and June 2017. These requests covered 52,280 user accounts and included 19,393 search warrants and 7632 subpoenas. In the same time period, Google received 16,823 requests regarding 33,709 accounts, and Twitter received 2111 requests regarding 4594 accounts. Each company produced at least some information for about eighty percent of requests.").

50 *Microsoft*, 829 F.3d at 200.

51 *Id*.

52 *Id*. at 200-01.

53 *Id*. at 201.

54 *Id*. at 200 (Lynch, J., concurring) ("Despite ultimately agreeing with the result in this case, I dwell on the reasons for thinking it close because the policy concerns raised by the government are significant, and require the attention of Congress."); The Second Circuit denied the government's motion to rehear the case en banc by a four-to-four plurality. Microsoft Corp. v. United States, 855 F.3d 53, 54 (2d Cir. 2017) (en banc); All four dissenting judges wrote separate opinions expressing their disagreement with both the legal conclusions of the panel decision and its potential ramifications. *See id*. at 60 (Jacobs, J., dissenting); *id*. at 62 (Cabranes, J., dissenting); *id*. at 69 (Raggi, J., dissenting); *id*. at 74 (Droney, J., dissenting).

55 18 U.S.C. §§ 2701–2712 (2012).

to apply beyond U.S. borders.[56] Significantly, the physical location or the nationality of the underlying 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 e-mail records of a US citizen located in the United States who sent e-mails to other US citizens from a computer located in the United States. The only relevant territorial nexus appears to be where the e-mail 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.[57] 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.[58] Accordingly, even if US law enforcement sought the data through 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.[59] And given that Google can move customers' data at will around the globe, the court concluded that forcing Google to reterritorialize the data in the United States does not violate any privacy interest.[60] Then, once the data is repatriated the warrant can issue just as it would in any other domestic situation.[61]

In order to resolve the ambiguity caused by these conflicting court decisions, the US Congress in 2018 enacted the CLOUD Act.[62] 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.[63] Thus, the statute sensibly looks at the underlying community affiliation of the user rather than the arbitrary territorial

---

56 *Microsoft*, 829 F.3d at 209, 212.

57 *In re* Search Warrant No. 16–960–M–01 to Google, 232 F.Supp.3d 708, 708 (E.D. Pa. 2017).

58 *Id.* at 724.

59 *Id.* at 719-22.

60 *Id.* at 721.

61 *Id.* at 722.

62 CLOUD Act, H.R. 4943, 115th Cong. (2018).

63 CLOUD Act, H.R. 4943, 115th Cong., § 103(a)(1) (2018), codified at 18 U.S.C. § 2713 (2018).

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.[64] This caveat still seems to unduly reify the physical location of data even though that physical location may be arbitrary and completely unrelated to the social reality of the person whose data is at issue.

V. ONLINE SEARCH

As with data, online searches are part of our social identity. And, as with data, searches are fundamentally virtual, 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 took this approach in a case involving Google.[65] A 1995 European Council data privacy directive had recognized that individuals possess privacy rights in data.[66] 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.[67]

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.[68] Moreover, again as with the *Yahoo!* case, the European Commission deemed it insufficient only to apply its ruling to google.es, the Spanish subsidiary, instead determining that google.com must also block offending websites from its search results.[69]

---

[64] CLOUD Act, H.R. 4943, 115th Cong., § 103(b) (2018), codified at 18 U.S.C. § 2703(h)(2) (2018).

[65] Google Spain SL v. Agencia Española de Protección de Datos, Case C-131/12 (May 13, 2014), http://perma.cc/ED5L-DZRK.

[66] Council Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data and on the Movement of such Data, 1995 O.J. (L 281) 31 (EC).

[67] *Google Spain SL*, Case C-131/12, ¶¶ 94.

[68] *Id*. at ¶¶ 80-83.

[69] *See* EC Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on* Google Spain v. AEPD, Nov. 26, 2014, https://perma.cc/AR4M-KS5L, at 3.

By making Google responsible for enforcing this so-called "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.[70] 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.[71] If the individual disagrees with Google's decision, then that decision can be challenged through local Data Protection Authorities and, presumably, in court.[72] Given that Google is constantly altering its search algorithms anyway, one can understand 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).

More recently, a 2017 Canadian Supreme Court decision[73] reprises many of the elements we saw in the *Google Spain* case. 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.[74] Equustek claimed that Datalink had begun to re-label one of Equustek's products in order to sell the product as its own.[75] 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.[76]

Thus, we see an inherent difficulty a territorially-based sovereign may face 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

---

70 *Id*. at 6-7 (laying out process under which individuals may request de-listing).

71 *Id*. at 7 (discussing the assessment process of search engines in response to a de-listing request); *Id*. at 10 ("[T]he Working Party strongly encourages the search engines to publish their own de-listing criteria….").

72 *Id*. at 11 (discussing claims brought by data subjects to Data Protection Authorities).

73 Google Inc. v. Equustek Solutions, Inc., [2017] 1 S.C.R. 34 at 34 (Can.).

74 *Id*.

75 *Id*.

76 *See id*. ("Despite court orders prohibiting the sale of inventory and the use of [Equustek's] intellectual property, [Datalink] continues to carry on its business from an unknown location, selling its impugned product on its websites to customers all over the world.").

courts would turn to Google, just as the European Court of Justice did in the "right to be forgotten" context.[77] As in that case, the court 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. Following the court order against Datalink and a request from Equustek, Google agreed to de-index some but not all of Datalink's webpages so that they would not be found if they were being searched for on Google's Canadian site, google.ca.[78] However, those same pages could still be found by searching on google.com or other countries' Google search sites.[79] Thus, as with the blocking of Nazi memorabilia only on yahoo.fr, the Canada-specific remedy was insufficient.

Equustek therefore sought a preliminary injunction against Google requiring the company to de-index Datalink's websites through any of its search portals worldwide.[80] Google argued in response that such an injunction would be improperly extraterritorial as it would mean that Canada's judgment would dictate search results around the world.[81]

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.[82]

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 non-party to the suit, to act as its global enforcement mechanism, just as the ECJ had in the *Google Spain* case.

Significantly, unlike the French *Yahoo!* 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.[83] Moreover, if the websites to be de-indexed were in fact infringing trademark, de-indexing them would be unlikely to be the basis for a successful First

---

77 *See supra*, text accompanying notes 65-72.
78 *Equustek Solutions, Inc.*, 1 S.C.R. at 34.
79 *Id*.
80 *Id*.
81 *Id*.
82 *Id*.
83 *See* Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of New York, 447 U.S. 557, 557 (1980).

Amendment claim. And of course, because Datalink is not a U.S. corporation, it is not clear the company would have valid First Amendment rights to assert in any event. And as to Google, it is an open question whether search results count as speech for First Amendment purposes.[84] Nevertheless, despite the lessened First Amendment concerns at stake, Google took the same path that Yahoo! had 16 years earlier, filing for a declaratory judgment in a US court that would declare the Canadian judgment unenforceable under US law.[85] 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.[86] And, as in the *Yahoo!* case, the District Court granted the Declaratory Judgment.[87]

The U.S. 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.[88] 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.[89] This is particularly so given

---

84 *Compare, e.g.*, Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495, 1498 (2013) ("Too much protection would threaten to constitutionalize many areas of commerce and private concern without promoting the values of the First Amendment."), *with* Stuart Minor Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1445, 1447 (2013) ("[I]f we accept Supreme Court jurisprudence, the First Amendment encompasses a great swath of algorithm-based decisions—specifically, algorithm-based outputs that entail a substantive communication."). At least two district courts have ruled that search results qualify as speech for First Amendment purposes. *See* Jian Zhang v. Baidu, 10 F.Supp.3d 433, 439-40 (S.D.N.Y. 2014); Search King v. Google, No. CIV-02-1457-M, 2003 WL 21464568, at *4 (W.D. Okla. May 27, 2003), while one district court has ruled that Google's decision to de-list a website based on the site's failure to comply with Google policies was, unlike an algorithm that ranks results, capable of being proven true or false and thus was *not* protected by the First Amendment. *See* eVentures Worldwide v. Google, 188 F.Supp.3d 1265, 1274 (M.D. Fla. 2016). To date, there has been no federal appellate or Supreme Court decision addressing the extent of First Amendment protection afforded to search results.

85 *See* Google v. Equustek Solutions, No. 5:17-cv-04207, 2017 WL 5000834, *1 (N.D. Cal. Nov. 2, 2017).

86 47 U.S.C. § 230 (2012).

87 *Equustek Solutions*, 2017 WL 5000834, *1.

88 *See supra*, text accompanying notes 31-33.

89 *See supra*, text accompanying notes 25-30.

that most of the First Amendment concerns in the *Yahoo!* case were not present here.

In the end, although the district court's declaratory judgment order (assuming it stands) 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 ultimately 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.

Ultimately, these cases not only illustrate 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, these intermediary companies, those companies are likely to become the brokers that territorially-based governments use to pursue regulation. And of course, the increasing power those companies have over data means that they will often be the target of complaints by individuals.

VI. VIRTUAL COMMUNICATION

Intermediaries also enable our virtual communication over media such as Skype, Google Hangouts, Zoom, and so on. This too raises questions about how much information those intermediaries collect and are required to disclose.

For example, Belgian authorities in 2009, seeking to require Yahoo! to disclose subscriber information about Yahoo! users as part of a fraud investigation, reprised certain arguments made during the French efforts against Yahoo! a decade earlier.[90] And Yahoo! once again argued that the application of the Belgium statute to a company without a physical presence in Belgium was impermissibly extraterritorial.[91] Moreover, Yahoo!'s argument was perhaps even more compelling than in the earlier 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.[92]

---

90 Public Prosecutor v. Yahoo!, Inc., Cours d'Appel [CA] Hoven van Beroep [HvB] [Court of Appeal], Nov. 20, 2013, 2012/CO/1054 Yahoo! Inc. (Belg.), *translated in* 11 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE L. REV. 137, 137 (2014).

91 *Id*. at 141.

92 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, 158 (2016).

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 service provider that actively directs [its] economic activity to consumers in Belgium," regardless of whether or not the operator or provider has a physical presence in Belgium.[93] In addition, the court reasoned that enforcing the law would not require Belgian authorities to act extraterritorially because the statute at issue did not "require Belgian police officers or magistrates, nor [any] persons acting on their behalf to be physically outside the jurisdiction."[94] From this perspective, the authorities were simply staying in Belgium asking for data to be provided by Yahoo!. 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.[95]

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.[96] Skype complied with regard to registration information, but argued that because Skype is a Luxembourg company there was no jurisdiction in Belgium.[97] Instead, according to Skype, any request for communications content must proceed via a mutual legal assistance request of the Luxembourg government.[98]

The Belgian court rejected this argument. The court ruled that, even though Skype was based in Luxembourg, it was "target[ing] Belgian consumers on the Belgian economic market" by offering services there and was therefore subject to Belgian jurisdiction.[99] 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.[100]

---

93 *Id*. at 157.

94 *Id*.

95 *Id*.

96 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.), https://perma.cc/C5Z7-EZ9Y.

97 *Id*.

98 *Id*.

99 Carly Page, *Microsoft Forced to Pay eur30k Fine for Refusing to Hand Over Skype Data*, THE INQUIRER (Nov. 16, 2017), https://perma.cc/7GDS-M9BA.

100 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*

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 "actively directs economic activity to consumers in 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 recalls early internet jurisdiction cases in the United States that asserted jurisdiction over websites wherever they were viewed or viewable, conceptualizing a website as a 24-hour-a-day advertisement "entering" every jurisdiction where the website was accessible.[101]

VII. GLOBAL ELECTRONIC CURRENCIES AND TRANSACTIONS

Although the global alternative currency Bitcoin has generated the most attention, it is only one instantiation of a more general ledger technology known as blockchain.[102] Blockchains store data in distributed computers and chain them together to form an unbroken record of that information.[103] 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 world.[104] Any change to information on one is immediately and automatically authenticated by the others, and any authenticated change immediately updates on all computers in the chain.[105] Second, the information is encrypted so that, in combination with its decentralization, it is difficult to hack.[106]

---

in 13 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 156, 157 (2016).

101 *See, e.g.*, Inset Systems. Inc. v. Instruction Set, Inc., 937 F.Supp. 161, 165 (D. Conn. 1996).

102 *See, e.g*., Louis F. Del Duca, *The Commercial Law of Bitcoin and Blockchain Transactions*, 47 No. 2 UCC. L. J. Art 4, 1 (2017) ("A blockchain is a distributed database, with entries verified by parties on the blockchain, using public encryption. Bitcoin and other public blockchains permit reliable identification of every transaction that has occurred on the blockchain.").

103 *See id*.

104 *See id*. at 4-5. ("A blockchain . . . allows anyone interested to see what valid transactions have occurred, allows free access without permission of a bank or government, and could be more efficient than having all the parties keep separate ledgers or sets of books.").

105 *See id*. (describing how Bitcoin, and blockchains more generally, work).

106 *See id*. at 12.

On the other hand, those same features make blockchains potentially difficult to regulate. Not only do blockchain transactions cross borders, but it will often 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."[107]

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 over-stated. That is because the parties to a blockchain transaction are still physically located somewhere on Earth, just as the participants in a virtual world are physically somewhere sitting in front of a screen. 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.*, 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.[108] 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.[109]

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.

---

107 Wulf A. Kaal & Craig Calcaterra, *Blockchain Technology's Distributed Jurisdiction*, MEDIUM (June 20, 2017), https://medium.com/semadaresearch/blockchain-technologys-distributed-jurisdiction-a2177c244538.

108 Greene v. Mizuho Bank, Ltd., 169 F.Supp.3d 855, 859 (N.D. Ill. 2016).

109 *See id*. at 862-63. ("[T]he conduct here alleged is sufficient to establish that Mizuho purposefully directed its conduct to California, given that the torts were completed only when Mizuho knowingly accepted a deposit from a California branch from somebody it knew to be a California resident and placed that deposit into the financial equivalent of a black hole.").

VIII. AUTONOMOUS AGENTS

The development of unmanned aerial vehicles and increasingly autonomous weapons systems as well as the potential use of drones, autonomous automobiles, and other robots using artificial intelligence radically challenge legal conceptions of jurisdiction and accountability. In particular, autonomous, machine-learning vehicles tend to spread responsibility for decision-making across a larger number of actors. Thus, it becomes difficult to determine both who is responsible for a machine-based action when it causes harm, and where the relevant action took place in order to determine legal responsibility and jurisdiction.

So far, this issue has been most explored in the context of automated weaponry and warfare. For example, consider the Israeli Harpy which, once launched by a human operator, can detect an enemy radar system and then autonomously dive bomb and strike that target.[110] As Laura Dickinson recounts:

> If the Harpy killed a large number of civilians in a manner that could be said to violate international humanitarian law, who could or should be held responsible? The human being who has the responsibility to override the weapons system? The commander of the territory where the weapons system was deployed? The individuals who set policy for using the technology? The individuals who drafted the targeting criteria? The engineers who designed the weapons system to apply the targeting criteria? Anyone who supplied intelligence that fed into the weapons system and that formed the basis for target selection? In the case of even partially autonomous systems, it is difficult to locate a responsible human agent.[111]

Similar questions can, and almost certainly will, be raised by automation in vehicles and by machine-learning based robotics and drones for commercial and consumer use. These new deployments will likely reshape legal rules regarding product liability, insurance, contract, jurisdiction, criminal law, and other areas.

---

110 Laura A. Dickinson, *Drones, Automated Weapons, and Private Military Contractors: Challenges to Domestic and International Legal Regimes Governing Armed Conflict*, *in* NEW TECHNOLOGIES FOR HUMAN RIGHTS LAW AND PRACTICE 93, 122 (Molly K. Land & Jay D. Aronson eds., 2018); *see also* Marcus Wagner, *The Dehumanization of International Humanitarian Law: Legal, Political, and Ethical Implications of Autonomous Weapons Systems* 47 VAND. J. TRANSNAT'L L. 1371, 1381 (2014); H. Roff, *Killing in War: Responsibility, Liability and Lethal Autonomous Robots*, *in* ROUTLEDGE HANDBOOK OF ETHICS AND WAR: JUST WAR THEORY IN THE 21ST CENTURY (A. Henschke et al. eds., 2013).

111 Dickinson, *supra* note 110, at 122.

IX. CONCLUSION

As difficult as the cases discussed above may be to resolve, if anything the future holds issues that may be tougher still. New deployments expanding the "virtual" in social life will likely reshape legal rules regarding product liability, insurance, contract, jurisdiction, criminal law, and other areas.

Or possibly not. Ever since the rise of the commercial internet in 1995, legal scholarship regarding online innovation has often divided into two broad camps. On one side were the cyberspace "unexceptionalists," who argued in various contexts that the online medium did not significantly alter the legal framework and that well-settled principles of law can simply be applied to online interaction.[112] On the other, cyberspace "exceptionalists" argued that the medium itself created radically new problems that required new analytical work to be done.[113]

One core problem with the unexceptionalist position is that it assumes that there actually *are* well-settled 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.

For example, in the nineteenth century "well-settled" US principles of legal jurisdiction and choice of law saw jurisdiction as rooted almost exclusively in the territorial power of the sovereign.[114] 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

---

112 *E.g.*, Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUDIES 475, 475 (1998); Allan R. Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INTERNATIONAL LAWYER 1167, 1167-68 (1998). Many of these arguments are reprised in Andrew K. Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 729 (2016).

113 *E.g.*, David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN L. REV. 1367 (1996); David G. Post, *Against Cyberanarchy*, 17 BERKELEY TECH. L.J. 1365, 1371-73 (2002). Many of these arguments are echoed in Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 179 (2018); *see also* Paul Schiff Berman, *Legal Jurisdiction and the Deterritorialization of Data*, *supra* note 9, at 12 (2018) (responding to Daskal's article and pointing to continuities with earlier legal scholarship concerning online interaction).

114 *See, e.g.*, Pennoyer v. Neff, 95 U.S. 714, 720 (1878).

state without actually being present there at the time of a lawsuit.[115] Not surprisingly, by the end of the twentieth century it had become "well-settled" in US 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.[116] Likewise, it had become "well-settled" that choice-of-law rules could be based on governmental interests or relationships as well as territorial connections.[117] And, of course, these new "well-settled" rules felt as commonsensical and obvious to most judges, lawyers, and observers as the sovereigntist 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 the virtualization of social life. Indeed, as the cases described in this Essay suggest, the idea of basing jurisdiction on where effects are felt is difficult to apply to online interaction because activity may cause harms in many different locations, anywhere data is stored, used, or viewed.

The answers that law will ultimately evolve to address the sorts of problems raised in this Essay 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 have relied too much on the application of mythical well-settled principles, the exceptionalists have, 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.

Moreover, as the discussion of digital data makes clear, governments need not only act through the traditional apparatus of lumbering, territorially-limited law enforcers or regulators. Instead, they can commandeer entities such as search engines or online service providers to regulate on the government's behalf, either by turning over data, adjudicating claims, or building certain regulations into the computer code that dictates online activity itself.

---

115 *See, e.g.*, Hess v. Pawloski, 274 U.S. 352, 356 (1927).
116 *See, e.g.*, International Shoe Co. v. State of Washington, 326 U.S. 310, 310 (1945).
117 *See, e.g.*, RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 6 (AM. LAW INST. 1971).

Perhaps then we need to evolve a more cosmopolitan and pluralist vision of conflict of laws. Just as 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 may now be yielding to a conception of jurisdiction based on multiple community affiliations. A *cosmopolitan*[118] 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. 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 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 *non-state* communities also assert various claims to jurisdictional authority and articulate alternative norms that are often incorporated into more "official" legal regimes. This *pluralist*[119] 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.[120]

Finally, as this survey of cases makes clear, in a world of virtual social life and deterritorialized data, the role of intermediaries as law-makers and law-enforcers has radically increased. When Facebook enforces a Terms of Service agreement, or Twitter is asked (or required) to police hate speech, or Google implements a European Court of Justice 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 these actions affect the behavior of real people in

---

118 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.").

119 For a more detailed application of the insights of legal pluralism to private international law, *see* Berman, GLOBAL LEGAL PLURALISM, *supra* note 8.

120 *See generally, e.g.*, Robert M. Cover, *The Supreme Court, 1982 Term–Foreword: Nomos and Narrative*, 97 HARV. L. REV. 4, 43 (1983).

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 non-governmental entities should remain within our legal analytical purview whether we call them law or not.[121]

In any event, it is incumbent on legal scholars today to recognize the new challenges arising in this increasingly virtual, data-driven world and to build new cosmopolitan pluralist legal models that may, over time, become simply the way we conceptualize law in the 21st 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. Neither law nor society ever stop moving, and so we must push forward to develop new models to respond to new practices in new contexts.

---

[121] As I have argued elsewhere,

> [P]luralism frees scholars from needing an essentialist definition of "law." For example, with legal pluralism as our analytical frame, we can get beyond the endless debates both about whether international law is law at all and whether it has any real effect. Indeed, the whole debate about law v. non-law is largely irrelevant in a pluralism context because the key questions involve the normative commitments of a community and the interactions among normative orders that give rise to such commitments, not their formal status. Thus, we can resist positivist reductionism and set nation-state law within a broader context. Moreover, an emphasis on social norms allows us to more readily see how it is that nonstate legal norms can have significant impact on the world. After all, if a statement of norms is ultimately internalized by a population, that statement will have important binding force, often even more so than a formal law backed by state sanction. Accordingly, by taking pluralism seriously we will more easily see the way in which the contest over norms creates legitimacy over time, and we can put to rest the idea that norms not associated with nation-states necessarily lack significance. Indeed, legal pluralists refuse to focus solely on who has the formal authority to articulate norms or the coercive power to enforce them. Instead, they aim to study empirically which statements of authority tend to be *treated* as binding in actual practice and by whom.

Paul Schiff Berman, *Global Legal Pluralism*, 80 S. CAL. L. REV. 1155, 1177-78 (2007) (footnotes omitted).