Bitcoin Foundation

A Bitcoin Primer on Jurisdiction*

The Internet minimizes the importance of geopolitical boundaries. Online, individuals and businesses conduct transactions in distant states and countries with ever-increasing ease and frequency. Bitcoin further diminishes geopolitical distinctions, allowing users to opt out of government-backed currencies in favor of a shared, global medium of exchange. But doing so may place Bitcoin users and businesses under the authority of unfamiliar or burdensome foreign laws, facing the prospect of defending themselves in regulatory proceedings and lawsuits in far-away places.

Because of the varied national and international legal rules that govern online transactions, the Bitcoin Foundation has commissioned this short primer to help Bitcoin users and businesses evaluate and reduce the risk of being subject to unfavorable laws. The key concept to understand is "jurisdiction."

Jurisdiction Limits Courts' and Governments' Powers Over Non-Residents

"Jurisdiction" is a government's coercive power to hold individuals accountable to its laws. Government power, and thus jurisdiction, is limited by political boundaries.

Traditional limitations on jurisdiction are illustrated well by the system in the United States. In the nineteenth century, an individual had to be physically present within a U.S. state to be subject to the jurisdiction of that state's courts.[1] Thus, an individual could evade the coercive authority of a particular state's laws simply by crossing state lines, by travelling across the Mississippi River from Illinois to Missouri, for example, or by stepping across the boundary between Pennsylvania and Ohio. Simply put, the courts in one state would not reach across state lines to assert jurisdiction over the citizens of another state because it would violate the sovereignty of their sister states.

As commerce increased and society became more complex, however, the strict requirement of physical presence was significantly relaxed.

Robert A. McFarlane is a partner in Hanson Bridgett LLP's San Francisco Office and chairs the firm's Technology Law Practice. He is a registered patent attorney and focuses his practice on federal court patent infringement litigation and advising his clients on a wide range of intellectual property matters and disputes. Mr. McFarlane would like to thank Alan S. Bishop for his assistance in preparing this primer. Mr. Bishop litigates as an associate in Hanson Bridgett's San Francisco office and is a licensed Civil Engineer. This publication does not constitute legal advice. Readers should consult with legal counsel for the most current information and to obtain professional advice before acting on any of the information presented.

[1] *Pennoyer v. Neff*, 95 U.S. 714, 733 (1878).

Modern American courts view interactions between the individual and the state as an exchange of duties. In exchange for receiving the benefit of a state's legal protections, the state expects that individuals and corporations doing business within their territory will consent to appear in the state's courts.[2] Enjoying the benefits of a state's laws makes one subject to its jurisdiction.

Under modern principles, incidental contact with a state will be insufficient to create jurisdiction. At some level of "minimum contact" with a state, however, an individual (or corporation) will be deemed to have sufficiently benefitted from the state's protections and laws so that exercising jurisdiction over the individual is considered fair, even if they are not physically present in the state.[3]

Continuous and systematic contact with a given state will subject an individual or corporation to that state's "general jurisdiction." If one's contacts with a state consist of isolated conduct or a single transaction, jurisdiction over an individual or corporation may be limited to controversies relating to that specific conduct or transaction. For example, if a company is incorporated, conducts extensive business, and has its headquarters in California, it would be subject to the general jurisdiction of California courts, and most disputes involving the company could be resolved in California courts. However, if that same company engaged in very limited activities in the neighboring state of Oregon, such as completing one or two individual sales in that state, it could be sued in Oregon only for disputes arising out of those specific sales.

From Physical Presence to Virtual Contact

Identifying minimum contacts sufficient to establish jurisdiction relating to a particular event or transaction is relatively straightforward when people physically move across state lines. A resident of Pennsylvania who drives a car into Massachusetts and injures a pedestrian before returning home can be ordered back into court in Massachusetts to be held accountable because of the location of the incident. Indeed, even if the motorist refuses to return to defend himself, the Massachusetts court could enter a judgment in the driver's absence, and his own Pennsylvania courts would enforce a judgment issued in Massachusetts against him.

Courts can also find minimum contacts without physical presence. For example, a casino in Nevada that does not have any employees or business locations in California can be subject to jurisdiction in California courts if it extensively targets advertising at residents in California and maintains an Internet presence within California.[4]

Jurisdiction established purely through Internet transactions is more complicated. Early cases addressing jurisdiction and the Internet tended to base their decisions on a website's degree of "interactivity." An influential decision called *Zippo Manufacturing* helped establish this approach in 1997.[5] The *Zippo Manufacturing* case categorized websites on a sliding scale,

---

[2] *Milliken v. Meyer*, 311 U.S. 457, 464 (1940).

[3] *International Shoe Co. v. Washington*, 326 U.S. 310 (1945)

[4] *Snowney v. Harrah's Entertainment, Inc.*, 35 Cal.4th 1054, (2005).

[5] *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119, 1124 (W.D.Pa.1997).

ranging from "passive" websites that merely provided information to web users to "interactive" websites through which Internet users could place orders or request further action from the website provider. Under the *Zippo Manufacturing* framework, operating a passive website would <u>not</u> be sufficient to subject the provider to jurisdiction anywhere its website could be accessed. Jurisdiction could, however, be asserted over an Internet website provider whose interactive website could be accessed and used in a given jurisdiction. Thus, businesses operating interactive websites may find themselves involved in lawsuits wherever users order products through their websites.

The *Zippo Manufacturing* framework has proven difficult to apply in the context of ever-evolving Internet functionality. Customized driving, bicycling, or public transportation directions could be provided to mobile users anywhere in the world; does customizing a user's experience subject the provider to personal jurisdiction in the user's locale? Is targeted advertising based on location to display bathing suits to potential customers in Florida but gloves to customers in Alaska "purposefully direct" advertising toward those two states and thereby subject the company to jurisdiction in them?

The law is still evolving on these important questions, but recent cases provide principles that give Bitcoin users and businesses the ability to at least reduce the chance that they will be subjected to burdensome state or national laws and distant court proceedings.

Asserting Jurisdiction Over Commercial Websites

The sliding scale approach described in *Zippo Manufacturing* resulted in a number of courts asserting jurisdiction over website owners located in distant venues if their sites could be accessed from within the forum state and were sufficiently "interactive." In *Zippo Manufacturing*, a Pennsylvania court asserted jurisdiction over a California subscription online news service, even though only two-percent of the approximately 140,000 paying subscribers worldwide were in Pennsylvania, primarily because the website permitted user interaction.

Other courts have taken a harder look at the sliding scale approach and are concluding that mere "interactivity" is not sufficient to establish jurisdiction over an Internet company that serves the entire world.

In a recent case, a woman in Nebraska found that her name appeared in a Massachusetts bookseller's online inventory simply because a rare book in the store's inventory was inscribed to her. She asserted that the bookseller violated her privacy by publishing her name and urged the Nebraska courts to take jurisdiction over the distant bookseller because his website was "interactive" and, therefore, his conduct was directed at Nebraska.[6] In response, the bookseller explained that in three years of website sales totaling $3.9 million, he had sold only eight books to customers in Nebraska.

The court rejected the "interactivity" test as being too aggressive, concluding that a defendant should not be haled into court in Nebraska simply because the defendant owns or operates an interactive website that is accessible in the state. The Nebraska court ruled that

---

[6] *Abdouch v. Lopez*, 285 Neb. 718 (2013).

a company should only be subject to jurisdiction within the state if it actually targeted its activities or sales to the state.

Although some states seem to be taking a step back from some of the broad concepts of jurisdiction that force distant Internet companies to defend themselves in unfamiliar courts, many states are adhering to the older principles of *Zippo Manufacturing*. For example, a New York court recently exercised jurisdiction over an online retailer in California that sold and shipped designer handbags worldwide.[7] Even though the company had no particular focus on New York, the court found that the website offered handbags "for sale to New York consumers, permitted New York consumers to purchase such bags, and facilitated the shipment of those bags into New York," and that the retailer had completed about fifty sales to customers in New York. These facts were sufficient to create jurisdiction in New York.

Cases like those from New York give rise to legitimate concerns among Bitcoin businesses that they may be hauled into a distant court virtually anywhere they conduct business, and that they will have to defend themselves under the laws of an unfamiliar venue. Although there are no fool-proof steps for Bitcoin businesses to avoid the laws of undesirable states or nations, recent case law hints at certain steps that can significantly reduce the risks.

Avoiding Jurisdiction by Avoiding Users

Perhaps the most straightforward way to avoid being subjected to jurisdiction in a given location is to avoid doing business there. New York cases give fair warning to online businesses that they may be subjected to the jurisdiction of New York courts if they sell products or provide services in the state. Companies that wish to avoid burdensome regulations or the prospect of defending lawsuits in a given state may choose not to conduct any business within its borders and not to send any materials to customers with addresses there.[8]

This "avoidance" approach may be difficult to apply in practice because the physical location of users is irrelevant for many types of online commercial services and may be impossible to determine. However, actively rejecting interaction with users who provide location data may prevent far-flung jurisdictional fights.[9] IP blocking (also known as "geofencing"), screening based on user-entered address data, electing not to display ads to audiences in undesirable jurisdictions, and providing less interactivity to users in undesirable jurisdictions may demonstrate that a company does not intend to conduct business in a particular state.

Avoiding Jurisdiction Through Forum Selection Clauses

Many commercial contracts contain clauses in which the parties agree on where any dispute between them will be heard and what body of law will govern such disputes. For example, a software company in California may include in its end user license agreement a requirement

---

[7] *Chloe v. Queen Bee of Beverly Hills, LLC*, 616 F. 3d 158 (2010).

[8] *American Network, Inc. v. Access America/Connect*, 975 F.Supp. 494 (1997); and see Stomp, Inc. v. Neato LLC, 61 F.Supp.2d 1074 (1999).

[9] *Accutest Corp. v. Accu Test Sys., Inc.*, 532 F.Supp. 416, 419-20 (D.Mass. 1982)

that its customers file any claim against the company in a court located in San Francisco and that any dispute will be governed by the laws of the State of California. These "forum selection" and "choice of law" clauses are widely enforced in most courts.

Choice of law and choice of venue clauses may also be applied to Internet transactions. A California court determined in 1999 that choice of law and choice of venue provisions that were included in an interactive "clickwrap agreement" were fully enforceable.[10] Indeed, properly written clickwrap agreements have generally been enforced for online transactions.[11]

If choice of law provisions are buried in a user agreement that does not require affirmative consent from the customer, they may work in some jurisdictions, but they are less likely to be enforced in others. Companies will have better success pre-selecting the law that will apply to their disputes if they are up-front and clear about it in interactive clickwrap agreements.

Conclusion

The jurisdictional principles that govern the Internet are still evolving, and there is no foolproof way for providers of Bitcoin-based services to eliminate the risk of being hauled into court in a distant jurisdiction. However, with the regulatory environment for Bitcoin varying widely, it may be important for Bitcoin businesses to control what governments have jurisdiction over them. Companies may minimize the probability of being forced to defend lawsuits or enforcement actions in distant jurisdictions by taking some or all of the following steps:

- Maintaining passive websites when possible for a company's business purposes;

- Including a statement within a website's, app's, or service's terms and conditions that it is intended for use only in certain jurisdictions;

- Taking measures not to transact business in jurisdictions of concern, e.g., declining business from users in undesirable jurisdictions;

- Requesting that users identify their locations, informing users in undesirable jurisdictions that the service is not intended for their use, and terminating any transactions with them;

- Blocking interaction with users in undesirable jurisdictions altogether;

- Blocking the interactive functions of websites, apps, and services for users who are in undesirable jurisdictions; and

- Including terms and conditions that require affirmative consent by the users that specify choice of law and choice of venue provisions.

---

[10] *Stomp, Inc. v. Neato LLC,* 61 F.Supp.2d 1074 (1999).

[11] *Thompson v. Handa-Lopez, Inc.,* 998 F.Supp. 783 (W.D. Tex. 1998) (improperly drafted venue selection clause not enforceable against users of online-gambling service).