PERSONAL JURISDICTION, INTERNET COMMERCE, AND PRIVACY: THE PERVASIVE LEGAL CONSEQUENCES OF MODERN GEOLOCATION TECHNOLOGIES

Kevin F. King[*]

TABLE OF CONTENTS

[*] Law Clerk, the Honorable Paul V. Niemeyer, U.S. Court of Appeals for the Fourth Circuit, 2010–2011; J.D., Northwestern University School of Law, 2010; B.A., Middlebury College, 2002. Thanks to Professor Jim Speta for overseeing the development of this article and contributing so many great ideas to it, and to Professors Stephen Calabresi, Peter DiCola, Tonja Jacobi, John Hines, Mark Spottswood, and Jacqueline Lipton, as well as Kristen Knapp, Nick Terrell, Richard Glover, Gautam Huded, Tom Gaeta, Colleen McNamara, and Alexandra Newman for their helpful comments.

I. INTRODUCTION

Modern geolocation technologies allow Internet sites to automatically and accurately identify a user's geographic location. This capability—unavailable just a few years ago—has begun to revolutionize Internet commerce and communication by enabling content localization, customization, and access regulation on a scale previously thought to be impossible. Yet thus far, the law has reacted inadequately to these technologies, or in some cases, failed to react at all.

While these failings are widespread, they are most glaring in three particular areas: personal jurisdiction, Internet commerce regulation, and privacy law. Personal jurisdiction doctrine has largely ignored the substantial role geolocation technologies play in the interaction between parties and a forum state. The dominant test for determining whether a web site is subject to personal jurisdiction, set forth in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F.Supp 1119 (W.D. Pa 1997), was conceived well before geolocation technologies were commercially available and has not been updated since. Applied rigidly, the *Zippo* test permits personal jurisdiction over an "active" website even when the site uses geolocation tools to block access to in-state users. More importantly, this test denies jurisdiction in many cases where a "passive" website could reasonably have used such tools to regulate access but has failed to do so.

Next, scores of Internet commerce cases have concluded that accurate geolocation is impossible, and have based legal conclusions on this now-erroneous premise. These cases have relied on two main lines of reasoning. First, in the absence of effective geographic screening mechanisms, state laws governing online content and commerce cannot avoid significant extraterritorial application, and thus violate the dormant Commerce Clause. Second, without an ability to filter users by jurisdiction, all sites would be subject to the rules imposed by the most stringent state regulator—resulting in an unacceptable burden on protected speech. Modern geolocation tools completely undermine both of these arguments by making it possible to tailor content type and availability by jurisdiction. As a result, state governments should now be free to impose Internet commerce regulations in several areas previously held to be off-limits by the courts.

Finally, there is the question of geolocation tools' impact on privacy. Current law fails to address this matter explicitly,

though the Federal Trade Commission's recently released guidelines for contextual and behavioral advertising do so indirectly. As a result, there is significant confusion regarding sites' privacy obligations with respect to geolocation data. Currently, most geolocation tools pose little privacy risk, as users are identified only at a regional level. As these tools begin to provide more granular and individualized location data, the need for privacy regulation will increase substantially, however.

In light of the now common market use of geolocation tools, courts, legislatures, and agencies must adapt each of these bodies of law to reflect the new technological reality.

A. Organization of Argument

This article provides an in-depth analysis of the problems geolocation technologies pose for personal jurisdiction, Internet commerce, and privacy law; as well as ways those problems can be resolved. The article is broken down into five parts—each addressing a separate segment of the challenge identified above. Part II begins by introducing the concept of geolocation and the various ways in which Internet-connected devices can be geographically located. Part II then turns to the state of geolocation technology in terms of market penetration, accuracy, and cost.

Part III examines the impact of modern geolocation technologies on personal jurisdiction doctrine, with an emphasis on the now-dominant *Zippo* test for determining when a website is subject to specific jurisdiction. From a descriptive standpoint, this Part argues that the *Zippo* test's active/passive distinction is incomplete because some "active" sites may employ geolocation tools to screen out forum state users, while some "passive" sites could reasonably block forum state users but fail to do so. These shortcomings lead to Part III's normative argument that courts should consider a party's use of (or failure to use) geolocation tools when applying the *Zippo* test. Under this modified standard, a site's failure to employ geolocation tools would not, as Professor Joel Reidenberg has argued, invariably lead to a finding of purposeful availment and thus personal jurisdiction. Rather, personal jurisdiction in such cases would depend on a balancing of several factors, including the costs associated with implementing geolocation tools, the relevance of geography to the underlying online conduct, and the burden on free speech.

In Part IV, the article reviews a long line of community

standards and dormant Commerce Clause cases that assume geolocation is impossible and base legal conclusions on that technological premise. Given the new technological reality, the question is not *whether* Congress and the States can compel sites to screen users by location, but rather *when* such a mandate may be imposed. Congress unquestionably has the power under the Commerce Clause to require most sites to engage in geographic screening. This power is significantly circumscribed by the First Amendment, however, because a geolocation mandate would unduly burden protected speech in many contexts. States face similar First Amendment limitations as well as those imposed by the extraterritoriality prong of the dormant Commerce Clause. Despite these restrictions, Part IV concludes that geolocation mandates would pass constitutional muster in a wide range of circumstances—most notably when applied to large online retailers and service providers.

Because geolocation technologies affect Internet users almost every time they venture online, Part V takes up the privacy impact of geolocation technologies. Current law does not explicitly regulate the use of geolocation tools; however the Federal Trade Commission (FTC) has begun to fill that void via its guidelines for contextual and behavioral advertising. The FTC staff and some privacy advocates have argued that geolocation data constitutes legally-protected personally identifiable information, or "PII." Part V argues for a more limited approach, as only some types of geolocation tools generate data individualized enough to qualify as PII. For this reason, the FTC should focus its efforts on requiring sites that use the most accurate forms of geolocation tools to provide users with notice- and consent-based privacy safeguards. As the technological landscape changes over time, the FTC should utilize its flexible enforcement authority under section 5 of the FTC Act to ensure that privacy law remains balanced and effective. Finally, Part V explores the conflict between consent-based privacy rules, which could cause many users to refuse to be geolocated, and personal jurisdiction doctrine, which in some cases may require all users to be identified and screened by jurisdiction. Part VI concludes.

II. STATE OF THE TECHNOLOGY

To fully appreciate the impact geolocation technologies have on law, one must first understand how these technologies function in practice. This Part provides a brief technical primer on the

way modern geolocation tools work, then describes the market penetration, accuracy, and cost associated with such tools. As the examples in Part II.B demonstrate, geolocation tools have already become an essential part of many electronic commerce business models, including advertising on sites that consumers may not perceive as commercial, such as newspapers. This trend will only continue as sites pursue ever more individualized marketing schemes and as wireless devices equipped with GPS capabilities proliferate.

A. Geolocation 101: How the Technology Works

Geolocation technologies provide an automated means of identifying an Internet end-user's location.[1] Although these technologies operate in an increasingly wide range of manners, most fall into one of two categories: client-side and server-side.[2] Client-side geolocation tools operate on a user's own computer or wireless device. These technologies generally pinpoint a user's location via a Global Positioning System (GPS) chip or triangulation of nearby wireless network towers.[3] Once a user's location is determined through those means, the user's device transmits the location whenever a website or content provider requests location information.[4] Client-side geolocation is

[1] Kevin F. King, *Geolocation and Federalism on the Internet: Cutting Internet Gambling's Gordian Knot*, 11 COLUM. SCI. & TECH. L. REV. 41, 58 (2010). *See* Dan Jerker B. Svantesson, *Geo-location Technologies and Other Means of Placing Borders on the 'Borderless' Internet*, 23 J. MARSHALL J. COMPUTER & INFO. L. 101, 109–10 (2004) (noting the process of finding an Internet user's geolocation through the translation of their IP address into a geographical location); Andrea M. Matwyshyn, *A Network Theory Approach to Internet Jurisdiction through Data Privacy*, 98 NW. U. L. REV. 493, 517 n.136 (2004) ("Geolocation is a service that geographically places in physical space the unique identifier of an individual surfing the Web with a high, but not perfect, degree of accuracy.").

[2] *See generally* YUVAL SHAVITT & NOA ZILBERMAN, *A STUDY OF GEOLOCATION DATABASES* 2–3 (2010), *available at* http://arxiv.org/abs/1005.5674 (discussing various configurations for geolocation systems); *What is IP Address Geolocation Used For?*, QUOVA.COM, http://www.quova.com/what/ (last visited Jan. 5, 2011) (describing Quova's server-side geolocation services that are provided to search engine providers, government agencies, broadcasters and big brand retailers).

[3] *See* Nick Doty, Deirdre K. Mulligan & Erik Wilde, *Privacy Issues of the W3C Geolocation API*, U. CAL. BERKELEY SCH. OF INFO, Feb. 2010, at 6, 12, *available at* http://escholarship.org/uc/item/0rp834wf [hereinafter *Berkeley W3C Study*] (noting mobile devices may be equipped with a GPS receiver to determine current geolocation).

[4] The Internet Engineering Task Force (IETF) Geopriv working group has advocated for and begun developing client-side geolocation tools that would

currently less common than server-side geolocation; however, this balance is shifting as GPS-enabled smart phones become more widely deployed.[5]

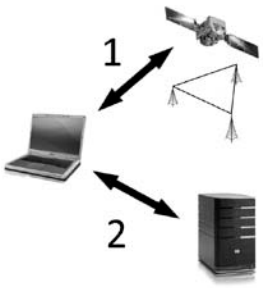

Fig. 1: A client-side approach to geolocation

By contrast, server-side geolocation tools work remotely. While websites could theoretically perform their own server-side geolocation, many outsource the process to third party platforms such as Quova's GeoDirectory, Akamai's EdgeScape, and Skyhook Wireless' Wi-Fi Positioning System.[6] These tools start by acquiring data from a user that does not indicate a specific location—such as the user's Internet Protocol (IP) address or the SSIDs for nearby wireless networks.[7] The geolocation provider then compares that data with information contained in an existing database that links IP addresses, SSIDs, and other identifiers with specific geographic locations.[8] For example, a database might associate all IP addresses in the 165.124.73.xxx

allow users to share location information at varying levels of abstraction—i.e., a user might elect to share the state in which he or she lives, but not the city or county. *See* RICHARD BARNES ET AL., AN ARCHITECTURE FOR LOCATION AND LOCATION PRIVACY IN INTERNET APPLICATIONS: DRAFT-IETF-GEOPRIV-ARCH-01 4, 6, 8 (Internet Engineering Task Force Oct. 26, 2009), *available at* http://tools.ietf.org/pdf/draft-ietf-geopriv-arch-01.pdf (noting that in the interest of the individual's privacy, the user may set privacy preferences regarding the use of their location); *Berkeley W3C Study*, *supra* note 3, at 4 (stating that IETF Geopriv relies on users instead of entities when choosing whether to consent to the privacy policy).

[5] *See* Ryan Kim, *Apple's Boosts Smart-Phone Market Share*, S.F. CHRON., Feb. 24, 2010, at D1 (describing the increasing rate of Apple's iPhone sales).

[6] *See* Riva Richmond, *We Know Where You Are: With New Software, Web Sites Can Tell What City a Visitor is Coming From; That Can Be Useful Information*, WALL ST. J., Sept. 29, 2008, at R8.

[7] *See id.*; *Berkeley W3C Study*, *supra* note 3, at 12.

[8] *Berkeley W3C Study*, *supra* note 3, at 12.

range with users at the Northwestern University School of Law in downtown Chicago. Alternatively, a database could, though previous collection of SSID data from users with known IP addresses, link users in range of wireless networks named "Reagan-DCA" and "Pentagon" with a location in the Arlington, Virginia area.[9] As a general matter, the data-geography linkages stored in these databases are culled from a wide range of sources, such as customer surveys, purchase records, and ongoing, specialized forms of network analysis.[10]

In most cases, user data matches an entry in the server's database, making a geographic identification possible.[11] Moreover, when a geolocation provider makes a location match, the provider can often supply a wealth of information about the customer to the site the user is accessing, such as the user's country, state, city, and the type of device used to access the site.[12] Current server-side geolocation tools can locate most users within a twenty to thirty-mile radius.[13]

---

[9] *See id*. (describing Skyhook Wireless' use of such data for its Wi-Fi Positioning System). This methodology does not work effectively when a user is only within range of one or two wireless networks, each of which lack a distinctive name. For instance, a user in range of one network with SSID "linksys" and another with SSID "router" likely could not be geolocated on the basis of nearby SSIDs alone.

[10] *See* PRICEWATERHOUSECOOPERS, REPORT OF INDEPENDENT ACCOUNTANTS: QUOVA. INC., 3 (Oct. 23, 2008), *available at* http://www.quova.com/documents/PricewaterhouseCoopers_Audit.pdf [hereinafter PWC STUDY] ("Quova utilizes information from multiple internal and external sources to make geolocation decisions . . . . [T]heir globally distributed data collection network . . . . is comprised of collectors spread throughout the world which obtain traceroutes and hostnames for IP address ranges . . . ."); *EdgeScape*, AKAMAI TECHNOLOGIES, http://www.akamai.com/html/technology/products/edgescape.html (last visited Jan. 5, 2011) ("Akamai['s] . . . data-gathering technology . . . collects geographical . . . information for every routable IP address on the Internet.").

[11] *Berkeley W3C Study*, *supra* note 3, at 12.

[12] *See* AKAMAI TECHNOLOGIES, *supra* note 10; Bob Tedeschi, *E-Commerce Report; The Market Is Growing for Software that Finds Internet Users' Locations*, N.Y. TIMES, June 16, 2003, at C7 (describing how MLB.com uses a geolocation software that prevents users in the Boston market access to watching a live webcast of the game in order to "avoid sapping the game's television ratings").

[13] *See* ACLU v. Gonzales, 478 F. Supp. 2d 775, 807 (E.D. Pa. 2007) (reviewing testimony from a Quova executive regarding the effectiveness of its technology). Quova, Press Release, *Quova's Geolocation Data Helps Continental Airlines Improve Web Banner CTR* (Mar. 24, 2009) ("Quova provides IP address location data down to a metro area (25 to 50 miles).").

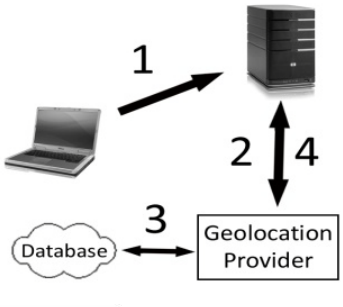

Figure 2: A typical four step
server-side approach to geolocation

For all their complexities on the back-end, geolocation technologies are remarkably simple from the end user's perspective. Although they were non-existent just a few years ago,[14] these technologies have become a seamless, almost invisible part of everyday Internet use. For example, when a user searches Google for the term "car dealerships" when connected to the Internet via RCN, a cable company serving much of the Chicagoland area, the first page of Google's search results includes three sponsored and seven general, un-sponsored links for dealers located in Chicago.[15] In this case, the user's search terms did not reference Chicago and Google did not ask the user whether it should identify his or her location. Nonetheless, Google's search engine assumes that the user will be best served by localizing its results accordingly.[16] In fact, before a user even has a chance to enter search terms, Google determines a user's location and serves the appropriate version of its homepage—i.e., google.fr for users in France, google.com for

[14] *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 60–62 (2006).

[15] *See generally,* Google, http://www.google.com/ (last visited Jan. 5, 2011) (In the search box enter the term "Car Dealerships" and left click on the search button). Search results for "car dealerships" made while connected to RCN, a Chicago area Internet provider, are on file with the author (retrieved Mar. 8, 2010).

[16] *Cf.* Digital Envoy, Inc. v. Google, Inc., 370 F. Supp. 2d 1025, 1029 (N.D. Cal. 2005) ("Google . . . regularly utilize[s] . . . geolocation technology as one factor in determining which advertisements to display for customers in its AdSense program.") (citation omitted).

users in the United States, and so on.[17] As described further in Part II.B, geolocation tools are not restricted to the realm of search engines, as retailers, online broadcasters, and banks all integrate these tools into the way their sites interact with end users.

B. Accuracy, Cost, and Market Penetration

Since they were introduced in the early 2000s,[18] server-side geolocation technologies have become increasingly accurate, inexpensive, and widely deployed.[19] Today, leading geolocation technologies are up to 99.9% accurate at the country level and more than 97% accurate at the state level within the United States.[20] These accuracy rates reflect a substantial increase from 2004, when popular geolocation tools were only 80% to 94% at the state level.[21] As noted above, server-side technologies can

[17] *See* Anick Jesdanun, *Not-Quite-Worldwide Web; Geolocation: Technology That Tracks Users' Whereabouts is Being Used Increasingly to Target Advertising as Well as Restrict Access on the Information Superhighway*, BALT. SUN, July 15, 2004, at 8D (noting that Google already redirects foreign visitors to country-specific home pages).

[18] *See* Press Release, Akamai, Akamai Advances Customized Content Delivery with Edgescape (Mar. 14, 2001), *available at* http://www.akamai.com/html/about/press/releases/2001/press_031401d.html (announcing the unveiling of EdgeScape Pro, an advanced geolocation program); *see also* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale L.J. 785, 810–12 (2001) (foretelling the development of technologies "that allow [a] webpage . . . provider [to] instantly . . . determine [the user's] geographical identity on the basis of the Internet protocol (IP) address of the user's computer").

[19] *See* King, *supra* note 1, at 59–62 (noting courts have taken judicial notice of the increasing accuracy of geolocation technologies).

[20] *See* PWC STUDY, *supra* note 10, at 6 (stating that these numbers are accompanied by a margin of error of less than 1% at a 95% confidence interval); Richmond, *supra* note 6 (putting the state level "accuracy rate[ ] in the low-to-high 90% range"); SHAVITT & ZILBERMAN, *supra* note 2, at 3 (country-level accuracy rates range from 97% to 99.9%); GOLDSMITH & WU, *supra* note 14, at 58–62 ("[W]hen . . . various databases are cross-referenced and analyzed by powerful computer algorithms, the geographical location of Internet users can be determined with over 99 percent accuracy at the country level."). Notably, accuracy rates differ in other countries depending on the extent to which each country has an established and well-documented Internet infrastructure. *See* Richmond, *supra* note 6; King, *supra* note 1, at 59 n.105 (indicating that accuracy rates vary depending on "the context in which a content provider is operating").

[21] *See* Jesdanun, *supra* note 17 (indicating that major geolocation companies claim an 80 percent or more accuracy rate for city-level data, while reporting a higher figure for country targeting at 99 percent); *see also* Press Release, Quova, *PricewaterhouseCoopers PwC Completes Annual Audit of Quova IP*

pinpoint a user's location within a twenty to thirty mile radius.[22] A number of important caveats apply to these calculations, however. First, server-side accuracy calculations tend to omit consideration of particularly troublesome addresses, such as those associated with America Online (which masks all of its users behind proxy servers).[23] Second, those calculations assume the absence of users who are intentionally attempting to circumvent the geolocation system via anonymization tools such as Tor.[24] Third, many accuracy studies do not make allowances for technologies such as wireless Internet access cards and Virtual Private Networks (VPNs), which may cause a user to appear to be connecting from work when the user is in fact traveling in another city or country.[25] While these shortcomings should not be ignored, even prominent critics do not contest the notion that server-side technologies are at least 70% to 80% accurate at the state level and improving with time.[26] Perhaps more importantly for the purposes of this article, several courts have taken explicit judicial notice of the increasing accuracy of geolocation technologies in recent years[27]—a fact that strongly

Geolocation Data (Apr. 14, 2009), *available at* http://www.quova.com/press-releases/pricewaterhousecoopers-pwc-completes-annual-audit-of-quova-ip-geolocation-data-2/ (noting that their IP geolocation accuracy has improved significantly from their 2004 level, 94 percent, to an accuracy of 98.2 percent in 2008); Matwyshyn, *supra* note 1, at 521 (concluding that as of 2004, geolocation technologies did not "offer adequate levels of certainty for jurisdiction purposes to be mandated as the tool of choice for jurisdictional determinations").

[22] *See* Richmond, *supra* note 6 and accompanying text (stating that as of 2007 Ace Hardware, through the use of Digital Element's geolocation software, was able to list stores within a thirty mile radius of the visitor's physical location); ACLU v. Gonzales, 478 F. Supp. 2d 775, 807 (E.D. Pa. 2007) (stating that a Quova procuct can determine a users' location within a "20 to 30 mile radius").

[23] *See, e.g.*, *Gonzales*, 478 F. Supp. 2d at 807 ("If a visitor is accessing a Web site through AOL, Quova can only determine whether the person is on the East or West coast of the United States."); *see also* Jesdanun, *supra* note 17 (noting that the major geolocation companies accuracy percentage rates are misleading due to the fact that addresses "known to cause trouble" are generally excluded).

[24] *See* Jesdanun, *supra* note 17; Hiawatha Bray*, Beating Censorship on the Internet: Tools Mask User Ids, Give Alternative Routes to Sites*, BOSTON GLOBE, Feb. 20, 2006, at A10 (explaining that Tor is a software program that allows users to surf the Internet anonymously by routing data "through private networks of proxy machines").

[25] *See generally Can Internet Gambling Be Effectively Regulated to Protect Consumers and the Payments System?: Hearing Before the H. Comm. on Fin. Servs.,*110th Cong. 18–19, 31 (2007) (statement of Jeff Schmidt, Chief Executive Officer of Authis).

[26] *Id*. at 31.

[27] *See Gonzales*, 478 F. Supp. 2d at 820 n.13 ("[T]echnology related to limiting access to Web sites based on the geographic location of the user has progressed

suggests that these technologies are now "accurate enough for legal purposes."[28]

Given the tremendous amount of investment that has gone into their development, most modern enterprise-level geolocation services are not cheap. As of 2007, geolocation tools provided by Quova cost between $6,000 and $500,000 per year, depending on the level of service and customization.[29] News reports indicate that one of Quova's chief competitors, Akamai, has charged similar rates.[30] While these prices fall well within the budget of most large online retailers and major content providers, they are also clearly cost prohibitive from the standpoint of small businesses, non-profits, and individual bloggers.[31] The Supreme Court reached a similar conclusion in *Reno v. ACLU* when it found that age verification technologies "would impose costs on non-commercial Web sites that would require many of them to shut down."[32]

Notably those costs are applicable only to sophisticated server-side geolocation tools.[33] Client-side geolocation tools, which have come into the market much more recently and which do not rely on extensive databases and data collection networks, can be utilized at a lower—though still significant—cost.[34] To do so, a host would simply need to insert code implementing the World Wide Web Consortium's (W3C) Geolocation Application Program Interface (API) in their web pages.[35] Once the code is in place,

since . . . 1999."); Hageseth v. Superior Court, 150 Cal. App. 4th 1399, 1423 (Cal. Ct. App. 2007) (noting that technological developments make it easier to identify and locate those who unlawfully sell drugs without a prescription over the Internet, because "[w]eb sites and Internet service providers already possess the ability to design or filter content based on user location").

[28] Svantesson, *supra* note 1, at 101–02.

[29] *Gonzales*, 478 F. Supp. 2d at 807.

[30] *See* Tedeschi, *supra* note 12 (quoting a corporate Akamai geolocation customer as paying $5,000 per month for "geotargeting service[s]").

[31] *See Gonzales*, 478 F. Supp. 2d at 820 n.13 (concluding that as of 2007, geolocation technologies were "far from perfect and cost prohibitive for many Web site operators that could be subject to COPA"); Goldsmith & Sykes, *supra* note 18, at 811 (describing the significant expense associated with implementation of geolocation tools).

[32] Reno v. ACLU, 521 U.S. 844, 855–56 (1997).

[33] *See Gonzales,* 478 F. Supp. 2d at 807 (noting that Quova's services cost anywhere from $6,000 to $500,000 a year).

[34] Some geolocation software, for instance, can be downloaded for free from sites such as www.cnet.com. Of course, once the software is downloaded it still must be implemented—a process which can be time consuming and expensive in its own right.

[35] *See Berkeley W3C Study*, *supra* note 3, at 1, 6–10 ("The API can be rapidly

the W3C Geolocation API can automatically access whatever geolocation data a user's device will provide and make that data available to the site to use for content customization, access restrictions, or other purposes.[36] Moreover, location data cultivated via client-side geolocation tools will often be much more accurate than that provided by server-side tools, as GPS and wireless tower triangulation tend to be more precise than the reverse-engineering done via IP detection and network analysis.[37]

These advantages come with two major drawbacks, however. First, the most common form of client-side geolocation only works when a user's device has a native geolocation capability. Only some wireless devices, such as the iPhone, come equipped with GPS,[38] and the overwhelming majority of laptop and desktop computers currently lack a similar capacity—thus limiting the effectiveness of GPS-based geolocation technologies. Second, client-side tools' increased level of accuracy may present a greater privacy challenge than server-side tools, as discussed in Part V below

Because geolocation technologies cost so much to implement, they have achieved the greatest level of market penetration among large online retailers and content providers.[39] Currently, these sites use geolocation tools for five principal purposes: (1) content localization; (2) content customization; (3) enforcement of access restrictions; (4) fraud prevention; and (5) traffic analysis. Each of these now-mainstream uses is illustrated below.

1. Content Localization

The most intuitive, and perhaps the most popular use of geolocation technologies is content localization.[40] Websites and applications modify generic content, such as the search results

deployed: Web developers can simply write scripting code to use this new browser functionality . . . .").

[36] *Id*. at 6–10.

[37] *Cf. id.* at 11–12 (comparing the accuracy of geolocation by IP address, Wi-Fi Networks, Cell Tower Triangulation, GPS and manual input).

[38] *See* Arman Mirkazemi, *HTML5 Apps: Positioning with Geolocation*, MOBILE TUTS+, (June 2, 2010), http://mobile.tutsplus.com/tutorials/html5/html5-geolocation/ (noting the iPhone3G and Android 2.0+ phones have GPS capabilities).

[39] *See* Tedeschi, *supra* note 12.

[40] *See id.* ("The most common application of geotargeting software may involve Internet advertising.").

for "car dealerships," to highlight aspects that are most relevant to a user's specific location.[41] Content localization is what makes the search function in Google Maps' iPhone application so useful: a search for "coffee shop" will return a listing of shops within a few blocks, rather than a list of links to companies that happen to sell coffee somewhere in the world—as one would have received in response to such a search before the dawn of the geolocation era. Ace Hardware uses this approach to serve a version of its home page featuring snowblowers to users in cold-weather climates during the winter months, while simultaneously serving a different version featuring patio furniture to users from Florida.[42] Similarly, the BBC uses IP geolocation to earn advertising revenue while still complying with United Kingdom licensing requirements that require video programming to be free of advertising.[43] To do so, the BBC's site transmits advertising-free digital video to UK-based users, and video with advertising included to users connecting from outside the UK.[44]

In this way, geolocation technologies "'allow a company to be two-faced or even 20-faced based on who they think is visiting.'"[45] Whereas Ace Hardware and the BBC serve different content to users depending on their location, other sites use geolocation tools to serve the same content to a diverse group of users, but in their native language or currency.[46] Other prominent businesses currently using geolocation tools for content localization include Continental Airlines, ESPN, Major League Baseball, Cheapflights.com, and jobs site Monster.com.[47]

2. Content Customization

Closely related to content localization is content customization. Whereas content localization is expressly concerned with a user's location as such, content customization utilizes location to make educated guesses as to facts about a user.[48] Geolocation provider

[41] *See* Richmond, *supra* note 6.

[42] *See id.*

[43] *See Quova IP Geolocation Drives Ad Revenues for BBC.com*, QUOVA, http://www.quova.com/downloads/cs-bbc-1109.pdf (last visited Jan. 5, 2011).

[44] *See id.*

[45] Jesdanun, *supra* note 17.

[46] *See id.*

[47] *Who,* QUOVA, http://www.quova.com/who/ (last visited Jan. 5, 2011) (listing corporations that use Quova's service).

[48] *See* Jesdanun, *supra* note 17.

Digital Envoy, for instance, combines a user's location with census data to target ads by demographic profile.[49] A site could use this approach to serve different ads to users of the same web page, with a user connecting from a wealthy suburb like Tiburon, California receiving an ad for a high-end "Gold" American Express card, while a user from a less-affluent area might receive an ad for a standard "Green" American Express card.[50] Similarly, Akamai provides clients with data regarding users' connection speeds, thus enabling advertisers "to show multimedia ads to prospective customers without slowing them down."[51] As geolocation technologies mature, it seems likely that providers will package location data with an increasing array of other forms of identifying information to provide ever-more granular customer targeting capabilities.

3. Enforcement of Access Restrictions

Laws vary substantially from one jurisdiction to the next, such that content or services may be legal in one jurisdiction and unlawful in another. This variation creates a tremendous demand for geolocation technologies that can accurately screen users by jurisdiction, so as to allow online vendors to do as much business as possible without breaking the law. The demand for this type of jurisdiction-by-jurisdiction access management is arguably the genesis of modern geolocation technologies. In 2000, a French court ordered Yahoo! to block Nazi memorabilia from being displayed to French users via its auction sites, on pain of significant financial penalties.[52] Crucial to that holding was the court's determination that Yahoo! had the ability to

[49] *Id.*

[50] *Cf.* Mike Farrell, *Canoe to Launch in 4-6 Weeks: Cable's Interactive Advertising Efforts Row Along Slowly*, MULTICHANNEL NEWS, Apr. 6, 2009, http://www.multichannel.com/article/191286-Canoe_to_Launch_in_4_6_Weeks.php (describing a similar marriage of subscriber location data and census data for advertising purposes in the cable television context).

[51] Tedeschi, *supra* note 12. Note that in these cases, geolocation providers infer a user's connection speed from the user's IP address, rather than by detecting the speed directly. *Id.*

[52] Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, May 22, 2000, obs. J. Gomez*See* UEJF et LICRA v. Yahoo! Inc. et Yahoo France, T.G.I. Paris, May 22, 2000, No. RG: 00/05308 (Fr.); GOLDSMITH & WU, *supra* note 14, at 7–8 (noting that in November 2000 Judge Gomez reaffirmed that Yahoo violated Fench law by allowing Nazi paraphernalia to placed for sale on their web page).

install a primitive type of geographic controls.[53] Yahoo! defied the French court's ruling at first, but eventually complied—sending a signal to other online content providers that sovereign governments could force borders upon the previously unfenced Internet.[54]

Currently, some Internet gambling sites, such as Party Poker, employ geolocation tools to block users from jurisdictions where online gambling is illegal.[55] Similarly, Major League Baseball (MLB) uses geolocation to enable it to sell streaming access to games via the Internet—to the tune of $160 million annually—while still enforcing contractual exclusivity arrangements with broadcasters.[56] Thus, MLB's servers prevent an Internet user in Washington, D.C. from watching a Nationals game online while allowing a user in Chicago, which falls outside of the Nationals' home television market, to do so.

4. Fraud Prevention

Fourth, online retailers and banks now frequently use geolocation tools to prevent fraud, for example, to see whether a user is located in a country frequently associated with identity theft and online malfeasance.[57] If a user connecting from Russia is attempting to access an account belonging to an Ohio resident, for instance, the site can then respond by asking a series of security questions or by blocking access. This capability is particularly significant when one considers a recent report concluding that "73% of [transactions] where the state in [a user's] credit-card billing address doesn't match the state associated with the [user's] IP address" are fraudulent.[58] Given

[53] *See* GOLDSMITH & WU, *supra* note 14, at 8 (noting that the judge in *UEJF v, Yahoo!* indicated that at the time Yahoo! was tailoring content for France and had the capability to identify and screen users by geography); s*ee also id*. at 59 (describing primitive forms of geotechnology prior to that used by Yahoo in the Yahoo case, such as "'choose a country' and 'choose a server' links").

[54] *See id*. at 8.

[55] *See* King, *supra* note 1, at 60 n.101; *see also* Richmond, *supra* note 6 (stating online gambling provider Ultimate Blackjack Tour LLC also uses geolocation software).

[56] *See* Richmond, *supra* note 6; *see also* Tedeschi, *supra* note 12 (indicating Major League Baseball's heavy reliance on geolocation technology for its webcasts of games).

[57] *See* Richmond, *supra* note 6 ("For e-commerce sites, the goal is threefold: to reduce fraud, reject as few legitimate orders as possible and minimize costly manual reviews of transactions.").

[58] *Id*.

the extraordinary difficulties associated with directly regulating online conduct by lone users in foreign jurisdictions—users privacy theorist Peter Swire refers to as hard to catch "mice"[59]—creative, server-side measures such as geolocation-based security may be the most realistic way to stem online fraud.

5. Traffic Analysis

Last, companies utilize geolocation tools to better understand which customers are visiting their site or are interested in particular products or services. [60] For example, a travel site like Expedia could determine which vacation destinations are of greatest interest to users from Ohio by using geolocation tools to identify trends among Ohio-based users. Geolocation tools can also be used to measure the effectiveness of a company's offline advertising efforts. If, for instance, a retailer advertises its site on cable networks across the country, the retailer can use geolocation tools to identify incoming users by Designated Market Area (DMA) or Metropolitan Statistical Areas (MSA).[61] In contrast to the four uses described above this class of use is essentially passive, as a site using geolocation does not modify content or regulate access based on geolocation data.[62]

Just a decade ago, each of the applications detailed above simply were not possible, due to the distributed nature of the Internet's architecture.[63] But geolocation technologies are now well within the mainstream of electronic commerce and are poised to further revolutionize the way retailers, advertisers, banks, content distributors, and service providers interact with end users. The more recent emergence of less costly client-side geolocation tools will further broaden the technology's market penetration by making it possible for smaller entities to customize content and regulate access by a user's location.[64]

---

[59] *See* Peter Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, 153 U. PA. L. REV. 1975, 1978–79 (2005).

[60] *See Why: Analyze Traffic*, QUOVA, http://www.quova.com/why/analyze-traffic/ (last visited Jan. 5, 2011) (describing Quova's capabilities of locating a visitor's Country, State, Region, City, Zip Code and Area Code through a user's IP address).

[61] *See Why: Target Advertising*, QUOVA, http://www.quova.com/why/target-advertising/ (last visited Jan. 5, 2011).

[62] *See Why: Analyze Traffic*, *supra* note 60.

[63] *See* GOLDSMITH & WU, *supra* note 14, at 6.

[64] *See Berkeley W3C Study*, *supra* note 3, at 13; *see also Why: Control Use of Digital Media*, QUOVA, http://www.quova.com/why/control-use-of-digital-media/

Though the market has fully embraced modern geolocation, as Parts III through V demonstrate, the law has yet to do so.

III. GEOLOCATION AND PERSONAL JURISDICTION: A CRITIQUE OF THE *ZIPPO* TEST

The 1997 decision in *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*[65] ushered in a new era of personal jurisdiction law designed specifically for application to the Internet. Building on the U.S. Supreme Court's "purposeful availment" line of cases, the *Zippo* court established a sliding scale of interactivity under which "active" websites—those which clearly do business within the forum state via the Internet—are subject to personal jurisdiction while "passive" sites—those that do "little more than make information available" to forum state users—are not.[66] For sites falling somewhere in between these two extremes, the test considers "the level of interactivity and commercial nature of the exchange of information that occurs" on the site to make a determination.[67]

In *Zippo*, Zippo Manufacturing Corporation, a Pennsylvania-based manufacturer of tobacco lighters, sued Zippo Dot Com, Inc., a California-based website operator, for trademark infringement.[68] Dot Com registered several domain names including Manufacturing's trademarked name, such as zippo.com and zippo.net, without Manufacturing's permission.[69] Dot Com then used these domains for online advertisements and subscription-based news services, both of which also made unauthorized use of Manufacturing's trademark.[70] After Dot Com moved to dismiss for lack of personal jurisdiction, the district court responded with the decision now famous for the sliding scale analysis described above.[71] In that decision, the

(last visited Jan. 5, 2011); *Why: Localize Content*, QUOVA, http://www.quova.com/why/localize-content/ (last visited Jan. 5, 2011).

65 952 F. Supp. 1119 (W.D. Pa. 1997).

66 *Id.* at 1124–27.

67 *Id.* at 1124.

68 *Id.* at 1120–21.

69 *Id.* at 1121–22; *see also* Zippo Manufacturing Co. Motion for Summary Judgment at 3–6, Zippo Mfg. Co., v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997) (No. 96-397) (arguing court should enter judgment against defendant due to creation of websites using plaintiff's name without permission).

70 *Zippo Mfg. Co.,* 952 F. Supp at 1121–22.

71 *Id.* at 1124.

court found that Dot Com was subject to personal jurisdiction in Pennsylvania—though interestingly the court refused to rest its decision on the interactivity of Dot Com's websites.[72] Rather, the court focused on the fact that Dot Com had contracts with approximately 3,000 Pennsylvania-based subscribers, all of whom provided their name and address prior to purchasing a subscription, as well as several Internet Service Providers in the state.[73] Because "Dot Com repeatedly and consciously chose to process Pennsylvania residents' [news subscription] applications" and knowingly transmitted electronic news messages into Pennsylvania, the court found that Dot Com had purposefully availed itself of the benefits of Pennsylvania law.[74] Moreover, since much of the alleged trademark dilution and resulting injury occurred within Pennsylvania, the court found that Manufacturing's trademark claims arose out of Dot Com's online activities within the state.[75]

In the decade plus that has passed since *Zippo* was decided, nearly every federal court of appeals has adopted the test announced in that case in one form or another.[76] As technology has continued to evolve, the *Zippo* test has failed to evolve with it. For instance, the test does not account for a site's use of geolocation tools.[77] More importantly, a rote application of

---

[72] *See id*. at 1125–26 ("This is not . . . an interactivity case . . . . We are not being asked to determine whether Dot Com's Web site alone constitutes the purposeful availment of doing business in Pennsylvania.").

[73] *Id*. at 1121, 1125–26.

[74] *Id*. at 1126–27.

[75] *Id*. at 1127.

[76] *See* McBee v. Delica Co., 417 F.3d 107, 124 (1st Cir. 2005); Toys "R" Us, Inc., v. Step Two, S.A., 318 F.3d 446, 452 (3d Cir. 2003); ALS Scan, Inc., v. Digital Serv. Consultants, Inc., 293 F.3d 707, 714–14 (4th Cir. 2002); Mink v. AAAA Dev. LLC, 190 F.3d 333, 336 (5th Cir. 1999); Neogen Corp., v. Neo Gen Screening, Inc., 282 F.3d 883, 890 (6th Cir. 2002); Jennings v. AC Hydraulic A/S, 383 F.3d 546, 549–50 (7th Cir. 2004); Lakin v. Prudential Secs., 348 F.3d 704, 710–12 (8th Cir. 2003); Gator.com Corp., v. L.L. Bean, Inc., 341 F.3d 1072, 1079–80 (9th Cir. 2003); Soma Med. Int'l v. Standard Chartered Bank, 196 F.3d 1292, 1296 (10th Cir. 1999). *But see* Best Van Lines, Inc., v. Walker, 490 F.3d 239, 252 (2d Cir. 2007) (rejecting the *Zippo* framework in favor of "'traditional statutory and constitutional principles'" governing personal jurisdiction (quoting Best Van Lines, Inc., v. Walker, No. 03 Civ. 6585, 2004 U.S. Dist. LEXIS 7830, at *9 (S.D.N.Y. May 4, 2004))); Gorman v. Ameritrade Holding Corp., 293 F.3d 506, 510–11 (D.C. Cir. 2002) (same). As a Florida district court recently noted, the Eleventh and Federal Circuits have not yet definitively adopted or rejected the *Zippo* framework. *See* Roblor Mktg. Group Inc. v. GPS Indus., Inc., 645 F. Supp. 2d 1130, 1138–41 (S.D. Fla. 2009).

[77] *See* Svantesson, *supra* note 1, at 104 n.16, 105–06 (discussing the *Zippo* sliding scale analysis).

Zippo's active/passive classification scheme can result in erroneous results depending on the way in which a site is using geolocation technologies. For these reasons, this Part argues that the *Zippo* test should be modified to explicitly consider a site's use (or non-use) of geolocation technologies in determining whether the site is subject to specific jurisdiction. Under this modified framework, sites failing to employ geolocation tools would not, contrary to Professor Joel Reidenberg's view, automatically be subject to personal jurisdiction in every locale. Rather, personal jurisdiction determinations would depend on the costs of implementation, the legal significance of geography to the underlying online conduct, the burden on protected speech, and the broader consequences associated with finding jurisdiction.

A. The Zippo Test and its Roots

As with all of personal jurisdiction law, the *Zippo* test is rooted in constitutional due process considerations.[78] Because few websites engage in "systematic and continuous" contact with any given state, the *Zippo* test contemplates an analysis under the doctrine of specific jurisdiction.[79] To be consistent with the Due Process Clauses of the Fifth and Fourteenth Amendments, an exercise of specific personal jurisdiction requires a showing that: "(1) a defendant has made "sufficient 'minimum contacts' with the forum state; (2) the claim asserted against the defendant [ ] arise[s] out of those contacts, and [that] (3) the exercise of jurisdiction [would be] reasonable [under the circumstances]."[80]

In most cases, the "minimum contacts" prong of this test contemplates the establishment of continuing relationships with and obligations to forum state residents[81] such that the defendant "purposefully avails itself of the privilege of conducting activities within the forum state, thus invoking the benefits and

[78] *Zippo Mfg. Co.*,952 F. Supp. at 1122–23, 1127.

[79] *Id.* at 1122.

[80] *Id.* at 1122–23(citing Mellon Bank (East) PSFS, Nat. Ass'n v. Farino, 960 F.2d 1217, 1221 (3d Cir. 1992)); *see* World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980) (analyzing whether "the defendant's conduct and connection with the forum State are such that he should reasonably anticipate being hauled into court there"); *see also* Shaffer v. Heitner, 433 U.S. 186, 187 (1977) (considering the relationship "among the forum [ ], the defendant, and the litigation").

[81] *See* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 474–75 (1985).

protections of its laws."[82] Where intentional torts are concerned, however, jurisdiction is proper in the absence of purposeful availment so long as the defendant "expressly aimed" its tortious behavior towards the forum state.[83] The reasonableness prong, on the other hand, focuses on whether an exercise of jurisdiction would run contrary to "traditional notions of fair play and substantial justice"[84]—a concept that encompasses the burden on the defendant, "'the forum state's interest in adjudicating the dispute,'" the plaintiff's interest in securing a convenient forum, and overall considerations of interstate judicial economy and efficiency.[85]

Zippo's staying power is largely attributable to the court's translation of these amorphous due process principles to the Internet setting. At the time *Zippo* was decided, only a few cases had considered the question of jurisdiction over out-of-state Internet sites, meaning that the court was largely free to write on a blank slate.[86] At the time, Professor Martin Redish argued that courts had four basic options with respect to personal jurisdiction over Internet sites:

offering a product or service via the Internet "automatically constitutes nationwide purposeful availment, [thus] rendering the defendant subject to suit in any forum in which its product or service has caused harm[;]"[87]

online acts should be converted to offline equivalents, which would then be used to determine whether jurisdiction is appropriate;[88]

using a website is never, standing alone, sufficient to constitute purposeful availment—even if the defendant's online

---

[82] Hanson v. Denckla, 357 U.S. 235, 253 (1958).

[83] *See* Calder v. Jones, 465 U.S. 783, 789–90 (1984) (discussing how petitioners' intentional and tortious actions were "expressly aimed" at the state); *see also* Martin H. Redish, *Of New Wine and Old Bottles: Personal Jurisdiction, the Internet, and the Nature of Constitutional Evolution*, 38 JURIMETRICS J. 575, 596–600 (1998) (discussing the impact of the *Calder* decision).

[84] *See* Int'l Shoe Co. v. Washington, Office of Unemployment Comp. & Placement, 326 U.S. 310, 316 (1945); Zippo Mfg. Co. v. Zippo Dot Com, 952 F. Supp. 1119, 1123 (W.D. Pa. 1997) (quoting *World-Wide Volkswagen*, 444 U.S. at 292).

[85] *Id.*

[86] *See id.* at 1123–24.

[87] Redish, *supra* note 83, at 585.

[88] *Id.* at 586 ("Under such an approach, a court would treat the Internet exactly as it would a defendant's resort to . . . traditional marketing methodologies.").

activity would give rise to jurisdiction if conducted via offline means;[89] or

Internet use is one of many relevant factors bearing on the propriety of jurisdiction.[90]

The *Zippo* test most closely resembles the third and fourth of these options, given the test's foundation on a "sliding scale" measuring "the nature and quality of commercial activity that an entity conducts over the Internet."[91] Analogizing to *Burger King*, the *Zippo* court concluded that jurisdiction is proper when "a defendant clearly does business over the Internet[,]" as evidenced by "contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet . . . ."[92] The court contrasted these "active" cases with those in which a "passive" defendant "has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions."[93] When a site cannot be easily classified as falling within one of the two categories above, the court stated that jurisdiction depends on an examination of "the level of [the site's] interactivity and [the] commercial nature of the exchange of information . . . ." which takes place on the site.[94]

B. Doctrinal Development Since 1997

As noted above, most courts have embraced *Zippo* in the years that have passed since 1997.[95] Throughout this process, the doctrine has slowly evolved, such that courts in each circuit apply the *Zippo* test in a slightly different manner. Currently, the majority rule states that a website operator purposely avails when it "knowingly conducts business with forum state residents via [its] site . . . ."[96] This test involves both a *Zippo* interactivity

[89] *Id.* ("[A] court may conclude that creation of an Internet home page can never, standing alone, meet the requisite purposeful availment standard, regardless of how it would view more traditional marketing devices.").

[90] *Id.* (describing what Redish refers to as the "'Internet plus' approach").

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

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *See* cases cited in *supra* note 76.

[96] Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446, 452 (3d Cir. 2003). Other courts have offered similar formulations. *See* ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 714–15 (4th Cir. 2002) (following the *Zippo* passive Web site standard); Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 417 (9th Cir. 1997) (finding purposeful availment when a site "'take[s] deliberate action within the forum state or . . . create[s] continuing obligations

analysis, and consideration of the degree to which the site's interactive features are actually used by residents of the forum state.[97] The threshold for in-state use is generally quite low, as courts have found this requirement met when a site received ten percent of its international revenue from the forum state,[98] and when a retailer sold thirty eight items to a total of twelve buyers in the forum state over five years.[99] Courts also consider other factors when determining whether jurisdiction is appropriate, such as the language used by a website,[100] a site's use of resellers in the forum state,[101] the currency in which a site lists its goods,[102] and the extent of "offline" contacts between a site's operator and the forum state.[103]

Some circuits have criticized the *Zippo* test as too simplistic for regular use, however.[104] Recently, the Eleventh Circuit noted

to forum residents.'" (quoting Ballard v. Savage, 65 F.3d 1495, 1498 (9th Cir. 1995))).

97 *See Toys "R" Us*, 318 F.3d at 454; *see also ALS Scan*, 293 F.3d at 713–15 ("[A]dopting and adapting the *Zippo* model . . . ."); *Cybersell*, 130 F.3d at 418–20 (following *Zippo* and focusing on use of the defendant's site by forum state residents).

98 M. Shanken Commc'ns, Inc. v. Cigar500.com, No. 07 Civ. 7371, 2008 U.S. Dist. LEXIS 51997, at *12–13 (S.D.N.Y. July 7, 2008).

99 Ty, Inc. v. Sullivan, No. 01 C 1604, 2002 U.S. Dist. LEXIS 4807, at *1–2 (N.D. Ill. Mar. 11, 2002). For other examples, see Licciardello v. Lovelady, 544 F.3d 1280 (11th Cir. 2008); Foreign Imported Prods. & Publ'g, Inc. v. Grupo Indus. Hotelero, S.A., No. 07-22066, 2008 U.S. Dist. LEXIS 108705, at *30–33 (S.D. Fla. Oct. 24, 2008).

100 *See Toys "R" Us*, 318 F.3d at 454 (finding that a company's website, written entirely in the Spanish language, was insufficient to meet the "purposeful availment" prong required to satisfy personal jurisdiction requirements); *see also Foreign Imported Prods.,* No. 07-22066, 2008 U.S. Dist. LEXIS 108705, at *31–32 (finding that the purposeful availment prong of the jurisdictional standard was met where information on the company's website could be read in the English language).

101 *See Foreign Imported Prods.,* No. 07-22066, 2008 U.S. Dist. LEXIS 108705, at *31–34 (finding that promotional advertisements on the foreign company's Internet site, which were directed toward Florida travel agencies, established sufficient business contacts to support the 'minimum contacts' requirement for personal jurisdiction).

102 *See Toys "R" Us*, 318 F.3d at 454.

103 *See id.* at 453–54; *Foreign Imported Productions*, 2008 U.S. Dist. LEXIS 108705, at *32–33 (stating that Defendants' attendance at trade shows in Florida "elevat[ed] Defendants' contacts with Florida from foreseeable to deliberate. . . ." (citing World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 314 (1980))). Note, however, that directing dozens of faxes, e-mails, and telephone calls into the forum state, without more, does not qualify under this rule. *See* FC Inv. Grp. LC v. IFX Mkts., Ltd., 479 F. Supp. 2d 30, 38–41 (D.D.C. 2007).

104 *See* Oldfield v. Pueblo De Bahia Lora, S.A., 558 F.3d 1210, 1219 n.26 (11th

sharp criticism of *Zippo* by academic commentators, including claims that *Zippo* is unpredictable and "inconsistent with traditional due process analysis because . . . the level of interactivity is of minimal significance with respect to whether a defendant has directed [its] website towards the forum."[105] The Second Circuit echoed these sentiments in *Best Van Lines, Inc. v. Walker* when it concluded that *Zippo*'s sliding scale analysis may "help frame the jurisdictional inquiry in some cases . . . [but,] 'it does not amount to a separate framework for analyzing internet-based jurisdiction.'"[106] Rather, the court held that "'traditional statutory and constitutional principles remain the touchstone'" of the personal jurisdiction inquiry.[107] Under this approach, the court would decide personal jurisdiction in Internet cases no differently than any other class of cases, with a party's physical and economic contacts with a state, as well as limitations embedded in the forum state's long-arm statute, serving as the focal point.[108]

Such a return to constitutional first principles is precisely what Professor Redish had in mind over a decade ago when he proposed that the Supreme Court eliminate the purposeful availment test altogether, using Internet cases as the starting point for this transformation.[109] Redish argued that such a dramatic step is necessary because most cases involving harms inflicted via the Internet will seldom involve purposeful availment.[110] In this sense, the Internet makes it easy to inflict harm on out-of-state residents without "affirmatively . . . connect[ing] oneself with the forum state for the purpose of acquiring benefits and privileges from that

Cir. 2009) (declining to apply the *Zippo* test in light of its failure "to preserve the constitutionally required 'foreseeability' and 'fairness' principles" of the traditional test. (citation omitted)); Best Van Lines, Inc. v. Walker, 490 F.3d 239, 252 (2d Cir. 2007) (finding that the Zippo test merely informs the traditional test for personal jurisdiction); Gorman v. Ameritrade Holding Corp., 293 F.3d 506, 510–13 (D.C. Cir. 2002) (asserting the adaptability of the traditional test as sufficient to determine personal jurisdiction in cases that involve the Internet).

[105] *Oldfield*, 558 F.3d at 1220 n.26.

[106] *Best Van Lines,* 490 F.3d at 252(quoting Best Van Lines, Inc. v. Walker, No. 03 Civ. 6585, 2004 WL 964009, at *3 (S.D.N.Y. May 5, 2004)).

[107] *Id.* (quoting Best Van Lines, Inc. v. Walker, No. 03 Civ. 6585, 2004 WL 964009, at *3 (S.D.N.Y. May 5, 2004)).

[108] *Id.*

[109] *See* Redish, *supra* note 83, at 601–05.

[110] *Id.* at 580, 602, 604.

state."[111] Thus, to require purposeful availment in Internet cases is to deny states the ability to protect their interests or those of their citizens—two of the key considerations animating the Supreme Court's personal jurisdiction jurisprudence.[112] At bottom, these considerations emanate from the Due Process Clause of the Fourteenth Amendment, which demands that courts consider not only "the quality and nature" of a defendant's contacts with a forum state, but also the defendant's "obligations" to the state and its citizens, enforced through the state's judicial system.[113]

In place of the purposeful availment rule (and by extension the *Zippo* test built thereupon), Professor Redish argued that the Court should adopt a new test for Internet jurisdiction cases that "would focus initially on considerations of state interest and procedural fairness. The two factors would correlate inversely: The stronger the state interest in asserting jurisdiction, the greater the procedural burdens on the out-of-state defendant the court should be willing to tolerate."[114] As Professor Redish hinted, this proposed standard shares several similarities with the *Calder*[115] "express aiming" test currently reserved for cases involving intentional torts.[116] Although the Supreme Court has not discarded the purposeful availment test,[117] Professor Redish's critique of the purposeful availment test seems as valid today as

---

[111] *Id.* at 580.

[112] *Id.* at 580; *see* Int'l Shoe Co. v. Wash., Office of Unemployment Comp. & Placement, 326 U.S. 310, 316 (1945) ("[I]t is a denial of due process to subject it to taxation or other money exaction. It thus denies the power of the state to lay the tax or to subject appellant to a suit for its collection."). In addition to this pragmatic objection, Professor Redish also argued that "[f]rom a conceptual . . . perspective, the [purposeful availment] standard is the outgrowth of a constitutionally illegitimate focus on interstate federalism, which has no independent grounding in the text of the Constitution and which has no conceptual or historical relevance to the considerations of Fourteenth Amendment procedural due process." Redish, *supra* note 83, at 601.

[113] *International Shoe*, 326 U.S. at 319.

[114] *See* Redish, *supra* note 83, at 609; Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1122–25 (W.D. Pa. 1997) (describing the test to determine when "the exercise of specific personal jurisdiction over a non-resident is appropriate").

[115] Calder v. Jones, 465 U.S. 783 (1984).

[116] *Id.* at 789–90 (setting forth the express aiming test, which differentiates between the effect of "mere untargeted negligence" and "tortious[ ] actions . . . expressly aimed" on jurisdiction over a party). *Cf.* Redish, *supra* note 83, at 603–05.

[117] *Zippo Mfg. Co.*, 952 F. Supp. at 1123 (citing Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985)).

it was over ten years ago. *Zippo* is indeed imperfect in many ways, one of which is sketched out in the section that follows.

C. Modern Geolocation Technologies Render the Zippo Test Incomplete

The *Zippo* test was conceived in an era in which geolocation was presumed to be impossible. The same year *Zippo* was decided, a celebrated district court opinion humbly announced that "[t]he Internet is wholly insensitive to geographic distinctions" and that "Internet protocols were designed to ignore rather than document geographic location."[118] As demonstrated in Part II, in the last decade the Internet has not only become sensitive to geographic distinctions; much of the commerce that takes place online has come to *rely on* such distinctions. Yet the *Zippo* test has failed to adapt to these changed circumstances. Only a miniscule number of cases applying the *Zippo* test's many iterations mention, much less consider the impact of geolocation on the jurisdictional analysis.[119]

Professor Reidenberg has argued convincingly that the *Zippo* test's failure to account for sites' use (or non-use) of geolocation technologies will often lead to erroneous results.[120] In Reidenberg's view, early cases such as *Zippo* were far too solicitous of a "naïve view of the Internet" reflective of "Internet activists' simple denial of law"[121]—i.e., the notion that cyberspace is a separate sphere, immune from legal control from offline sovereigns.[122] Thus, the early doctrine must be re-worked to ensure that states can adequately enforce the rule of law and protect their citizens from digitally-inflicted harms—a theme common to both Reidenberg and Redish's respective proposals. In this sense, Reidenberg argues that the rise of "geolocation and

[118] Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 170 (S.D.N.Y. 1997); *see also* GOLDSMITH & WU, *supra* note 14, at 13–27 (explaining that early Internet thinkers and engineers conceptualized and designed the Internet with the purpose of evading regulation by traditional sovereign entities).

[119] At the time of this writing, a Lexis search for the terms "Zippo AND geolocation" returns only one result: ACLU v. Gonzales, 478 F. Supp. 2d 775 (E.D. Pa. 2007). That decision mentions the two concepts in entirely different sections and considers jurisdictional issues only in passing. *Id.* at 807, 811.

[120] Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951, 1955–56, 1961–62 (2005).

[121] *Id.* at 1955–56.

[122] *See* GOLDSMITH & WU, *supra* note 14, at 13–17, 23, 27 (explaining that the early Internet thinkers and engineers believed that the Internet could and should exist separately from any kind of government jurisdiction).

the re-creation of geographic origin and destination . . . mean that Internet activity is 'purposely availing' throughout the Internet whenever content is posted without geolocation filtering."[123] This conclusion, Reidenberg asserts, follows from the notion that widespread availability of geolocation tools "shifts the burden from demonstrating that a jurisdiction was targeted to showing that reasonable efforts were made to avoid contact with the jurisdiction."[124] This expansive view essentially amounts to an effects test in which a party is subject to jurisdiction whenever it has targeted a forum and caused "deleterious effects within the forum" via its online acts.[125]

A brief example illustrates Reidenberg's argument that some forms of online behavior should be subject to personal jurisdiction even if a straightforward application of the *Zippo* test would indicate otherwise. Imagine a website based in Russia that contains only one element: streaming video of child pornography that is clearly illegal in the United States and other jurisdictions. The site employs no geolocation tools of any kind, and its operators make no effort to determine which jurisdictions users visit from. Further, the site contains no advertising, offers no products or services for sale, and makes no use of individual accounts, message boards, or other interactive features.

Under the *Zippo* test, this hypothetical site clearly falls on the passive side of the scale. The site does not serve as a vehicle for any form of commercial exchange between host and user, and features no interactivity. More importantly, the site falls squarely within *Zippo*'s paradigm case for passivity, since the site operator has "simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions."[126] Since the site is passive, a court following *Zippo* would conclude that the site could not be subject to personal jurisdiction in a U.S. forum.

When one applies Reidenberg's theory instead of *Zippo*, however, the jurisdictional result changes. Under this theory, one starts by asking whether the site has caused harm within the forum state.[127] Here in the scenario presented, the information

---

[123] Reidenberg, *supra* note 120, at 1956.

[124] *Id.* at 1962.

[125] *Id.* at 1955–56, 1962.

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

[127] Reidenberg, *supra* note 120, at 1955–56.

being displayed is unquestionably illegal,[128] and can thus be presumed to cause harm. Having made that determination, Reidenberg would find personal jurisdiction because the site (1) must "avail" itself of the processing power of a user's computer to display the streaming video; and (2) could have employed geolocation tools to block access to users in jurisdictions in which child pornography is illegal.[129]

Whereas the *Zippo* test does not even consider a site operator's choice to use or not use available geolocation tools, Professor Reidenberg's approach places nearly dispositive weight on that question.[130] This difference between the two tests means that otherwise passive sites could be subject to personal jurisdiction if they fail to employ available screening measures. Similarly, active sites might be able to escape jurisdiction by using geolocation tools to block users within a forum state. Even if some in-state users were able to evade those access controls, a plaintiff would still be unable to show that the site engaged in the kind of "*purposeful* conduct directed at the State" needed to obtain specific jurisdiction.[131] In light of these differences, Part III.D seeks to refine Reidenberg's approach and, in doing so, better adapt the *Zippo* test for an era in which geolocation is becoming a commercial norm.

D. The Zippo Test Should Be Expanded to Include Consideration of a Party's Use (or Non-Use) of Geolocation Technologies

Because the active/passive distinction often breaks down once one considers a site's use or non-use of geolocation tools, the *Zippo* test is in need of an upgrade. This section argues for a modified *Zippo* test under which a site's use of geolocation technologies is relevant to, but not dispositive of the specific jurisdiction inquiry. These relevancy considerations vary depending on whether a site has chosen to utilize geolocation

[128] *See* 18 U.S.C. § 2252A (2010) (identifying various child pornography offenses and corresponding punishments).

[129] Reidenberg, *supra* note 120, at 1962 ("The technological attack against jurisdiction cannot be justified where information processing resources within the sovereign state are enlisted by remote Internet participants and where sophisticated Internet participants can, if they desire, avoid the global scope of their online activities.").

[130] *Id.* at 1961–62.

[131] ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 713 (4th Cir. 2002).

technologies or not.

When a site elects to use geolocation tools to target users within a particular forum state, such use will almost always be relevant to *Zippo*'s interactivity analysis, while simultaneously being irrelevant to *Calder* intentional tort cases. However, when a site employs geolocation tools to block users from a forum state, those efforts should—so long as they are executed in a reasonable manner—militate heavily towards a denial of personal jurisdiction. On the other hand, a site's failure to use geolocation tools to screen users should not, as Reidenberg claims, automatically give rise to personal jurisdiction.[132] Instead, courts should consider the costs of implementing geolocation tools, the legal significance of geography to the underlying online conduct, the burden of a geolocation mandate on protected speech, and the broader consequences associated with finding jurisdiction. This more nuanced approach is superior to Reidenberg's *per se* approach, because it is more compatible with the First Amendment, more sensitive to differences between commercial and non-commercial sites, and more consistent with the Internet's longstanding tradition of widespread content availability.

The sections below explicate these modifications to the *Zippo* test, starting with cases where a site has employed some form of geolocation technology.

1. Application to Sites that Use Geolocation Technologies

As described in Part II.B, geolocation technologies are currently used for a variety of purposes. Some of these uses, such as content localization and enforcement of access restrictions, are of great relevance to personal jurisdiction determinations, while others, such as traffic analysis, are not. Accordingly, the mere use of geolocation tools cannot determine the outcome of a *Zippo* interactivity analysis. Rather, courts should consider the use to which geolocation tools are put and the connection between that use and the wrongful conduct in question.

[132] Reidenberg, *supra* note 120, at 1961–62 ("In effect, the technological choice either to filter or not to filter becomes a normative decision to 'purposefully avail' of the user's forum state.").

a. Sites that Use Geolocation Tools to Target a Forum State

When a site uses geolocation tools to target users within a forum state, for instance by localizing content, that targeting effort will generally be relevant to cases falling in the *Zippo* scale's middle ground.[133] These cases typically involve classifying sites according to two factors: the "level of interactivity" and [the] commercial nature of the exchange of information that occurs on the Web site."[134] By definition, localization or customization of content according to a user's geographic location constitutes a form of interactivity.[135] The same holds true when a site employs geolocation tools to prevent fraudulent purchases or account access attempts.[136] Despite Reidenberg's claims to the contrary,[137] geo-targeting in this manner will not always be sufficient to support jurisdiction, since not every attempt to target a forum state will invoke the benefits and protections of the forum's laws.[138] For example, if a politics blog utilized geolocation tools to ensure that stories relevant to local House and Senate races are featured at the top of the page, that use would target a user's state without invoking the benefits of the forum state's laws[139] or establishing any continuing relationships or obligations within the forum state.[140]

Intentional tort cases present a different calculus. In *Calder v. Jones*, the Supreme Court upheld a California court's assertion of personal jurisdiction over a Florida-based newspaper publisher

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

134 *Id.*

135 *See supra* Part II.B.3.

136 *See supra* Part II.B.4.

137 *See* Reidenberg, *supra* note 120, at 1961 ("[S]treaming video purposefully avails itself of the user's computing capability at the user's location."); *id.* at 1962 ("Technological innovation that enhances interactivity also shifts the burden from demonstrating that a jurisdiction was targeted to showing that reasonable efforts were made to avoid contact with the jurisdiction.").

138 *See* Hanson v. Denckla, 357 U.S. 235, 253 (1958) (noting that the court lacked personal jurisdiction over a nonresident defendant in an action over a trust because there was no act which granted defendant the protections and benefits of the forum state).

139 *See id.* (explaining that a nonresident defendant must "purposefully avail[ ] itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws" in order for there to be personal jurisdiction).

140 *See* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475–76 (1985) (holding that when a defendant has created continuing obligations in the forum state, it is not unreasonable for him to be subject to jurisdiction there).

because the publisher's "intentional, and allegedly tortious, actions were expressly aimed at California" and because "California [was] the focal point both of the story and of the harm suffered" by the plaintiff.[141] As Professor Redish notes, the Court "refused to find that the defendants had purposefully availed themselves of the benefits" of California's laws in reaching this conclusion—a decision characterized by Redish as a dramatic and inexplicable departure from the purposeful availment standard announced in *World-Wide Volkswagen*.[142] Confronted with this inconsistency, lower courts have interpreted *Calder*'s more relaxed effects test as limited to intentional tort cases.[143] Thus, where tortious communications over the Internet are concerned, the *Calder* test likely supports jurisdiction independent of a site's use or non-use of geolocation tools.[144] Defamatory speech directed specifically at an Illinois plaintiff, for instance, targets Illinois almost regardless of the medium by which it is published—thus rendering superfluous any inquiry into whether an online medium took the added step of using geolocation tools to ensure that the communication reached users in Illinois.[145]

b. Sites that Use Geolocation Tools to Restrict Access by Jurisdiction

As discussed in Part II.B, geolocation tools are often used to regulate access to content depending on whether it is legal within a user's jurisdiction. Common examples of this use include Major League Baseball's use of geolocation to stream live games on the Internet without breaching regional broadcasting rights agreements[146] and European Internet gambling sites' efforts to

[141] Calder v. Jones, 465 U.S. 783, 789–90 (1984).

[142] Redish, *supra* note 83, at 583–85.

[143] *See id.* at 584 & n.50.

[144] *See* Tamburo v. Dworkin, 601 F.3d 693, 702–04, 703 n.7 (7th Cir. 2010) (noting that intentional tort allegations are brought within the *Calder* formula irrespective of whether there is any "express aiming" at the forum state (citing Calder v. Jones, 465 U.S. 783(1984))); Baldwin v. Fischer-Smith, 315 S.W.3d 389, 392, 398, 394–95 (Mo. Ct. App. 2010) (concluding in an Internet defamation case involving out-of-state defendants that "if you pick a fight in Missouri, you can reasonably expect to settle it here")).

[145] Additionally, the plaintiff in such a case suffers harm in Illinois even when the defamatory speech is published solely in other jurisdictions. *See Calder*, 465 U.S. at 788–91 (finding that California had jurisdiction over a reporter and an editor who were residents of Florida due to their calculated and intentional conduct to cause injury in California).

[146] *See* Ben Klayman, *Major League Baseball Awarded Geolocation Patent*,

block users within the United States, where provision of online gambling services is illegal.[147] Under a *Zippo* analysis, many sites using geolocation to restrict access by jurisdiction nonetheless nominally qualify as "active" sites—certainly both the subscription-based MLB.tv site and the highly interactive PartyPoker gambling service fit this description.

"Active" sites that employ geolocation tools to block users from a forum state should not be subject to personal jurisdiction. The *Zippo* test itself hints at this outcome, in that it highlights "the *knowing* and repeated transmission" of content to forum state users.[148] The *purposeful* availment standard that undergirds the *Zippo* test likewise suggests that when a site has attempted to exclude forum state users, it should not be subject to jurisdiction.[149] Yet not all geolocation technologies are created equal and some may be implemented in name but not in substance—meaning that good faith efforts, rather than any efforts, to screen users by jurisdiction should be required for a site to escape jurisdiction when it would otherwise arise.[150]

When a site has utilized geolocation tools to block users from a particular jurisdiction or jurisdictions, a second question arises regarding those jurisdictions which are not blocked. For example, if a site blocks access to users in Alabama, Kentucky, and New York, should it be inferred that the site is subject to jurisdiction in California and every other state in which its content is available? Reidenberg argues that the answer must be yes.[151] That may be the right result most of the time. However, as a purely theoretical matter when a site fails to use geolocation to screen forum state users, *as to that particular state* the site is essentially one that does not use geolocation at all. Thus, the proper approach is to apply the framework in section 2 below while taking some account of the fact that the site has used geolocation tools to block users from other jurisdictions.

REUTERS, May 15, 2009, http://www.reuters.com/article/idUSTRE54E5Y220090515.

147 QUOVA INC., GEOLOCATION: ENSURING COMPLIANCE WITH ONLINE GAMING REGULATIONS, 4 (2010), *available at* http://www.quova.com/downloads/wp-gaming-compliance.pdf.

148 Zippo Mfg. Co. v. Zippo Dot Com Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (emphasis added).

149 *Id.* at 1125–27.

150 *See* King, *supra* note 1, at 64–67 (referring to the incentive for sites to build negligence into their screening systems).

151 Reidenberg, *supra* note 120, at 1956.

2. Application to Sites that Do Not Use Geolocation Technologies

In his critique of current personal jurisdiction doctrine, Reidenberg argues unapologetically that a site purposely avails itself of every jurisdiction "whenever content is posted without geolocation filtering."[152] This position amounts to a *per se* rule: when a site chooses not to use geolocation technologies to regulate access to its content, the site must be subject to personal jurisdiction in every forum in which the content is accessible.[153] Despite its elegance and simplicity, this rule is both contrary to established law and normatively undesirable. As Jack Goldsmith and Alan Sykes have written, it is simply "false to assume . . . that every website is exposed to liability in every jurisdiction where its content appears."[154]

Instead, when a site has failed to use geolocation to screen by jurisdiction, jurisdiction should depend on a balancing of the costs of implementation, the legal significance of geography to the underlying online conduct, the burden of a geolocation mandate on protected speech, and the broader consequences associated with finding jurisdiction. Although it offers less certainty than Reidenberg's approach, such a balancing test does a much better job of protecting important First Amendment values, of differentiating between commercial and non-commercial sites, and of upholding the Internet's fundamentally open character.

a. Reasons to Reject the Per Se Approach

Put simply, Professor Reidenberg's *per se* rule would violate the Due Process Clauses of the Fifth and Fourteenth Amendments. This rule would subject any site not utilizing geolocation tools to jurisdiction in every forum regardless of whether doing so would comport with the "'traditional notions of fair play and substantial justice"'[155] For example, there is simply

---

[152] *Id.*

[153] *Cf.* ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 712–13 (4th Cir. 2002) (explaining that the concept of personal jurisdiction would no longer exist with regard to Internet activity if merely placing information on the Internet subjected a person to personal jurisdiction).

[154] Goldsmith & Sykes, *supra* note 18, at 815.

[155] Int'l Shoe Co. v. Wash., Office of Unemployment Comp. & Placement, 326 U.S. 310, 316 (1945) (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)). *See* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475–78 (1985) (reciting

no way that a foreign non-profit site without the means to afford server-side geolocation tools "should reasonably anticipate being haled into court" in every jurisdiction in the world.[156] Though Reidenberg is undoubtedly correct that changes in technology can and should bring about changes in law, long ago the Supreme Court indicated that "it is a mistake to assume that [the technological] trend heralds the eventual demise of all restrictions" on the exercise of jurisdiction.[157] As the Fourth Circuit has concluded:

> If we were to conclude as a general principle that a person's act of placing information on the Internet subjects that person to personal jurisdiction in each State in which the information is accessed, then the defense of personal jurisdiction, in the sense that a State has geographically limited judicial power, would no longer exist.[158]

Reidenberg attempts to buttress his *per se* rule with a second argument: a site's active use of remote users' computing power, for instance by transmitting streaming video that must be decoded in order to be played back, constitutes purposeful availment.[159] This too is a misreading of precedent. While a site's employment of computing resources within a forum state may well be relevant to the personal jurisdiction inquiry in some fashion, purposeful availment requires more. Specifically, the minimum contacts prong demands that a defendant "purposefully avail[] itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protections [of the forum state's] laws."[160] A site that does nothing more than instruct a user's computer to decode digital video does not invoke, rely on, or even consider a state's laws; such a site in no way purposefully avails itself of the privilege of conducting activities within the user's state. Even if one could stretch purposeful availment to include Reidenberg's streaming

reasonableness requirement for specific jurisdiction (citations omitted)).

156 World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980).

157 Hanson v. Denckla, 357 U.S. 235, 250–51 (1958).

158 *ALS Scan, Inc.*, 293 F.3d at 712.

159 Reidenberg, *supra* note 120, at 1961 ("For example, streaming video purposefully avails itself of the user's computing capability at the user's location."); *id.* at 1956 ("Internet activity is 'purposely availing' throughout the Internet whenever content is posted without geolocation filtering.").

160 *Hanson*, 357 U.S. at 253. *See* Traveler's Health Ass'n v. Va. *ex rel.* State Corp. Comm'n, 339 U.S. 643, 647 (1950) (reasoning that jurisdiction will lie when a defendant "reach[es] out beyond one state and create[s] continuing relationships and obligations with citizens of another state").

video claim, precedent guarding against reliance on "random, isolated, or fortuitous" contacts to support jurisdiction would point towards a denial of jurisdiction.[161]

From a normative standpoint, the *per se* rule is undesirable due to its essentially legislative character and extreme overbreadth. Subjecting every site to jurisdiction unless the site uses geolocation tools imposes a tremendous cost on every single website populating the Internet, large and small. As noted in Part II, leading server-side geolocation tools cost between $6,000 and $500,000 per year.[162] Lower-cost client-side technologies are emerging, however, even those tools require a non-trivial amount of time and expertise to implement properly.[163] In this regard, geolocation technologies are very similar to the age verification technologies found to be cost-prohibitive, and thus "'effectively unavailable'" to non-commercial sites in *Reno v. ACLU*.[164] As the Court recognized in *Reno*, many sites would likely disappear when faced with a choice between paying for (and integrating) user identification tools on the one hand, and simply shutting down on the other.[165] For these reasons, the question of whether to impose a geolocation cost on all, or even some, websites is one that is best—and perhaps only—suited to federal and state legislatures.

In terms of breadth, the *per se* rule reaches further than it needs to in order to accomplish Reidenberg's stated goal of enabling sovereigns to protect their citizens from online harms.[166] Most of Reidenberg's examples involve either intentional torts or major corporate parties, such as Dow Jones, RealNetworks, Verizon, and Yahoo!, all of which are presumably well-equipped to afford the cost of implementing geolocation technologies.[167] As a result, the *per se* rule could conceivably be limited to only those classes of cases, while exempting individual bloggers, small businesses, and non-profits from the geolocation mandate. Yet

---

[161] *See* Keeton v. Hustler Magazine, Inc., 465 U.S. 770, 774 (1984).

[162] *See* ACLU v. Gonzales, 478 F. Supp. 2d 775, 807 (E.D. Pa. 2007); *supra* notes 28–30 and accompanying text.

[163] *See Berkeley W3C Study*, *supra* note 3, at 7–9.

[164] *See* Reno v. ACLU, 521 U.S. 844, 856 (1997) (quoting ACLU v. Reno, 929 F Supp. 824, 846 (E.D. Pa. 1996).

[165] *See id.* at 856 ("Using credit card possession as a surrogate for proof of age would impose costs on non-commercial Web sites that would require many of them to shut down."); *id*. at 880 (discussing specific costs in dollar terms).

[166] *See* Reidenberg, *supra* note 120, at 1969.

[167] *See id.* at 1955–56, 1961–62.

Reidenberg's repeated assertion that "Internet activity is 'purposely availing' throughout the Internet whenever content is posted without geolocation filtering" shows that he intends no such limitation.[168]

To recap, despite its elegance and noble intentions, the *per se* rule should be rejected because it is unconstitutional, inconsistent with precedent, legislative in character, and acutely overbroad. As the next section demonstrates, however, many of the policy considerations animating the *per se* rule are worthwhile and should be retained in a modified *Zippo* test.

b. Reasons to Adopt the Balancing Approach

In place of the *per se* rule, when a site has failed to employ geolocation tools, courts should adopt a specific jurisdiction test that balances the costs of implementation, the legal significance of geography to the underlying online conduct, the burden of a geolocation mandate on protected speech, and the broader consequences associated with finding jurisdiction. The first of these factors, implementation costs, is essential due to the high cost of geolocation tools described above.[169] In theory geolocation tools are available to every Internet site. In practice, however, only some sites can realistically afford to employ them.[170] Thus, courts should consider whether a defendant could reasonably afford to implement geolocation technologies before demanding that the site do so to avoid personal jurisdiction.

One federal district court has already hinted at such an approach. In *National Federation for the Blind v. Target Corp.*, a suit involving application of a California law to retailer Target's online store, the court explicitly considered the economic feasibility of requiring Target to use geolocation to create a "separate website" for California users in denying Target's motion to dismiss.[171] In some cases, this factor may turn on a straightforward financial analysis: when a site has considerable online revenues, as Target and Yahoo! do via their websites, it is reasonable to conclude that the site can afford to implement

[168] *Id.* at 1956, 1961 (making a similar claim regarding streaming video).

[169] *See* ACLU v. Gonzales, 478 F. Supp. 2d 775, 807 (E.D. Pa. 2007); *supra* notes 29-32 and accompanying text.

[170] *See Reno*, 521 U.S. at 881 (discussing how some speakers are unable to afford the cost of geolocation technologies).

[171] *See* Nat'l Fed'n of the Blind v. Target Corp., 452 F. Supp. 2d 946, 960–62 (N.D. Cal. 2006).

geolocation tools. An individual blog with no revenues, on the other hand, would have an easy time showing a lack of affordability. When financial proof is contested or difficult to come by, courts should consider whether similar sites employ geolocation tools. For instance, a court might look to the practices of a commercial site's competitors to resolve this factor. The mere fact that no site within a particular class or industry uses geolocation tools should be insufficient to prove a lack of affordability, however.[172]

The next factor, the legal significance of geography to the underlying online conduct, speaks to the interaction between a state's protective interests and the variety of content available online. As a general matter, courts must consider "the forum State's interest in adjudicating the dispute" when making personal jurisdiction determinations.[173] The magnitude of a state's interest naturally varies depending on the type of conduct at issue, and reaches its maximum in areas that involve socially or economically controversial subject matter. As Jack Goldsmith and Tim Wu have written, "when communications on the Internet collide with sensitive local public policies like gambling, pornography, consumer protection, libel, and the like, there are strong reasons to prefer a decentralized approach."[174] In such cases, actors are generally well aware that the law varies significantly from one jurisdiction to the next and that they might be haled into court wherever their conduct has harmful or unlawful effects.[175] It may be reasonable to require an Internet gambling provider or tabloid newspaper to screen its users by jurisdiction, but unreasonable to require an online tic-tac-toe server or weather site to do so. When a site's business tends towards the sensitive side of this continuum, and thus falls within the core of a state's interest in protecting its citizens, the site should be more prone to personal jurisdiction when it fails to

---

[172] *Cf.* The T. J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) ("[I]n most cases reasonable prudence is in fact common prudence; but strictly it is never a measure; a whole calling may have unduly lagged in the adoption of new and available devices.").

[173] World Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 291–92 (1980) (citing McGee v. Int'l Life Ins. Co., 355 U.S 220, 223 (1957)).

[174] GOLDSMITH & WU, *supra* note 14, at 161.

[175] *Cf. World Wide Volkswagen*, 444 U.S at 297 (discussing the relevance of foreseeability to personal jurisdiction determinations); Kulko v. Cal. Super. Ct., 436 U.S. 84, 97–98 (1978) (discussing the reasonableness of a forum that the defendant has not personally availed himself of).

implement geolocation tools.

Third, the proposed balancing test considers the burden on protected speech. While the elements above are included because they tend to produce more sensible results, this element may be constitutionally required in light of the First Amendment. The Internet plays a central role in the free exchange of ideas in modern society, including core forms of protected speech, such as political debate.[176] Though not all laws that burden free speech are subject to strict scrutiny, even those that have only "an incidental effect on expressive conduct . . . [must] withstand[ ] intermediate scrutiny."[177] Under either test, courts would need to assess the potential chilling effect associated with requiring a particular site or class of sites to utilize geolocation tools in order to avoid personal jurisdiction. Thus, while a decision finding personal jurisdiction over an online retailer whose site contains little expressive content might burden speech only slightly, a similar finding with respect to an individual's political advocacy blog would involve a much more troublesome set of consequences.

Finally, the proposed balancing test would involve an inquiry into the broader consequences associated with finding jurisdiction in a particular case. Among the many considerations relevant to this inquiry is the tension between users' desire for a more granular and relevant Internet experience[178] and the longstanding tradition of openness on the Internet.[179] Allowing personal jurisdiction absent good faith efforts to employ geolocation tools could, if done too frequently, devastate the Internet's diverse character by creating a 'zero percent content availability' starting presumption in which users are required to justify each request for information.[180] For example, such a presumption might cause news sites and online video providers to block access to any user located outside of the site's home state or country. To the extent that there is any room for policy

176 *Cf.* Reno v. ACLU, 521 U.S. 844, 882 (1997) (discussing the importance of free speech on the Internet); Zeran v. Am. Online, Inc., 129 F.3d 327, 328–30 (4th Cir. 1997) (noting Congress's intention to protect free speech on the Internet in enacting § 230 of the Communications Decency Act of 1996).

177 Doe v. Reed, 586 F.3d 671, 678 (9th Cir. 2009).

178 *Cf.* Reidenberg, *supra* note 120, at 1972–73 (arguing that "using public values to drive technical rules" provides for state jurisdiction that that is more relevant to a community's Internet experience).

179 *Cf.* Svantesson, *supra* note 1, at 101, 131, 137 (noting that the lack of a geographic location has been a feature distinguishing the Internet from other mediums, but that this assumption is changing).

180 *See id.* at 129, 131–32.

considerations when deciding personal jurisdiction questions, inquiries of this kind could help contribute to a better-reasoned and less disruptive body of law over time.

In most cases, the balancing test described above will yield the same result as Reidenberg's *per se* rule. For instance, in the case of the hypothetical Russian child pornography site described in Part III.C both the *per se* rule and the balancing test would lead to a finding of personal jurisdiction.[181] Under the balancing test, the first factor—affordability—would work against personal jurisdiction because the site generates no revenue and is non-commercial in nature. The second factor—significance of geography to the underlying conduct—would point strongly in the other direction, however, as child pornography is (1) illegal in the United States and many other nations;[182] and (2) closely linked to states' interest in protecting vulnerable citizens from abuse.[183] Third, finding personal jurisdiction over the site would have no impact on protected speech whatsoever, since child pornography is categorically unprotected under the First Amendment.[184] Finally, because child pornography falls well outside the mainstream of Internet commerce and informational exchange, as evidenced by efforts throughout the globe to prosecute traffickers and block access to such material, the effect of finding jurisdiction on the Internet's openness would be limited.[185] Given the fact that three of the four factors support a finding of personal jurisdiction—two strongly so—the lack of affordability highlighted in the first factor would be far too insufficient to change the outcome.

The balancing test's real value comes through, however, in the cases it resolves differently than Reidenberg's *per se* rule. As the

---

[181] Of course, even if one could establish personal jurisdiction over the site, it could be impossible to proceed against the site in a U.S. forum due to an inability to properly serve the site in accordance with the Federal Rules of Civil Procedure. *See generally* FED. R. CIV. P. 4(c), (f), (h) (enumerating proper ways in which to serve foreign individuals and businesses).

[182] *See*, *e.g.*, 18 U.S.C. §§ 1466, 1466A, 2252A (2010).

[183] *See* New York v. Ferber, 458 U.S. 747, 756–61 (1982) (discussing states' reasons to protect children from obscenity and child pornography).

[184] *Id.* at 76–65 (upholding the Constitutional validity of a statute prohibiting child pornography generally and finding that it does not qualify for First Amendment protection).

[185] *Cf.* Michael Geist, *Child Pornography Blocking Plan a Risk Worth Taking*, TORONTO STAR, Dec. 4, 2006, at E2, *available at* http://www.michaelgeist.ca/content/view/1560/159/ (discussing a Canadian initiative to restrict online access to child pornography).

two examples below demonstrate, the balancing test does a better job tracking precedent and avoiding anomalous unjust results.[186] To begin with, consider *Bensusan Restaurant Corp. v. King*,[187] a case in which the New York-based owner of "The Blue Note" jazz club sued the owner of a similarly named jazz club located in Columbia, Missouri for trademark infringement in the Southern District of New York.[188] The plaintiff owned "all rights, title and interest in and to the federally registered mark 'The Blue Note'" and alleged that the defendant operated a promotional website which contained an infringing logo.[189] Logo aside, the defendant's site was quite basic, as it was accessible to the public without an account or other access code, contained only general information about the Missouri-based club (such as its location and a calendar of upcoming events), and included a disclaimer informing users that the site was not affiliated with the New York-based club.[190] The site provided no direct mechanism for online commerce, as ticket sales and other inquiries were available only by calling the Missouri-based club or visiting in person.[191] Moreover, the record before the court reflected "no allegation or proof that any infringing goods were shipped into New York or that any other infringing activity was directed at New York" by the defendant.[192]

On these facts, the court granted the defendant's motion to dismiss for lack of personal jurisdiction.[193] The rationale for this decision was simple: the defendant had not targeted New York or otherwise purposefully availed himself of the state's laws—either via advertising, contracts, physical presence, or sales.[194] Rather, the defendant had "simply created a Web site and permitted anyone who could find it to access it," an act which, "like placing a product into the stream of commerce, may be felt nationwide—or even worldwide—but, without more, it is not an act

186 These qualities are important in light of the emphasis on "traditional notions of fair play and substantial justice" in personal jurisdiction law. Int'l Shoe Co. v. Wash., Office of Unemployment Comp. & Placement, 326 U.S. 310, 316 (1945).

187 937 F. Supp. 295 (S.D.N.Y. 1996).

188 *Id.* at 297.

189 *Id.*

190 *Id.* at 297–98.

191 *Id.* at 299.

192 *Id.*

193 *Id.* at 301.

194 *Id.* at 300–01.

purposefully directed toward the forum state." [195]

Under the *per se* test, the result would be clear: the defendant's site was available in New York, and it caused harm to plaintiff's trademark in New York, therefore the defendant would be subject to personal jurisdiction in New York.[196] Personal jurisdiction would not be available under the balancing test, however, as three of the four factors cut in the defendant's favor. Specifically, the first factor supports a finding of jurisdiction, as the defendant's site was operated by a for-profit company that presumably generated revenues sufficient to cover at least the cost of client-side geolocation tools, at least in the absence of evidence to the contrary. Factor two would weigh against finding jurisdiction, however, because the defendant's site did not target New York in any way,[197] and because commercial advertising, unlike gambling or child pornography, is not a socially or economically sensitive area of the law subject to widely differing regulations in each jurisdiction. The third factor would point in this direction as well, as the defendant's site was a vehicle for protected commercial speech, and subjecting the site to jurisdiction in New York would have a severe chilling effect on speech by similar entities.[198] The fourth and final factor would also work against a finding of jurisdiction, since if the facts above were sufficient to support jurisdiction, it would be difficult to imagine any case where the site operator would not be subject to jurisdiction in a remote forum.[199] The prospect of universal jurisdiction over Internet content would, in turn, dramatically undermine the openness that allows for robust commerce and interaction online.[200]

---

[195] *Id.* at 301.

[196] Assuming that the state's long-arm law provides for jurisdiction. *See, e.g.,* N.Y. C.P.L.R. § 302(a) (Mckinney 2008) (establishing that New York courts "may exercise personal jurisdiction over any non-domiciliary" who commits a tort within the state or commits a tort outside the state and "engages in any other persistent course of conduct" within the state).

[197] *See Bensusan*, 937 F. Supp. at 299, 301.

[198] *Cf.* Zauderer v. Office of Disciplinary Counsel, 471 U.S. 626, 651 (1985) ("We recognize that unjustified or unduly burdensome [regulations] . . . might offend the First Amendment by chilling protected commercial speech.").

[199] *See* ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 712 (4th Cir. 2002) ("[If the] general principle that a person's act of placing information on the Internet subjects that person to personal jurisdiction in each State in which the information is accessed, then the defense of personal jurisdiction, in the sense that a State has geographically limited judicial power, would no longer exist.").

[200] *See* Svantesson, *supra* note 1, at 132–33 (describing the sacrifices society

Cybersell, Inc. v. Cybersell, Inc.,[201] an early Internet jurisdiction case from the Ninth Circuit, provides another example of a situation in which the balancing test comes out differently than the *per se* rule. In *Cybersell*, an Arizona-based Internet marketing firm and a Florida-based business consulting company both initially used the same name for their online businesses.[202] The Arizona-based plaintiff, however, had registered the name "Cybersell" as a service mark, and upon discovering the use of its mark on the Florida-based company's website filed suit in Arizona alleging trademark infringement and unfair competition.[203] As in *Bensusan*, the out-of-state defendant moved for and ultimately prevailed on a claim that its contacts with the forum state were too attenuated to support a finding of personal jurisdiction.[204] The court based this decision largely on its conclusion that the defendant had no Arizona-based clients, "entered into no contracts in Arizona, made no sales in Arizona, received no telephone calls from Arizona, earned no income from Arizona, and sent no messages over the Internet to Arizona."[205] While the defendant's site was available in Arizona, the site included no interactive features and failed to target the state in any manner.[206]

According to the *per se* rule, the defendant's website was available to users in Arizona, and caused harm to the plaintiff's business there via dilution of its service mark. Thus, because the defendant failed to block access to its site in Arizona, it would have been subject to personal jurisdiction there. The balancing test analysis leads to the opposite result, as the calculus remains unchanged on each of the four factors discussed in relation to *Bensusan* above. If one were to modify the facts to convert the Florida-based defendant into a non-commercial politics blog, then the first factor would cut against a finding of personal jurisdiction for affordability reasons and the third factor would militate even more strongly in that direction than before (given the First Amendment's enhanced protection for political

would have to make in terms of content availability if the Internet were to become more regionalized).

[201] 130 F.3d 414 (9th Cir. 1997).

[202] *Id.* at 415.

[203] *Id.* at 415–16.

[204] *Id.* at 419–20; Bensusan Rest. Corp. v. King, 937 F, Supp. 295, 301 (S.D.N.Y. 1996).

[205] *Cybersell*, 130 F.3d at 419.

[206] *Id.*

speech).[207]

3. Synthesis

As the *Zippo* test has fallen behind the technological curve in recent years, courts and academic commentators have begun to point out its flaws and propose improvements.[208] Professor Reidenberg in particular has identified some of the most glaring problems with a personal jurisdiction regime that fails to consider sites' use and non-use of geolocation technologies.[209] While Reidenberg's proposed remedy to those problems should not be adopted for the reasons given in section 1 above, a balancing test that incorporates several of the policy considerations he identifies, as described in section 2, would go a long way towards modernizing the *Zippo* personal jurisdiction test. That modernization would, in turn, help safeguard states' interests in adjudicating disputes and plaintiffs' interests in obtaining convenient and effective relief from online harms—goals consistent with precedent, and both Professor Redish and Professor Reidenberg's proposals.[210]

On a broader note, geolocation technologies also likely affect the calculus in related areas of the law such as enforcement of foreign judgments[211] and the availability of diversity jurisdiction in suits involving anonymous Doe defendants.[212] Notably, a small number of sovereign and quasi-sovereign entities have

---

[207] *See* FEC v. Wis. Right to Life, Inc., 551 U.S. 449, 457 (2007) ("[T]he First Amendment requires us to err on the side of protecting political speech rather than suppressing it.").

[208] *See* Redish, *supra* note 83, at 591–93.

[209] *See* Reidenberg, *supra* note 120, at 1956, 1961–62.

[210] *See* World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 292 (1980); Redish, *supra* note 83, at 606–10; Reidenberg, *supra* note 120, at 1971–74.

[211] *See* Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 433 F.3d 1199, 1212–13 (9th Cir. 2006) (W.A. Fletcher, J., plurality opinion) ("[A]n American court will not enforce a judgment if 'the cause of action on which the judgment was based, or the judgment itself, *is repugnant to the public policy* of the United States or of the State where recognition is sought[.]'" (quoting the RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 482(2)(d))). *See also id.* at 1215 ("Inconsistency with American law is not necessarily enough to prevent recognition and enforcement of a foreign judgment in the United States. The foreign judgment must be, in addition, repugnant to public policy.").

[212] *Cf.* Sony Music Entm't, Inc. v. Does 1-40, 326 F. Supp.2d 556, 567–68 (S.D.N.Y. 2004) (refusing to grant a motion for a dismissal for lack of personal jurisdiction, because it was unclear from IP addresses where the defendants were located).

considered enacting liability shields to protect against the perceived expansion of the law governing personal jurisdiction and enforcement of judgments.[213] In Iceland, for instance, activists have begun to push for passage of "a jurisdictional 'safe haven' for information on the global network, a set of highly-protective laws for anonymity protection, free expression, immunities for information providers, and the like for those who make information available on the net."[214] These proposed laws represent a market response akin to Delaware's development of a business-friendly body of corporate law in the United States.[215]

IV. INTERNET COMMERCE AND GEOLOCATION MANDATES

From the late 1990s through the mid-2000s, virtually every court to confront the question of whether it was possible for websites to screen users by jurisdiction determined—correctly at the time—that it was impossible to do so.[216] This fact drove decisions in a string of cases involving community standards legislation and Internet commerce regulations.[217] Due almost entirely to the fact that "cyberspace . . . remain[ed] largely unzoned—and unzoneable,"[218] courts struck down numerous

[213] *See* David Post, *The Iceland of the Internet*, THE VOLOKH CONSPIRACY (Jan. 8, 2010, 11:41 AM), http://volokh.com/2010/01/08/the-iceland-of-the-internet/. *See also* GOLDSMITH & WU, *supra* note 14, at 65–66 (discussing the brief history of the "Principality of Sealand," a small concrete platform off the coast of the United Kingdom, and the home of "HavenCo," – an entity whose purpose was to rent out sever space to those who wanted to evade government regulation of the Internet).

[214] Post, *supra* note 213.

[215] *Cf.* ERIN A. O'HARA & LARRY E. RIBSTEIN, LAW MARKET, 65–70 (2009) (discussing the creation of law markets).

[216] *See* Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 661 (E.D. Pa. 2004) ("[E]very federal court that examined a state law that directly regulated the Internet determined that the state law failed the *Pike* balancing test." (citations omitted)). *See also, e.g.*, ACLU v. Johnson, 4 F. Supp. 2d 1029, 1032 (D.N.M. 1998), *aff'd*, 194 F.3d 1149, 1164 (10th Cir. 1999) (determining that it was impossible for speakers utilizing certain Internet-based communications to determine the location of those accessing their speech); Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 165, 169–72 (S.D.N.Y. 1997) (discussing that a party's geographic location is generally unknown and perhaps unknowable, and stating that jurisdiction is based on geography which is basically meaningless when the Internet is involved).

[217] Courts were quick to grant preliminary injunctions against enforcement of state laws that regulated the Internet based on the belief that "[t]he nature of the internet ma[de] it impossible to restrict the effects" of a state law to conduct occurring within that state. *See Pataki*, 969 F. Supp. at 177, 183–84; *Pappert*, 337 F. Supp. 2d at 662–63; *Johnson*, 4 F. Supp. 2d at 1033–34.

[218] Reno v. ACLU, 521 U.S. 844, 891 (1997) (O'Connor, J., concurring in the

federal and state statutes which would have prohibited transmission of certain forms of content deemed harmful to minors.[219]

Modern geolocation technologies completely undermine the justification for these decisions. In the spirit of Lawrence Lessig's axiom that "code is law,"[220] the architecture of the Internet in the late 1990s and early 2000s dictated the legal result in each of the cases above.[221] But that architecture has changed. Extremely accurate geolocation technologies are now not only available, but they are also in widespread use.[222] Thus, it is proper to inquire whether the rules of those cases should change as well. As the discussion below indicates, the question now is not *whether* sites can screen according to jurisdiction; rather, it is *when* legislatures should be free to compel them to do so. While Congress clearly has the power to impose a geolocation mandate on sites in or affecting interstate commerce, it is less clear whether state legislatures may constitutionally exercise a similar power. This difference arises due to the dormant Commerce Clause, which prohibits states from discriminating against or imposing excessive burdens on interstate commerce.[223] Carefully-tailored state regulations that serve valid governmental interests and avoid burdening free expression will likely pass this test, however. In addition, the First Amendment circumscribes when both the federal and state governments may impose geolocation mandates, as such mandates necessarily involve compliance costs that could interfere with protected

judgment in part and dissenting in part).

[219] *See id.* at 849 (majority opinion) (finding that two federal statutes designed to protect minors from sexually explicit material violated the First Amendment); PSINET Inc. v. Chapman, 362 F.3d 227, 229–31, 232, 239–41 (4th Cir. 2004) (finding that a Virginia statute designed to protect minors from sexually explicit material violated both the First Amendment and the dormant Commerce Clause).

[220] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999) (explaining that the software and hardware code that operates the Internet is the de facto regulator of Internet activity).

[221] Federal district courts have found on several occasions that the decentralized nature of the Internet makes it very difficult for states to regulate it without violating either the First Amendment or the dormant Commerce Clause. *See Pappert*, 337 F. Supp. 2d at 663; *Johnson*, 4 F. Supp. 2d at 1031–34; *Pataki*, 969 F. Supp. at 161.

[222] *See supra* Part II.B.

[223] *See* King, *supra* note 1, at 49–53 (arguing that the states are not, and indeed should not, be free to compel use of geolocation on their own—as this would, in effect, allow one state to dictate the law in all fifty states).

online speech.

A. Code is Law: The Inability to Geo-Locate Users Drives Early Court Decisions

Two cases, both decided in 1997, undergird the basic proposition that the inability to screen users by jurisdiction renders Internet decency regulations invalid. The first of these cases, *American Libraries Ass'n v. Pataki*,[224] is widely considered as the seminal authority for this approach.[225] In *Pataki*, the Southern District of New York addressed the constitutionality of a New York law that prohibited transmission of sexual content deemed "harmful to minors" via the Internet.[226] Ultimately, the court determined that the New York statute violated the dormant Commerce Clause for three reasons. First, the "extreme burden[s]" the statute imposed on interstate commerce exceeded the somewhat limited local benefits the statute would have conferred, since the law would not stop harmful content originating overseas from reaching New York users.[227] Second, the statute constituted a *per se* constitutional violation, since it projected "New York law into conduct that occurs wholly outside New York."[228] Finally, the court held that Internet communications represented a "type[] of commerce [that] demand[s] consistent treatment[,]" meaning that such communications are "susceptible to regulation only on a national level."[229]

The court's legal conclusions flowed from a series of factual determinations regarding the nature of Internet communications. The court began by finding that "[t]he Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic

[224] 969 F. Supp. 160, 167 (S.D.N.Y. 1997).

[225] *See, e.g.,* Am. Booksellers Found. for Free Expression v. Strickland, 512 F. Supp. 2d 1082, 1102 (S.D. Ohio 2007) (referring to *Pataki* as the "seminal" case in this area of the law); PSINet Inc. v. Chapman, 167 F. Supp. 2d 878, 891 (W.D. Va. 2001) (labeling *Pataki* as the "leading" case regarding dormant Commerce Clause challenges to Internet regulations).

[226] *Pataki*, 969 F. Supp. at 161, 163.

[227] *Id.* at 177–81.

[228] *Id.* at 169, 175, 177.

[229] *Id.* at 181.

location . . . ."[230] Continuing with this theme, the court went on to state that "[t]he unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed." [231] Putting to rest any remaining doubts that it thought some form of geographic screening might be possible, the court added that "[t]ypically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet."[232]

The Supreme Court took a similar approach in *Reno v. ACLU*, a case challenging the constitutionality of the Communications Decency Act of 1996.[233] As in *Pataki*, the Court found the statute unconstitutional—though on First Amendment rather than Commerce Clause grounds.[234] Initially, the Court determined that accurate user-identification measures were either effectively unavailable or prohibitively expensive.[235] Concurring in the result, Justice O'Connor echoed this sentiment when she concluded that the Internet was "largely unzoned—and unzoneable."[236] Because no viable means existed to "zone" the Internet at the time, the Court concluded that the CDA's "'community standards' criterion as applied to the Internet mean[t] that any communication available to a nation wide audience [would] be judged by the standards of the community most likely to be offended by the message."[237]

In the decade following *Pataki* and *Reno*, a considerable number of other cases reached similar legal results. For example, in *ACLU v. Johnson*, a federal district court granted a preliminary injunction enjoining the enforcement of a New Mexico child protection measure similar to that at issue in *Pataki*.[238] Such a result was required, the court held, since it was

[230] *Id.* at 170.
[231] *Id.* at 168–69.
[232] *Id.* at 169.
[233] Reno v. ACLU, 521 U.S. 844, 844 (1997).
[234] *See id.* at 885.
[235] *Id.* at 876–77 (commenting on age verification technologies).
[236] *Id.* at 891 (O'Connor, J., concurring in the judgment in part and dissenting in part). While Justice O'Connor noted that future technological developments could lead to a different result, she nonetheless reasoned that it would be improper "to rely on unproven future technology to save the statute." *Id.* at 881–82.
[237] *Id.* at 876–78 (majority opinion).
[238] *See* ACLU v. Johnson, 4 F. Supp.2d 1029, 1033–34 (D.N.M. 1998) (finding

"impossible for speakers using . . . the World Wide Web to determine the geographic location of persons who access their speech," and thus impossible "to prevent speech communicated by . . . the World Wide Web from reaching persons residing in the State of New Mexico."[239] The same chain of reasoning eventually doomed similar state laws in Michigan,[240] Vermont,[241] Pennsylvania,[242] and South Carolina.[243] Though its decision was later vacated by the Supreme Court on other grounds, the Third Circuit employed the same brand of logic en route to finding the federal Child Online Protection Act unconstitutional.[244] When it interred Virginia's child protection statute on similar grounds in *PSInet, Inc. v. Chapman*, the Fourth Circuit put the matter in memorable, visual terms:

> [T]he content of the Internet is analogous to the content of the night sky. One state simply cannot block a constellation from the view of its own citizens without blocking or affecting the view of the citizens of other states. Unlike sexually explicit materials disseminated in brick and mortar space, electronic materials are not distributed piecemeal. The Internet uniformly and simultaneously distributes its content worldwide.[245]

---

a statutory provision criminalizing the dissemination, by computer, of speech "harmful to a minor" violated both the Commerce Clause, and the First Amendment, and granting an injunction enjoining enforcement of the provision), *aff'd* 194 F.3d 1149 (10th Cir. 1999).

[239] *Id.* at 1032.

[240] Cyberspace Commc'ns, Inc. v. Engler, 55 F. Supp.2d 737, 737, 744, 751, 753–54 (E.D. Mich. 1999) ("The majority of Internet addresses contain no geographic indicators.").

[241] Am. Booksellers Found. v. Dean, 342 F.3d 96, 103–105 (2d Cir. 2003) ("[T]he internet does not recognize geographic boundaries, [thus making it] difficult, if not impossible, for a state to regulate internet activities without 'project[ing] its legislation into other States.'" (quoting Healy v. Beer Inst., 491 U.S. 324, 334 (1989)).

[242] *See* Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp.2d 606, 606, 662–63 (E.D. Pa. 2004) (invalidating a Pennsylvania statute that required ISPs to "block access to websites displaying child pornography," because its "extraterritorial effect violat[ed] the dormant commerce clause").

[243] *See* Se. Booksellers Ass'n v. McMaster, 371 F. Supp. 2d 773, 787–88 (D.S.C. 2005) (internal citations omitted) ("[H]ere, it is undisputed that (1) Internet speakers have no practical, reliable means of determining the geographic location of the recipients of their online communications; and (2) Internet speakers have no way of ensuring their communications are not accessed in a certain geographic location, such as the State of South Carolina.").

[244] *See* ACLU v. Reno, 217 F.3d 162, 175, 181 (3d Cir. 2000) ("[O]f extreme significance, is the fact, as found by the District Court, that Web publishers are without any means to limit access to their sites based on the geographic location of particular Internet users."), *vacated* 535 U.S. 564 (2002).

[245] 362 F.3d 227, 240 (4th Cir. 2004).

Unlike many of its predecessors, however, the *PSInet* decision explicitly noted that "there may some day be sufficient technology to render [the Virginia] statute constitutional."[246] This recognition of the potential for change coincided roughly with the first wave of truly modern IP-based geolocation technologies.[247] Now that geolocation is possible and widespread, the Internet is no longer "wholly insensitive to geographic distinctions."[248] Thus, the factual basis for each of the decisions described above has been severely undermined if not destroyed entirely. That being the case, the time has come to revisit the holdings in the *Pataki*/*Reno* line of cases.

B. The New Technological Order: Legislative Options for Geolocation Mandates.

Because every website operator now has the ability to screen users by jurisdiction,[249] the chief obstacle to the constitutionality of many of these laws is now gone. That new technological order shifts the focus to a new question: when are legislatures free to compel sites to adopt geolocation technologies? The mere fact that such technologies exist does not mean that a mandate for their use would be constitutionally permissible, particularly if the mandate originated in state law subject to the dormant Commerce Clause. Depending on their coverage, geolocation mandates—whether state or federal in origin—may also need to withstand a challenge on First Amendment grounds. On closer reflection, it seems clear that Congress may require sites in or affecting interstate commerce to utilize geolocation technologies so long as such requirements avoid excessive reach. Though state mandates present a more difficult question, recent well-reasoned cases suggest that these mandates may also be valid if carefully tailored.

1. Congress

Congress has broad power to regulate websites in or effecting interstate commerce via its powers under Article I, section 8 and

---

[246] *Id*. at 241.

[247] *See* Tedeschi, *supra* note 12 (explaining how technology companies producing geolocation software are finding niche markets).

[248] Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 170 (S.D.N.Y. 1997).

[249] *See supra* Part II.A.

the Necessary and Proper Clause.[250] This greater power unquestionably includes the lesser power to require at least some classes of websites, in at least some cases, to implement geolocation tools and to use those tools to screen users by jurisdiction. Though there are many sources of potential limitations on this broad authority, the First Amendment is likely the most substantial. This greater power unquestionably includes the lesser power to require at least some classes of websites, in at least some cases, to implement geolocation tools and to use those tools to screen users by jurisdiction. Though there are many sources of potential limitations on this broad authority, the First Amendment is likely the most substantial. This is so because, as discussed earlier in Part III, many Internet sites serve as channels for the free expression of ideas.[251] Blogs, such as The Volokh Conspiracy (volokh.com), and non-profit advocacy pages, such as those operated by Public Citizen (www.citizen.com) and the National Rifle Association (www.nra.org), are examples of such speech-infused sites. Since server-side geolocation tools cost thousands of dollars per year and client-side tools still involve non-trivial implementation costs as well,[252] requiring these classes of non-commercial sites to implement geolocation technologies would involve a substantial burden on protected speech.[253] Even a mandate limited to commercial sites would have some impact on protected commercial speech, particularly considering the Supreme Court's recent decision underscoring such speech rights in *Citizens United v. FEC*.[254]

Assuming Congress constructed a geolocation mandate that

[250] *See* Gonzales v. Raich, 545 U.S. 1, 5, 8 (2005); *id.* at 33–34 (Scalia, J., concurring) (acknowledging that Congress's power to regulate intrastate activities that substantially affect interstate commerce is derived from the Necessary and Proper Clause in addition to the Commerce Clause); United States v. Rodia, 194 F.3d 465, 469, 474–77, 482 (3d Cir. 1999) (reasoning that Congress could have a rational basis for believing that intrastate possession of pornography has a substantial effect on interstate commerce because it can be transmitted through the Internet). *Cf.* Ashcroft v. ACLU, 535 U.S. 564, 569–70, 585–86 (2002) (narrowly upholding the breadth of the COPA, an act of Congress prohibiting any individual from engaging in interstate commerce that involved pornographic communications to minors).

[251] *See supra* Part III.D.2.b.

[252] *See supra* Part II.B.

[253] *See* Matwyshyn, *supra* note 1, at 521.

[254] *See* Citizens United v. FEC, 130 S. Ct. 876, 886, 888, 913, 917 (2010) (invalidating the Bipartisan Campaign Reform Act of 2002, which imposed a variety of regulations on corporate participation in federal elections).

was viewpoint and content neutral (i.e., one which has "an incidental effect on expressive conduct"), the mandate would comply with the First Amendment so long as it could survive intermediate scrutiny.[255] Under the Supreme Court's *O'Brien* test, a regulation meets that test when it (1) "is within the constitutional power of the Government;" (2) "furthers an important or substantial governmental interest;" (3) is based on interests "unrelated to the suppression of free expression"; and (4) imposes a burden on First Amendment freedoms "no greater than is essential to the furtherance of that interest."[256]

While there are an infinite number of ways a geolocation mandate could be constructed, a bill currently pending in Congress—the Internet Gambling Regulation, Consumer Protection, and Enforcement Act (IGRCPEA)—provides a window into how these standards work in practice. In short, the IGRCPEA would allow Internet gambling sites to provide gambling services within the United States so long as they employ geolocation tools capable of blocking users from states that choose to opt-out of the market.[257] Because the Supreme Court has twice concluded that "gambling . . . implicates no constitutionally protected right,"[258] the IGRCPEA likely falls outside of the First Amendment's sweep. The Third Circuit's recent decision in *Interactive Media Entertainment & Gaming Association v. Attorney General of the United States* supports this view, as the court concluded that the Unlawful Internet Gambling Enforcement Act (UIGEA) of 2006[259] "lacks any 'communicative element' sufficient to bring it within the ambit of the First Amendment," since it "only criminalizes the knowing

---

[255] *See* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 662 (1994); Jacobs v. Clark Cnty. Sch. Dist., 526 F.3d 419, 434 (9th Cir. 2008).

[256] United States v. O'Brien, 391 U.S. 367, 377 (1968); Doe v. Reed, 586 F.3d 671, 678 (9th Cir. 2009) (reaffirming the validity of the *O'Brien* test). More broadly targeted mandates, on the other hand, would be subjected to strict scrutiny—a form of analysis often considered "fatal in fact." *See Citizens United*, 130 S. Ct. at 882; Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 275 (1995) (Ginsburg, J., dissenting) (indicating that the strict scrutiny standard had historically been considered "'fatal in fact'").

[257] Internet Gambling Regulation, Consumer Protection, and Enforcement Act, H.R. 2267, 111th Cong. § 5384(b) (2009).

[258] *See* United States v. Edge Broad. Co., 509 U.S. 418, 426 (1993); Posadas de Puerto Rico Assocs. v. Tourism Co. of Puerto Rico, 478 U.S. 328, 345–46, 348 (1986) (noting that since gambling can be prohibited outright, the government can choose to allow it while trying to lower its demand by restricting advertising).

[259] 31 U.S.C. §§ 5361-67 (2010).

acceptance of certain financial instruments in connection with unlawful gambling."[260] Even if one were to find some aspect of the IGRCPEA that does involve a 'communicative element,' it seems clear that the Act is (1) a valid exercise of Congress's interstate commerce power, since most online gaming transactions cross state or international borders; that (2) prevention of fraud, money laundering, and underage gambling are important government interests;[261] that (3) those interests are not intended to suppress speech, and that (4) the geolocation requirement is minimally intrusive, particularly in light of the fact that it would be impossible to include a state opt-out feature without the mandate. Thus, the IGRCPEA serves as one example of a geolocation mandate that would survive First Amendment scrutiny.

In contrast to the IGRCPEA, several other types of federal geolocation mandates would not comply with the First Amendment's strictures. For example, legislation requiring all sites, on penalty of a significant fine, to utilize geolocation tools to block users from domains frequently associated with hacking efforts would likely fail the fourth *O'Brien* factor, which requires a regulation to burden speech no more "than is essential to the furtherance of [the government's] interest."[262] Forcing low-tech, low-content non-commercial sites, such as an individually run politics blog, to geo-locate their users can hardly be classified as 'essential' to the anti-hacking objective, if that word is to have any limiting meaning. Considering the Supreme Court's conclusion in *Reno v. ACLU* that user verification costs would drive many non-commercial sites out of existence entirely,[263] one could also argue that such a mandate would (at least on an as-applied basis) have much more than an incidental effect on protected speech, and thus be subject to strict scrutiny—a form of review usually "fatal in fact."[264]

---

[260] Interactive Media Entm't & Gaming Ass'n. Inc. v. Att'y Gen. of the U.S., 580 F.3d 113, 118 & n.8 (3d Cir. 2009).

[261] *See Edge Broad. Co.*, 509 U.S. at 425–26 ("[Gambling] falls into a category of 'vice' activity that [can] be, and frequently has been, banned altogether"). *See also* King, *supra* note 1, at 42–46 (discussing valid governmental interests in regulating gambling).

[262] United States v. O'Brien, 391 U.S. 367, 377 (1968).

[263] *See* Reno v. ACLU, 521 U.S. 844, 856 (1997).

[264] *But see* Adarand Constructors Inc. v. Pena, 515 U.S. 200, 237 (1995) (dispelling the notion that strict scrutiny is "fatal in fact.").

2. The States

The rise of widely-accessible geolocation tools means that state laws regulating the Internet are less likely to result in wholly extra-territorial applicability, and are thus less likely to be invalidated pursuant to the *Pataki*/*Reno* rationale.[265] Nonetheless, the dormant Commerce Clause still presents a challenge for state regulations, because they may still discriminate against or otherwise burden interstate commerce. Under the *Pike* balancing test, a state regulation violates the dormant Commerce Clause when its out-of-state burdens outweigh the in-state benefits it provides.[266] Interestingly, several recent decisions have upheld state regulations against dormant Commerce Clause challenges in areas including spam prevention,[267] fraudulent advertising,[268] and online sales.[269]

National Federation for the Blind v. Target Corporation, a recent federal district court case, provides a good example. *National Federation* involved the application of a California law guaranteeing the disabled equal rights to "'all business establishments of every kind whatsoever'" to a national online retailer.[270] Because the retailer could use geolocation tools "to make a California-specific website" and thus "avoid

---

[265] *See* Goldsmith & Sykes, *supra* note 18, at 809–12.

[266] *See* Pike v. Bruce Church, Inc. 397 U.S. 137, 142 (1970). *See also* Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 610, 661 (E.D. Pa. 2004) (applying the *Pike* test to a state statute imposing criminal liability on ISPs for allowing access to child pornography through their networks, but stating that heightened scrutiny applies, however, when a state regulation discriminates against interstate commerce).

[267] *See, e.g.*, Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255, 1257–58, 1262, 1266 (Cal. Ct. App. 2002) (holding that a California law regulating spam provided legitimate local benefits and that the law's burden the law on interstate commerce was not excessive).

[268] *See, e.g.*, Washington v. Heckel, 143 Wash. 2d 824, 839–40 (2001) (holding that the Act did not violate the Commerce Clause because it only regulated the conduct of spammers targeting Washington customers and, therefore, the local benefits outweighed the extraterritorial effect).

[269] *See, e.g.* Nat'l Fed'n of the Blind v. Target Corp., 452 F. Supp.2d 946, 959 (N.D. Cal. 2006) (examining state laws that have survived commerce clauses challenges including a California law criminalizing use of the Internet to distribute harmful materials to minors) (citations omitted); Ford Motor Co. v. Texas Dep't of Transp., 264 F.3d 493, 498, 499–500, 502, 512 (5th Cir. 2001) (upholding the application of a state law that prohibits selling vehicles to Texas consumers without a dealer's license to Ford's marketing of pre-owned vehicles in Texas through a website).

[270] *Nat'l Fed'n*, 452 F. Supp. 2d at 957 (citing Unruh Civil Rights Act, Cal. Civ. Code § 51(b) (West 2006)).

extraterritorial application" of the law, the court found that California's law probably did not implicate the dormant Commerce Clause.[271] En route to reaching that decision, the court sharply criticized *Pataki* for its "incorrect technical understanding of the Internet"[272] and failure to recognize that "[i]t is common practice for websites for entities operating in multiple countries to have a single site that directs customers to different versions based upon language."[273] *National Federation*'s explicit recognition of a website's ability to "tailor its content based on the location of its users" puts it among the few U.S. cases that have recognized the existence of geolocation in the first place.[274]

In some ways, the *National Federation* decision reflects a trend in which geographic filtering requirements are increasingly becoming the legal norm. Banks and retailers now use geolocation tools to prevent fraudulent account access and purchases.[275] Likewise, as noted in Part II.B.3, online broadcasters such as Major League Baseball and the BBC screen users by jurisdiction to comply with contractual obligations. Two states, Utah and Kentucky, have taken legal steps that would seem to require parties to employ geolocation tools in order to avoid liability—the former with respect to trademark infringement[276] and the latter with respect to online gambling.[277] Along those same lines, one of the world's largest online poker sites recently entered into a plea agreement with federal

[271] *Id.* at 950, 960–62.

[272] *Id.* at 961 (citing Goldsmith & Sykes, *supra* note 18, at 822).

[273] *Id.*

[274] *Id.* at 961–62. *See, e.g.,* ACLU v. Gonzales, 478 F. Supp. 2d 775, 807 (E.D. Pa. 2007) (explaining that a company can "direct traffic so that only users in the United States can view products that can only be distributed in the United States"); Digital Envoy, Inc. v. Google, Inc., 370 F. Supp. 2d 1025, 1027 (N.D. Cal. 2005) (explaining how Google tailors its advertising to account for the geographic location of its users); Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 433 F.3d 1199, 1203, 1225 (9th Cir. 2006) (W.A. Fletcher, J., plurality opinion) (describing the accuracy with which Internet users' locations can be identified); Hageseth v. Superior Court., 150 Cal. App. 4th 1399, 1420–23 (Cal. Ct. App. 2007) (discussing the Internet's effect on the concept of geographic location, and stating that technology exists to determine the location of an Internet user).

[275] *See* Richmond, *supra* note 6.

[276] *See* Matthew Nelson, Comment, *Utah's Trademark Protection Act: Over-Reaching Unconstitutional Protectionism or Decisive Clarifying Legislation*?, 2007 UTAH L. REV. 1199, 1215 (2007).

[277] *See* King, *supra* note 1, at 48–53.

prosecutors that requires it to block all U.S. users.[278]

Going forward, the *Pike* dormant Commerce Clause test and the First Amendment protections described above seem more than adequate to prevent states from imposing disruptive or onerous geolocation mandates. These limitations on state action mirror the proposed limits on personal jurisdiction in Part III, as both stress the costs associated with an effective geolocation mandate, the relevance of geography to the underlying online conduct, and the burden on protected speech. Nevertheless, since a uniform set of geolocation mandates would be preferable to a series of conflicting requirements, and since a federal mandate would still allow some degree of federalism, federal pre-emption in the field of geolocation may be the more efficient approach.

V. PRIVACY AND PERSONALLY-IDENTIFIABLE INFORMATION

Nearly everyone who uses the Internet is affected by geolocation each time they surf the web. Though the process is largely invisible, geolocation tools are constantly working to identify users and, in some cases, to create profiles of those users.[279] These identification and tracking mechanisms pose a considerable risk to individual privacy, yet Congress and federal agencies have done little to address those risks thus far.[280] That being the case, the privacy interests implicated by geolocation technologies are best addressed under section 5 of the Federal Trade Commission (FTC) Act, which enables the Commission to take a flexible, context-sensitive enforcement approach.[281] Because server-side geolocation tools identify users indirectly and on a regional basis, and because client-side tools do so directly and within a much smaller geographic radius, the FTC should focus initially on providing notice and consent safeguards when sites use the latter. Moreover, as the technological landscape evolves over time, the FTC should utilize its flexible enforcement authority under section 5 of the FTC Act to ensure that privacy protections adequately guard against the risks posed by geolocation tools.

---

[278] *Id.* at 68–69.

[279] *See* Goldsmith & Sykes, *supra* note 18, at 810–11.

[280] *Id.* at 808–11 ("[D]eveloping technologies . . . allow webpage content providers instantly to determine the content receiver's geographical identity . . . .").

[281] *See* 15 U.S.C. § 45 (2010).

A. The Relevant Body of Law

Currently, federal law does not explicitly regulate or otherwise speak to the use of geolocation technologies.[282] In the absence of such laws, general rules governing Internet communications are the most relevant body of law to the privacy questions raised in this Part. Section 5 of the FTC Act stands out among such laws, because it has been used extensively to safeguard online privacy in the past and the FTC has issued contextual and behavioral advertising guidelines in connection with its section 5 enforcement authority.[283] This body of law consists of section 5 itself, which empowers the Commission to restrain "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce,"[284] the FTC's recently issued *Self-Regulatory Principles for Online Behavioral Advertising,*[285] and quasi-judicial decisions in individual enforcement cases.[286]

One dominant theme throughout the FTC's section 5 privacy law is heightened protection for "personally identifiable information," or "PII" for short.[287] In general, the Commission defines PII as "information that can be linked to a specific individual including, but not limited to, name, postal address, email address, Social Security number, or driver's license

[282] *But see* 15 U.S.C. § 7701(a)(11) (2006) (noting that e-mail addresses "do[] not specify a geographic location," thus making it "extremely difficult" for states to enforce their own anti-spam regulations); 18 U.S.C. § 2258A (2010) (requiring Internet Service Providers to provide geographic information regarding individuals or websites in cases involving missing and exploited children); 47 C.F.R. § 10.320(f) & tbl.10.320(f) (2009) (providing for the use of geolocation tools in connection with operation of a homeland security-oriented "Commercial Mobile Alert System").

[283] *See* PETER P. SWIRE, CTR. FOR AM. PROGRESS, THE INTERNET AND THE FUTURE OF CONSUMER PROTECTION 4–9, 11 (2006), *available at* http://www.peterswire.net/SWIRE_CONSUMER_PROTECTION_REPORT.pdf ("[P]rivacy and data security have become major topics for enforcement under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices.").

[284] 15 U.S.C. § 45(a)(1).

[285] FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVER. 1, 45–47 (2009), [hereinafter BEHAVIORAL ADVERTISING PRINCIPLES], *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[286] *See, e.g.*, *In re* Microsoft Corp., 134 F.T.C. 709, 740, 742 (2002) (ordering that Microsoft shall not misrepresent its information practices).

[287] *See* BEHAVIORAL ADVERTISING PRINCIPLES, *supra* note 285, at 20–22 & n.49, 25.

number."[288] This category excludes "anonymous data that, without more, cannot identify a specific person."[289] When interpreting the term "personally identifiable information" in other statutory contexts, courts have taken a similar approach. For instance, courts have read the reference to PII in the Cable Communications Privacy Act[290] to include information pertaining to a subscriber's demographics or "bank transactions, shopping habits, political contributions, viewing habits, and other significant personal decisions."[291] According to the FTC staff, covered classes of information include data such as "financial data, data about children, health information, *precise geographic location information*, and Social Security numbers."[292] Parts V.B and V.C consider this "precision requirement" in the context of server-side and client-side geolocation tools.

In terms of enforcement, the FTC has interpreted section 5 to require businesses to provide consumers with prominent notice when collecting PII,[293] to obtain consumers' consent with regard to such practices,[294] and to provide for adequate security of consumer information once it is collected.[295] Two very recent

---

[288] *Id.* at 20 n.47.

[289] *Id.*

[290] 47 U.S.C. § 551 (2010).

[291] Scofield v. Telecable of Overland Park, Inc., 973 F.2d 874, 876 (10th Cir. 1992) (citing H.R. REP. NO. 98-934, at 29 (1984)); Metrovision of Livonia, Inc. v. Wood, 864 F. Supp. 675, 681 (E.D. Mich. 1994) (citing H.R. REP. NO. 98-934, at 29 (1984)).

[292] BEHAVIORAL ADVERTISING PRINCIPLES, *supra* note 285, at 44 (emphasis added). The FTC staff has advocated extending some protection to information traditionally considered non-PII, such as any data that could potentially implicate individual privacy interests. *See id.* at 20–25.

[293] *See* Sony BMG Music Entertainment; Analysis of Proposed Consent Order To Aid Public Comment, 72 Fed. Reg. 13286, 13287 (Mar. 21, 2007) (requiring respondent, Sony BMG, to display a prominent disclosure notifying consumers that its products install software that create security vulnerabilities). *See also* In re Microsoft Corp., 134 F.T.C. 709, 742, 749–50 (2002) (requiring respondent, Microsoft, to implement an information security program that identifies risks to the security of customer information).

[294] *See* BEHAVIORAL ADVERTISING PRINCIPLES, *supra* note 285, at 42–44 ("The fourth principle states that companies should only collect sensitive data for behavioral advertising after they obtain affirmative express consent from the consumer to receive the advertising."). *See also* Sony BMG Music Entertainment; Analysis of Proposed Consent Order To Aid Public Comment, 72 Fed. Reg. at 13287 (requiring Sony to secure consumers' consent before installing tracking software via audio CDs).

[295] *See* Complaint at 4-5 In re Reed Elsevier, Inc., No. C-4226, 2008 FTC LEXIS 73 (F.T.C. July 29, 2008); Complaint at 3–6, In re Guidance Software, Inc., No C-4187, 2007 FTC LEXIS 34 (F.T.C. Mar. 30, 2007); *In re Microsoft Corp.*, 134 F.T.C. at 742–43.

examples show how these requirements work in practice. First, in 2009 Google launched its My Location feature for personal computers, which uses SSID-based client-side geolocation tools to provide "more accurate local search results on Google" and third party sites via the W3C Geolocation API.[296] During the product launch, users equipped with Google's in-browser toolbar received an automatic prompt explaining the "My Location" feature and asking for consent to install the application.[297] Only after a user indicated his or her consent via this prompt did the toolbar begin collecting and reporting geolocation data via My Location.[298]

Second, in August 2010, popular social networking site Facebook launched Facebook Places, a new feature that enables users to automatically share their whereabouts with friends—either via Facebook directly or through third-party platforms.[299] As with Google's My Location feature, Facebook Places is an opt-in feature that requires user consent to be activated.[300] That notice and consent-based model is the product of a development effort that put a much higher premium on privacy rights than previous Facebook feature launches, which had drawn heavy criticism from the Electronic Frontier Foundation and other privacy watchdogs.[301]

---

[296] *Master Advanced Features: My Location*, GOOGLE TOOLBAR, http://www.google.com/support/toolbar/bin/answer.py?answer=166104 (last visited Jan. 5, 2011); Ian Paul, *Google's 'My Location' Tracks PC's Location on Google Maps*, PCWORLD (July 10, 2009, 9:43 AM), http://www.pcworld.com/article/168203/googles_my_location_tracks_your_pcs_location_on_google_maps.html.

[297] *See Master Advanced Features: My Location*, *supra* note 296 (describing how to enable "My Location" and explaining that the user must click on "Share my location" to give Google Maps permission to share the user's location).

[298] *Id.* (explaining that after "My Location" is installed, the user's "local network information (including, but not limited to, visible WiFi access points)" will be collected to determine the user's location). For documentation of this process, see materials on file with author.

[299] Mark Milian, *New Facebook Feature is Going Places*, L.A. TIMES, Aug. 29, 2010, at B1; Nick Bilton, *Facebook Will Allow Users to Share Location*, N.Y. TIMES BITS BLOG (Mar. 9, 2010, 1:44 PM), http://bits.blogs.nytimes.com/2010/03/09/facebook-will-allow-users-to-share-location/.

[300] *See* Bilton, *supra* note 299 ("'If [Facebook] offer[s] a service that supports this type of location sharing [it] will present you with an opt-in choice of whether you want to participate.'").

[301] *See* Benny Evangelista, *Experts Advise Caution Using Facebook Places*, S.F. CHRON., Aug. 25, 2010, at D1; Bilton, *supra* note 299 ("Facebook has been trying to figure out how to add location data to its service without raising potential privacy concerns.").

B. Application to Server-Side Geolocation Tools

Server-side geolocation tools, which rely principally on IP-based and SSID-based identification techniques,[302] generally do not collect PII and therefore do not pose a serious privacy risk.[303] This is the case because server-side geolocation technologies are not meant to identify a *particular* user. Rather, these tools seek to identify users only at the regional or community-level,[304] and are usually able to pinpoint a user only within a twenty- to fifty-mile radius.[305] This level of specificity is insufficiently "precise" to bring the resulting location data within the FTC's Behavioral Advertising Principles.[306] Furthermore, because most Internet Service Providers (ISPs) provide users with constantly rotating dynamic IP addresses, a particular address could be utilized by several different users over just a few days time—thus making matches between an individual and a specific IP address virtually impossible.[307]

In some cases, geolocation data can be combined with other forms of non-PII to create PII.[308] In most cases, however, location information generated by server-side geolocation tools would not be useful in such an enterprise. This is so because user data is often not stored once a location match has been made and transmitted to a site for content customization, localization, or other uses.[309] In fact, the increasing use of server-side

---

[302] *See supra* Part II.A.

[303] *See* Tedeschi, *supra* note 12 (explaining that geolocation mapping applications determine the location of the Internet service provider or server computer, not the exact location of the user).

[304] *See* Richmond, *supra* note 6 ("[T]he major geolocation companies say they don't track Web usage by IP address; rather, they simply maintain databases of IP addresses and their associated geographic locations."); Larry Dobrow, *Scratching the Surface on Geo-Location Services*, 1 TO 1MEDIA (Apr. 9, 2009), http://www.1to1media.com/view.aspx?DocID=31534 ("[C]ompanies using Quova get[ ] data about the location of an IP address and how that device has logged onto the Internet, as opposed to the e-mail or street address of a person.").

[305] Dobrow, *supra* note 304 (explaining that geolocation firms, such as Quova, can typically only locate a user within a twenty- to fifty- mile radius); *Quova's Geolocation Data Helps Continental Airlines Improve Web Banner CTR*, *supra* note 13 ("Quova provides IP address location data down to a metro area (25 to 50 miles) . . . .").

[306] *See* BEHAVIORAL ADVERTISING PRINCIPLES, *supra* note 285, at 42 & n.75, 43–44 (suggesting that a user's precise geographic location is a category of information that would be considered sensitive).

[307] *See* Dobrow, *supra* note 304.

[308] *See* BEHAVIORAL ADVERTISING PRINCIPLES, *supra* note 285, at 22–23 ("[I]t may be possible to link or merge non-PII with PII.").

[309] *See* Dobrow, *supra* note 304 ("Quova compiles no personal information

geolocation tools to prevent fraudulent transactions and unauthorized account access—for instance to online banking data—suggests that geolocation technologies can play a decidedly pro-privacy role in some circumstances.[310]

All of this could change when the imminent transition to the IPv6 addressing scheme begins, however.[311] To begin with, the vast amount of address space available under IPv6 will likely eliminate the need for ISPs to assign dynamic IP addresses. Similarly, the increased address space will also likely be the end of widespread private addressing—i.e., use of addresses in the 10.x.x.x and 192.x.x.x. ranges that cannot be resolved by devices outside of a user's home network.[312] The shift from dynamic to static and private to public addresses will in turn make it easier to focus on an individual user via IP-based geolocation. Second, by default, the IPv6 address format calls on clients to use their unique MAC address for half of the address.[313] In fact, it may even be possible to encode a device's specific location within an IPv6 address.[314] These features mean that IPv6 addresses will

whatsoever . . . .).

[310] *See* Liz Parks, *Pin-Pointing Perpetrators*, NRF STORES (June 2009), http://www.stores.org/stores-magazine-june-2009/pin-pointing-perpetrators; Richmond, *supra* note 6 (explaining how the Quova system has been used to protect against fraud and unauthorized credit card use).

[311] Currently, most devices connected to the Internet are assigned an IPv4 address consisting of four octets of data—for instance 192.168.0.1. *See* Iljitsch van Beijnum, *Everything You Need to Know About IPv6*, ARS TECHNICA (Mar. 7, 2007, 9:10 PM), http://arstechnica.com/hardware/news/2007/03/IPv6.ars. These addresses are necessary for the device to be able to successfully communicate with other Internet-connected devices; however, the explosive growth of the Internet since the mid-1990s has depleted the pool of available addresses. *See id.* Currently, less than 10% of the usable IPv4 address space remains available for allocation by ICANN, the Internet Corporation for Assigned Names and Numbers. *See* Iljitsch van Beijnum, *>90% of IPv4 Address Space Used; IPv6 Move Looking Messy*, ARS TECHNICA (Jan. 21, 2010, 8:05 PM), http://arstechnica.com/tech-policy/news/2010/01/90-of-ipv4-address-space-used-ipv6-move-looking-messy.ars [hereinafter Iljitsch van Beijnum II].

[312] *See* DANIEL O. AWDUCHE, VERIZON, BENEFITS OF IPV6 FOR ENTERPRISES 2 (2010), *available at* http://www.verizonbusiness.com/resources/whitepapers/wp_benefits-of-ipv6-for-enterprises_en_xg.pdf ("The abundance of IPv6 addresses allows the assignment of globally-unique IP addresses to objects within the enterprise environment, remov[ing] the need for private addressing . . . .").

[313] *See* Louise Mckeag, *The Basics of IPv6 Address Structure*, TECHWORD (June 22, 2004), http://features.techworld.com/networking/665/the-basics-of-ipv6-address-structures/ ("There's an option within IPv6 that will autoconfigure any v6 host address using its MAC address").

[314] *See Geolocation-Based Addressing Method for IPv6 Addresses*, WORLD INTELLECTUAL PROPERTY. ORGANIZATION,

likely contain considerably more private information than IPv4 addresses—raising new questions with regard to PII collection and once again illustrating Lessig's point that code is law.[315]

C. Application to Client-Side Geolocation Tools

In contrast to server-side geolocation tools, client-side technologies initiate the location process via an individual's Internet-connected device, for instance by sending a query to the device's GPS chip.[316] This user-centric model makes client-side technologies much more likely to collect and disseminate *personally* identifiable information, as opposed to just generally identifiable information of the kind most often associated with server-side technologies. In addition to their much closer nexus with a particular user, client-side geolocation tools offer a much higher degree of accuracy than server-side tools, since iPhones and other GPS-equipped wireless devices can frequently be located within a radius of a few dozen feet.[317] Because that level of accuracy can safely be said to involve a user's "precise geographic location," client-side geolocation tools almost certainly involve the collection of PII.[318] The caution exercised by Google and Facebook in rolling out new client-side geolocation features lends further support to this view, as the notice and consent steps taken by each are fully consistent with treatment of the geolocation data as PII. The privacy policy accompanying Google's My Location service goes one step further in stating that:

> If you allow a website to get your location via this service, we will collect, depending on the capabilities of your device, information

http://www.wipo.int/pctdb/en/wo.jsp?wo=2008006041&IA=US2007072886 (last visited Jan. 5, 2011) ("[T]he IP[v6] address requested . . . may be assigned by encoding the geographical location into the IP address.").

[315] *See id.* (explaining how IPv6 addresses will collect location data and track locations by updating the IP address when movement occurs). Market-driven re-allocation of IPv4 addresses, combined with advanced features of IPv6 such as mobility and multi-homing may complicate geolocation efforts, however. *See* Iljitsch van Beijnum II, *supra* note 311. Other commentators are divided on this ultimate conclusion, however, with some arguing that geolocation will become *more* difficult and less precise under IPv6. *See* Svantesson, *supra* note 1, at 118–19.

[316] *See supra* Part II.A.

[317] *See* Hiawatha Bray, *Software Puts Captions on the Real World*, BOSTON GLOBE, Sept. 24, 2009, at B7 ("GPS and compass data are only accurate to within a few dozen feet.").

[318] *See* BEHAVIORAL ADVERTISING PRINCIPLES, *supra* note 285, at 22, 44.

> about the wifi routers closest to you, cell ids of the cell towers closest to you, and the strength of your wifi or cell signal. We use this information to return an estimated location to the Firefox browser and the Firefox browser sends the estimated location to the requesting website. For each request sent to our service, we also collect IP address, user agent information, and unique identifier of your client. We use this information to distinguish requests, not to identify you.[319]

Those somewhat cautious steps notwithstanding, a recent study by researchers at the University of California-Berkeley School of Information indicates that numerous high-profile websites collect geolocation data via the W3C Geolocation API without providing notice or securing consent.[320] These findings strongly suggest that the FTC's scarce enforcement resources should be focused on encouraging sites that use client-side geolocation tools to provide users with notice- and consent-based safeguards.

D. Consent vs. Mandates – Doctrines in Conflict

FTC regulations require, or in the context of behavioral advertising, forcefully suggest, that sites must obtain a user's consent before collecting precise geographic location data.[321] This approach is consistent with that advocated by privacy theorist Peter Swire, who has argued that "individuals should have a realistic way to choose not to be profiled when they go online."[322] While this consent-based approach may be normatively desirable when viewed in a vacuum, it causes problems for sites subject to direct or indirect geolocation mandates. Assume for a moment that geolocation data is classified as PII and that sites must allow users to control whether that data is collected. Under this regime, a significant number of consumers will opt out, meaning that sites will not be able to geographically locate those users. This inability to locate opt-out users would mean that sites could not effectively regulate access to sensitive content, as may be necessary to avoid personal jurisdiction in a remote forum or to comply with state Internet commerce laws.[323]

---

[319] *Privacy Center: Google Location Service in Mozilla Firefox Privacy Policy*, GOOGLE (Apr. 24, 2009), http://www.google.com/privacy-lsf.html.

[320] *See Berkeley W3C Study*, *supra* note 3, at 8–10.

[321] *See supra* Part V.A.

[322] Peter Swire, CTR. FOR AM. PROGRESS, WE ARE THE WEB (Dec. 18, 2007), http://www.americanprogress.org/issues/2007/12/we_are_the_web.html.

[323] *See supra* Parts III.–IV.

There are several potential solutions to this conflict between privacy law on the one hand, and personal jurisdiction and Internet commerce law on the other. In view of the need of sovereigns to be able to protect their citizens from online harms, the best solution to this conundrum may be to allow sites to geo-locate users without permission when doing so is necessary to comply with an independent legal obligation. Such a rule would prevent users from effectively treating consent requirements as a way to circumvent access controls. In this regard, if a user is located in the United States and wants to gamble on PartyPoker.com (a site that blocks access to all U.S. customers), the user should not be able to gain access merely by refusing to allow Party to determine his or her location in the first instance. An alternative to this approach would be to use technological intermediaries to provide a "thin" layer of location information on a one-time basis when a site must geo-locate a user who otherwise opts-out. For example, users could designate a privacy-focused proxy server in their browser settings to provide geolocation data when necessary, or simply instruct their browser to provide only the most general level of location detail necessary to meet a site's needs. The W3C Geolocation API's implementation in Mozilla Firefox resembles this last option, as it allows users to express some general preferences about the way client-side location data is shared.[324]

VI. CONCLUSION

Though no such capability existed less than a decade ago, modern geolocation technologies now offer an automatic, accurate, and, for the commercial sector, affordable means of identifying an Internet user's geographic location. Attracted by these benefits, a wide range of websites now use geolocation tools for content localization, access control, fraud prevention, and other purposes. While the marketplace has reacted swiftly to geolocation technologies, the law has reacted slowly where it has reacted at all.

In areas such as personal jurisdiction and dormant Commerce Clause doctrine, geolocation technologies will—or at least as this article argues, should—shape legal outcomes in a great many ways. These changes will likely include modification of the *Zippo*

[324] *See Berkeley W3C Study*, *supra* note 3, at 6–7 (discussing the methods websites use to obtain permission to access geolocation data of users).

test to effectively require sites to use geolocation tools in some contexts in order to avoid personal jurisdiction in remote fora, for instance. With respect to privacy, however, the question is not how geolocation will affect the law; but rather how the law will affect geolocation. Though current technologies pose only a limited threat to individual privacy, client-side tools just now beginning to come into use involve a much more significant risk.

At a macro level, the three doctrinal analyses above reveal significant linkages between one another. For instance, the First Amendment plays a significant role in limiting the ability of courts and legislatures to impose geolocation mandates. This limitation comes up directly in the context of federal and state Internet commerce regulations, as a geolocation mandate on non-commercial, advocacy-oriented sites would likely constitute an unconstitutional burden on protected speech. As described in parts III and IV above, these types of speech-infused sites frequently lack the financial means to implement geolocation tools, and would close down if subjected to a mandate. In the personal jurisdiction context, the First Amendment plays a less obvious, though nonetheless limiting role. If courts adopted a *per se* rule subjecting sites to personal jurisdiction in any forum in which they are available, that rule would, in effect, amount to an indirect geolocation mandate. Such a mandate would face the same First Amendment difficulties as direct mandates imposed by Congress or the States.

Additionally, the well-entrenched policy that sites must procure users' consent before collecting personally identifiable information is in tension with the need for some sites to identify and screen all users according to location—thus giving rise to a conflict between privacy law and the other two bodies of law discussed above. As courts, legislatures, and agencies adapt existing law to respond to the difficulties posed by geolocation tools, they should remain cognizant of these tensions and linkages, as the structure of a rule in one area of the law could have profound ramifications in several others.