Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws

Tony Glosson*

TABLE OF CONTENTS

**J.D., The George Washington University Law School, 2015; Associate, Drinker Biddle & Reath LLP.* *I would like to thank Matthew Gerst for his helpful guidance and encouragement; Berin Szoka for the conversations that sparked my interest in this topic; Stephan Satterfield for providing valuable feedback on my arguments; and Natalie Roisman and Ryan Wallach for showing me how much fun communications law can be.*

I. INTRODUCTION

In 2013, Target drew fire for mailing pregnancy-themed advertisements to a teenage girl who had not yet revealed her pregnancy to her parents.[1] Drawing from myriad data points including age, income, address, ethnicity, spending patterns, and more, Target's analytics algorithm identified the girl as likely to be pregnant.[2] In other words, Target knew before her parents did—ultimately forcing her hand in the timing of her announcement to her family.[3]

Even as privacy advocates increasingly express concern, the demand for consumer data is exploding. One industry study projects that consumer data collection—or colloquially, "big data"—will be a $16.9 billion industry in 2015, up from $3.2 billion in 2010.[4] Simultaneously, it is becoming cheaper to gather information. Consulting firm McKinsey & Co. has estimated a growth rate of roughly 40% in consumer data collected year over year, with a mere 5% corresponding increase in IT spending.[5] In fact, the growth in data collection may force major changes in technological infrastructure: according to some reports, over half of the surveyed C-level executives acknowledge that their infrastructure lacks the capacity to handle the demands of modern data collection.[6]

But the story does not end with the collection of traditional demographic data by previously disinterested players. Instead, wholly new data points emerge daily, each with its own set of privacy implications. The so-called Internet of Things—geek-speak for network connectivity built into traditionally "dumb" apparatus like refrigerators or thermostats—allows collection of personal data in the unlikeliest of places.[7]

---

1. Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 02, 2012), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

2. *See id.*

3. Since this revelation, California lawmakers have introduced a ballot measure that would potentially provide tort damages for instances like this one where companies use consumer data in an unpredictable way without first obtaining the data subject's affirmative permission. *See* Cynthia Larose, *Will California Voters Move US to Opt-In?*, PRIVACY & SECURITY MATTERS (Aug. 6th, 2013), http://www.privacyandsecuritymatters.com/2013/08/3949/.

4. *Big Data Will Be a $16.9 Billion Market by 2015: IDC*, IDC (Mar. 09, 2012), http://www.cioinsight.com/c/a/Latest-News/Big-Data-Market-to-Grow-to-169-Billion-by-2015-IDC-118144/.

5. James Manyika et al., *Big Data: The Next Frontier For Innovation, Competition, And Productivity*, MCKINSEY GLOBAL INSTITUTE (May 2011), http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

6. *Is Big Data Producing Big Returns?*, AVANADE (June 2012), http://www.avanade.com/en-us/approach/research/pages/big-data.aspx.

7. Michael Chui et al., *The Internet of Things*, MCKINSEY GLOBAL INSTITUTE (Mar. 2010), http://www.mckinsey.com/insights/high_tech_telecoms_Internet/the_Internet_of_things; *see*

But what role should the law play in guarding privacy during the data revolution? More fundamentally, *whose* law should play *which* roles in our federalist system? The allocation of regulatory authority over data collection may be as consequential as the substantive regulations imposed.[8] On the one hand, technology firms view the prospect of a medley of fifty assorted state privacy regimes as economically unworkable, and have already begun to object that recent state laws are "impossible to implement" and "extremely burdensome for start-up [companies]." [9] These firms assert that, if data collection is to be regulated, it is the role of the federal government to implement a single, coherent set of laws that apply nationwide.[10] Some state attorneys general, meanwhile, argue that the federal government might not act as quickly or as sweepingly as they would like.[11]

This Note offers a constitutional framework for analyzing the distribution of regulatory authority over data privacy, and ultimately concludes that the Dormant Commerce Clause precludes most state data privacy legislation.[12]

A. Overview of Note

When assessing state data privacy law, the challenge is to apply traditional principles of federalism to a revolutionary industry. The academic literature in this emerging field is somewhat sparse. Nonetheless, established constitutional doctrines guide this inquiry and this Note proffers a methodical application of those principles to the growing body of state data privacy laws.

This Note begins by reviewing a seminal district court decision on state Internet regulation, *American Library Association v. Pataki*.[13] *Pataki*

---

also FTC Seeks Input on Privacy and Security Implications of the Internet of Things, FTC (Apr. 17, 2013), http://www.ftc.gov/news-events/press-releases/2013/04/ftc-seeks-input-privacy-and-security-implications-Internet-things.

8. In this regard, it is worth considering the implications for the national economy should individual states continue down the path of the European Union, which has enacted stringent data privacy regimes forbidding data transfers to nations with less demanding privacy laws. If certain states enact similar laws aimed at preventing data transfers to other states that do not have congruent privacy protections, it is not difficult to imagine, for example, a startup webmail company becoming trapped in California, unable to transfer its data to new servers in Texas if the latter state had fewer privacy protections.

9. Steven Harmon, *Silicon Valley tech firms win privacy bill battle*, MERCURY NEWS (May 3, 2013), http://www.mercurynews.com/ci_23160780/silicon-valley-tech-firms-win-privacy-bill-battle.

10. Jessica Meyer, *States Defend Turf from Feds on Data Breach Rules*, POLITICO (Feb. 19, 2014), http://www.politico.com/story/2014/02/states-defend-turf-from-feds-on-data-breach-rules-103647.html.

11. *See id.*

12. Importantly, this note does *not* argue that any particular privacy protection, or set of protections, are good or bad policy objectives. Rather, this note suggests that as a matter of constitutional law, those policy debates must transpire at the federal level.

13. American Library Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997).

demonstrates how courts have traditionally applied the Dormant Commerce Clause doctrine in the Internet context. Next, the Note addresses the ways in which modern technology has altered the applicability of the *Pataki* analysis. Finally, this Note concludes that geolocation changes the Dormant Commerce Clause analysis, but leaves several problems with state data privacy laws unresolved.

It bears mention that there are a number of constitutional grounds on which an entity might challenge state Internet regulations. Although this Note focuses on one, the Dormant Commerce Clause, state Internet regulations may implicate constitutional doctrines like preemption and personal jurisdiction as well.

II. BACKGROUND

The federal government has enacted a number of laws regulating elements of Internet activity and commerce.[14] However, many of those laws deal with criminal concerns such as hacking or gambling, or particular sets of data such as health records or information about children. Unlike most European countries,[15] and the European Union as a whole,[16] the United States has not enacted an overarching set of data privacy standards.[17] Instead, the United States tends toward spot-regulation, targeting specific data privacy issues or high-risk industries.[18] The closest the United States has come to enacting a uniform standard is the Federal Trade Commission's ("FTC") authority to prosecute "unfair or deceptive" business acts or practices,[19] which the FTC has interpreted to include regulation of data protection practices.[20] Some states, perceiving a gap in privacy protections,

14. *See, e.g.*, Unlawful Internet Gambling Enforcement Act, 31 U.S.C. §§ 5361–5367 (2012); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012); Internet Tax Freedom Act, Public Law No. 105-277, Title XI (1998) (extended until Dec. 11, 2015).

15. *See, e.g.*, Germany's Federal Data Protection Act (Bundesdatenschutzgesetz), http://translate.google.com/translate?hl=en&prev=search&sl=de&u=http://www.bfdi.bund.de/SharedDocs/Publikationen/GesetzeVerordnungen/BDSG.pdf%3F__blob%3DpublicationFile&sandbox=0&usg=ALkJrhi0OuKjCszTXrsZgauQoKtf97Uziw; European Commission, *National data protection authorities*, EU JUSTICE (last visited May 05, 2015), http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm.

16. *See* Elizabeth Dwoskin, *EU Seeks to Tighten Data Privacy Laws*, WALL ST. J. (Mar. 10, 2015), http://blogs.wsj.com/digits/2015/03/10/eu-seeks-to-tighten-data-privacy-laws/.

17. Paul M. Schwartz, *The Eu-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013) [hereinafter Schwartz, *Eu-U.S. Privacy Collision*].

18. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, Aug. 21, 1996, 110 Stat. 1936.

19. *See* Federal Trade Commission Act, 15 U.S.C. § 45.

20. *See* Pl.'s Opp. Mot. Dismiss, *FTC v. Wyndham Worldwide Corp.*, 2012 WL 4766957 (D. Ariz.).

have passed their own privacy regulations.[21] For example, several states have enacted data breach disclosure obligations, which mandate that businesses inform their customers when private information may have been compromised in a data breach.[22] More aggressive examples include California's "Online Eraser" law, which requires websites to implement a mechanism for registered users who are minors to take down any embarrassing past posts,[23] and California's "Do Not Track" law, which requires website operators to explain how they respond to data collection opt-out signals sent by users' browsers.[24] This patchwork of state laws can be particularly onerous for Internet-based companies because, in addition to tracking the developments in fifty-one jurisdictions, they must also tailor their products to comply with sometimes-conflicting demands under state laws. These state laws also raise questions regarding the constitutional allocation of regulatory authority over the Internet.

Under the U.S. Constitution, state authority is limited by several provisions, including the so-called "Dormant Commerce Clause." The Commerce Clause grants to Congress the power "[t]o regulate commerce . . . among the several states . . . ."[25] Over time, the courts have recognized that this grant of federal power precludes the states from enacting regulations that unjustifiably burden interstate commerce.[26] Nevertheless, states retain a residuum of power by which they may regulate matters affecting their citizens' health and safety, even if those regulations have an incidental effect on interstate commerce.[27] Accordingly, the constitutional analysis of a state data privacy law examines whether the law's effects on interstate commerce adequately respect the sovereignty of the coequal states over their own economies.

21. *State Laws Related to Internet Privacy*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 02, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-Internet-privacy.aspx.

22. National Conference of State Legislatures, *Security Breach Notification Laws*, NCSL RESEARCH (last visited May 06, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

23. *See* S.B. 568, 2013-14 Sess. (Cal. 2013), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

24. *See* A.B. 370, 2013-14 Sess. (Cal. 2013), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370.

25. *Id.* art. I, § 8, cl. 3.

26. City of Philadelphia v. New Jersey, 437 U.S. 617, 623 (1978)

27. Southern Pacific Co. v. Arizona. *ex rel.* Sullivan, 325 U.S. 761, 766 (1945).

III. THE DORMANT COMMERCE CLAUSE AND THE EARLY APPROACH TO THE INTERNET: *AMERICAN LIBRARY ASSOCIATION V. PATAKI*

American Library Association v. Pataki, decided in 1997, was one of the first cases to apply the Dormant Commerce Clause to a state Internet regulation.[28] Since that decision, three circuit courts have adopted the *Pataki* court's reasoning to invalidate other state legislation regulating the Internet.[29] In *Pataki*, the law at issue was a New York statute that prohibited transmitting obscene content to minors.[30] Because libraries often provide content through their websites that could be considered obscene, the American Library Association ("ALA") sued to enjoin New York from enforcing the law. The ALA explained that its members generally did not know the ages or locations of their website visitors, and were therefore concerned that they would need to censor content that was perfectly legal in other states to guard against prosecution under New York law.[31]

The court agreed, and issued an injunction.[32] Judge Preska began her analysis by noting that laws governing the Internet inherently regulate interstate commerce.[33] She observed that "Internet protocols were designed to ignore rather than document geographic location;"[34] that the Internet itself is an instrument of interstate commerce because it "serves as a conduit for transporting digitized goods;"[35] and that "the novelty of the technology should not obscure the fact that regulation of the Internet impels traditional Commerce Clause considerations."[36] Having established that Dormant Commerce Clause principles apply to Internet regulations, Judge Preska worked through three independent modes of Dormant Commerce Clause doctrine: (a) extraterritoriality; (b) *Pike* balancing; and (c) susceptibility to inconsistent regulations.[37]

28. *Pataki*, 969 F. Supp. 160 (1997).

29. *See, e.g.*, American Booksellers Foundation v. Dean, 342 F.3d 96 (2d Cir. 2003); American Civil Liberties Union v. Johnson, 194 F.3d 1149 (10th Cir. 1999); PSINet, Inc. v. Chapman, 362 F.3d 227 (4th Cir. 2004).

30. *See* N.Y. Penal Law § 235.20(6).

31. *Pataki*, 969 F. Supp. at 162.

32. *See id*.

33. *Id*.

34. *Id*. at 170.

35. *Id*. at 173.

36. *Id*.

37. *Id*.

A. *Extraterritoriality: New York's Law Was Invalid Because It Necessarily Governed Wholly Out-of-State Transactions.*

Extraterritoriality doctrine holds that a state law is invalid if it regulates transactions outside the borders of the regulating state.[38] Judge Preska invoked several Supreme Court extraterritoriality decisions to hold the New York law invalid, including *Healy v. The Beer Institute*[39] and *Southern Pacific Co. v. Arizona*.[40]

First, in *Healy v. Beer Institute*, the Court invalidated a Connecticut statute that required beer distributers to affirm that the prices they charged in Connecticut did not exceed those charged in neighboring states.[41] Though the distributors were free to charge whatever prices they wished in other states, the affirmation requirement for beer shipped to Connecticut effectively compelled the distributors to account for the Connecticut market when making price determinations for other states.[42] The Supreme Court invalidated the provision, noting that a law may violate the commerce clause "regardless of whether the statute's extraterritorial reach was intended by the legislature."[43] The inquiry, according to the *Healy* court, is simply "whether the practical effect of the regulation is to control conduct beyond the boundaries of the State."[44] Moreover, the Supreme Court reasoned, the analysis turns on "what effect would arise if not one, but many or every, State adopted similar legislation."[45] Under this analysis, the Connecticut statute was unconstitutional because distributors had to take Connecticut price law into account while engaging in wholly out-of-state liquor sales, thereby precluding them from setting promotional prices or taking full advantage of unique market conditions in neighboring states.[46]

Second, in *Southern Pacific Co. v. Arizona*, the Court held unconstitutional an Arizona train length limitation because, as a practical matter, it forced railroad companies to limit the length of their trains in every state on the rail line.[47] Although the statute purported to regulate only trains within Arizona's borders, the Court in that case reasoned that a law that made it economically infeasible to tailor compliance to the regulating state had the same practical effect as one that explicitly regulated conduct within other

38. Healy v. The Beer Institute, 491 U.S. 324 (1989).
39. *Id.*
40. Southern Pacific Co. v. Arizona, 325 U.S. 761 (1945).
41. *Healy*, 491 U.S. 324.
42. *Id.*
43. *Id.* at 336.
44. *Id.*
45. *Id.*
46. *Id.* at 338-40.
47. *Southern Pacific Co.*, 325 U.S. at 775.

states.[48] Accordingly, the Arizona statute was unconstitutional under the extraterritoriality mode of Dormant Commerce Clause analysis.[49]

Applying those concepts to the New York law, Judge Preska determined that the law contained the same constitutional defects as the Connecticut statute in *Healy* and the Arizona statute in *Southern Pacific*.[50] Because website administrators could not determine whether a user resided in New York or elsewhere, much less the user's age, it was impossible to spot-comply with New York's statute.[51] Citing testimony that the plaintiffs had restricted the content available on their website nationwide to comply with New York's statute, Judge Preska concluded that New York's law was an "encroachment upon the authority which the Constitution specifically confers upon the federal government and upon the sovereignty of New York's sister states."[52] Thus, the extraterritoriality analysis counseled in favor of granting the injunction.

B. Pike Balancing: New York's Law Was Unconstitutional Because It Substantially Chilled Interstate Commerce with Few Countervailing Local Benefits.

Judge Preska next moved to a second mode of Dormant Commerce Clause analysis, the *Pike* balancing test.[53] *Pike* balancing, derived from the Supreme Court's analysis in *Pike v. Bruce Church*, applies to state laws that indirectly regulate interstate commerce.[54] The difference between a direct regulation of interstate commerce and an indirect one is not always a bright line, but the inquiry centers on whether a regulation facially applies to out-of-state transactions.[55] The *Pike* analysis consists of two steps: first, the court must determine the legitimacy of the state interest in enforcing the law; and second, the court must weigh the burden that the law places on interstate commerce against its legitimate local benefit.[56]

---

48. *Id.* at 774-75.
49. *Id.* at 775.
50. *Pataki*, 969 F. Supp. at 176-77.
51. *Id.*
52. *Id.*
53. *Id.*
54. 397 U.S. 137, 142 (1970).
55. Brown-Forman Distillers Corp. v. New York State Liquor Auth., 476 U.S. 573, 578-79 (1986):

> This Court has adopted what amounts to a two-tiered approach to analyzing state economic regulation under the Commerce Clause. When a state statute directly regulates or discriminates against interstate commerce, or when its effect is to favor in-state economic interests over out-of-state interests, we have generally struck down the statute without further inquiry.

56. *Id.* at 579.

In evaluating the legitimacy of an asserted state interest, courts give the legislature wide latitude to determine the problems their constituents face, and the relative benefit of solving them.[57] Stating that "[i]t is evident beyond the need for elaboration that a State's interest in safeguarding the physical and psychological well-being of a minor is compelling," Judge Preska quickly determined that New York's prohibition on obscene-for-minors internet communications fell within the legitimate scope of state interest.[58]

New York's law, however, did not fare as well under *Pike*'s second prong: because the law could not possibly affect content originating from outside the United States, the local benefits were "not overwhelming."[59] Foreign obscene-for-minors content is just as readily accessible to New York children as United States content, the court noted.[60]

On the other hand, the burden on interstate commerce was "extreme."[61] Beyond the burden of removing content actually deemed illegal under the New York law, website administrators would likely be forced to "steer clear of the Act by a significant margin."[62] Unsure of whether a given set of content—say, a library's collection of artwork—would offend New York's community standards of obscenity for minors, a website administrator may decide not to host that content on its site, regardless of whether the artwork was, in fact, obscene for New York minors.[63] Judge Preska then reasoned that the modest local benefits could not outweigh the law's burden on interstate commerce.[64] Accordingly, New York's law failed under the *Pike* test as well as under the extraterritoriality analysis.[65]

C. Inconsistent Regulations: New York's Law Was Unconstitutional Because Permitting States to Govern the Internet Would Result in Interlocking Regulatory Schemes that Would Stifle Interstate Commerce.

Finally, Judge Preska turned to the probability that, were other states to enact similar laws, website administrators could be subjected to inconsistent regulatory schemes.[66] In *Southern Pacific Co. v. Arizona*, the

57. *Pike*, 397 U.S. at 148.
58. *Pataki*, 969 F. Supp. at 169 (*citing* New York v. Ferber, 458 U.S. 747, 756–57 (1982)).
59. *Id.* at 170.
60. *Id.*
61. *Id.* at 171.
62. *Id.* at 179.
63. *Id.* at 179.
64. *Id.*
65. *Id.* at 183.
66. *Id.*

Court was particularly concerned that differing state regimes would create confusion for train operators given the inherently interstate nature of their businesses, observing that, "[w]ith such laws in force in states which are interspersed with those having no limit on train lengths, the confusion and difficulty with which interstate operations would be burdened under the varied system of state regulation and the unsatisfied need for uniformity in such regulation, if any, are evident."[67] There was, of course, one way a railroad could comply with all such limits: by configuring all of its trains to meet the most stringent limit. The railroad in *Southern Pacific* was forced to resort to that strategy, causing the Supreme Court to note disapprovingly that the effect of Arizona's length limit was to regulate trains "all the way from Los Angeles to El Paso."[68] Similarly, in *Bibb v. Navajo Freight Lines*, the Court invalidated an Illinois statute that required trucks on its highways to use contoured mud guards.[69] In that case, different states had contradictory mud guard requirements, so truckers would have to carry multiple sets of mud guards to change out during trips through states with different standards.[70]

Importantly, in neither case was compliance with the differing state regulatory schemes *technically impossible*. Indeed, Judge Preska noted that "the truck driver or train engineer . . . can steer around Illinois or Arizona, or change the mudguard or train configuration at the state line."[71] Rather, in both decisions, the Supreme Court struck the regulations down because compliance would be *economically infeasible*. Specifically, both laws would have forced businesses operating primarily through the instruments of interstate commerce to track and comply with numerous sets of regulatory schemes—a tall order even for the relatively well-established freight businesses in those cases.[72]

Applying the rationale behind both these cases to the facts in *Pataki*, Judge Preska concluded that the New York law was also likely to be unconstitutional under the third mode of analysis because other states would enact different regulatory standards, forcing website administrators either to track developments in each state and comply with each individually, or else to comply with the most stringent across the board.[73] This predicament was substantially the same as the choice put to railroads in *Southern Pacific* and truckers in *Bibb*, and resulted in the same constitutional defects for the New York law.[74] Having determined that New York's obscenity-for-minors statute impermissibly burdened online interstate commerce under each of the

67. *Id.* at 181 (quoting *Southern Pacific Co.*, 325 U.S. at 773-74).
68. *Southern Pacific Co*., 325 U.S. at 774.
69. 359 U.S. 520 (1959).
70. *Id.* at 525.
71. *Pataki*, 969 F. Supp. at 183.
72. *Id.*
73. *Id.* at 181-82.
74. *Id.*

three proffered Dormant Commerce Clause analyses, Judge Preska preliminarily enjoined enforcement of the law.[75]

IV. GEOLOCATION TECHNOLOGY CHANGES THE DORMANT COMMERCE CLAUSE ANALYSIS, BUT NOT NECESSARILY THE RESULT

Pataki has since become a landmark case in Internet law.[76] It is not, however, without its weak points. For one, *Pataki*'s language, at times, seems to foreclose *any* state laws affecting the Internet,[77] although in the context of the Court's balancing analysis, that interpretation seems strained. One commentator suggests that the Court wrongly imported elements of First Amendment scrutiny into its Dormant Commerce Clause analysis by framing the law's burden in terms of its "chilling effect" on commerce.[78] But today, the most common critique is that dramatic improvements in geolocation capabilities—technologies that enable service providers to identify a user's location—have undermined the *Pataki* analysis.[79] This Section briefly overviews the state of modern geolocation technology, then walks through their implications for the *Pataki* analysis, and concludes that geolocation does not solve the Dormant Commerce Clause problems with many state data privacy laws.

Businesses use a variety of geolocation technologies today. Four of the most common are Internet protocol (IP) geolocation, WiFi network mapping, cell site geolocation, and GPS.[80] IP geolocation relies on Internet protocol addresses, the structural feature of the Internet that permits computers to identify and communicate with one another. Internet service providers (ISPs) obtain blocks of IP addresses that they then distribute to customers.[81] Thus, if one knows that a user's IP address is associated with an ISP located in

75. *Id.* at 183.

76. *See, e.g.*, ORIN S. KERR, COMPUTER CRIME LAW 697 (2013) (excerpting Pataki as the first case for state-based Internet regulations).

77. *Pataki*, 969 F. Supp. at 177 ("New York has deliberately imposed its legislation on the Internet and, by doing so, projected its law into other states whose citizens use the Net."). This criticism, however, seems to undervalue the *Pike* balancing analysis, which would permit some state internet regulations

78. James E. Gaylord, *State Regulatory Jurisdiction and the Internet: Letting the Dormant Commerce Clause Lie*, 52 VAND. L. REV. 1095, 1116 (1999) [hereinafter *State Regulatory Jurisdiction*].

79. *See, e.g.*, Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785 (2001) [hereinafter *The Internet*].

80. Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 567, 594 (2012) [hereinafter *The Future of Cybertravel*]; Timothy J. Van Hal, *Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for A Class Action Regime for Privacy Protection*, 15 VAND. J. ENT. & TECH. L. 713, 716 (2013) [hereinafter *Taming the Golden Goose*].

81. Trimble, *supra* note 110, at 594.

Illinois, that information supports a preliminary inference that the user is accessing the service from Illinois.

The second method, WiFi network mapping, is a relatively newer technology.[82] Companies that offer WiFi network mapping services collect data on the names of WiFi networks and their corresponding locational coordinates.[83] Once a company has compiled a sufficiently large database of WiFi networks, it can query a user's device for names of nearby WiFi networks, and compare the response to the database, establishing the device's location.[84] Cell site geolocation and GPS technologies can help determine the location of users accessing a website or application from a mobile device configured to permit disclosure of location data.[85]

The accuracy of these technologies is somewhat disputed.[86] However, most accept that, using some combination of the available technologies, geolocation accuracy is at least in the eighty percent range at the state level. Estimates run up to 99.9 percent accuracy on the high end.[87] Even if geolocation is insufficiently accurate for legal purposes at the present, the progress of technology may moot the accuracy debate in the relatively near future.[88] Still, location-masking tools will likely continue to advance as well, so no geolocation regime will be perfect in all situations.

A. Extraterritoriality: Geolocation Mandates Are On Constitutionally Questionably Ground Because They Directly Regulate Wholly Out-of-State Transactions

The advancement in technology has several implications for the analysis employed in *Pataki*. First, geolocation muddies the once

82. Van Hal, *supra* note 110, at 717.

83. *Id.* at 118

84. *Id.*

85. *Id.* at 716.

86. Trimble, *supra* note 110, at 598; *see also* Mahesh Balakrishnan, et al., *Where's That Phone?: Geolocating IP Addresses on 3G Networks*, 9 ACM SIGCOMM 294 (2009).

87. Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61, 70 (2011) (citing PriceWaterhouseCoopers, Report of Independent Accountants: Quova. Inc., 3 (Oct. 23, 2008), http://www.quova.com/documents/PricewaterhouseCoopers_Audit.pdf) ("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.") [hereinafter *Personal Jurisdiction*]; Kevin F. King, G*eolocation and Federalism on the Internet: Cutting Internet Gambling's Gordian Knot*, 11 COLUM. SCI. & TECH. L. REV. 41, 59 (2010) ("Experts have estimated accuracy rates of between 85 and 98 percent at the state level and over 99 percent at the national level.") [hereinafter *Geolocation and Federalism*]; *see also* Pioneer Military Lending, Inc. v. Dufauchard, CIV S061445 LKKPAN, 2006 WL 2053486 (E.D. Cal. 2006) (reciting a forensic expert's assessment that "the accuracy level of a 'state level' geolocation investigation is approximately 80% to 99% accurate"). Note that the latter assessment reflects the state of the technology over eight years ago.

88. *Cf.* Trimble, *supra* note 110.

straightforward extraterritoriality analysis. Unlike *Pike* balancing, which applies to laws governing commercial activity with *both* in-state and out-of-state elements, extraterritoriality doctrine is concerned with the possibility of *wholly out-of-state* application of state laws.[89] The *Pataki* court, in addressing extraterritoriality, relied heavily on the idea that "[a]n Internet user who posts a Web page cannot prevent New Yorkers or Oklahomans or Iowans from accessing that page and will not even know from what state visitors to that site hail."[90] As a result, *all* website administrators would need to comply with New York law during *all* transactions or risk liability in the case of the indistinguishable New York visitor. On this understanding, the *Pataki* court concluded that New York's regulation necessarily imposed its policy preferences on out-of-state transactions. In the Court's parlance, New York was *directly* regulating out-of-state commerce, as there was no way to isolate in-state commerce.[91] Under the extraterritoriality analysis, then, the law was *per se* invalid.

With the advent of geolocation technology, however, the question becomes more complex. Now it *is* often possible, at least in theory, to distinguish communications sent to devices in New York from those sent to devices in any other state. At this point, the extraterritoriality conversation undergoes an important shift: no longer is the analysis centered on the problems associated with identifying the jurisdiction in which a user resides; instead, firms have the option of implementing geolocation technologies, then blocking or tailoring their services on a state-by-state basis.

In many cases, firms would likely choose to comply with the most stringent state laws across the board, rather than incurring the expense of adopting geolocation technologies and tailoring their products accordingly. Consequently, the result from an end-user standpoint is indistinguishable from a *Pataki*-like regime in which the provider universally complies with one state's law because it cannot possibly know whether it governs a transaction. Either way, providers are choosing to apply the regulating state's law universally, even as they reach that decision for different reasons. From a *legal* standpoint, however, a court might decide that the technical possibility of tailoring content's availability based on geolocation is all that matters, even if that option is economically infeasible.

The analysis is further complicated by the fact that extraterritoriality doctrine is unsettled. As one commentator aptly noted: "[c]yberspace imbues state regulation with tremendous potential for extraterritorial effect, potential which invites the federal judiciary to cut down a broad swath of state law. This invitation is made all the more appealing by the rather amorphous nature

89. *See Brown-Forman Distillers Corp. v. New York State Liquor Auth*., 476 U.S. 573, 582 (1986).

90. *Pataki*, 969 F. Supp. at 171.

91. *Id.* at 177.

of the Supreme Court's extraterritoriality jurisprudence."[92] *Healy* provides perhaps the most complete judicial expression of extraterritoriality doctrine:

> Taken together, our cases concerning the extraterritorial effects of state economic regulation stand at a minimum for the following propositions: First, the Commerce Clause precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State, and, specifically, a State may not adopt legislation that has the practical effect of establishing a scale of prices for use in other states. Second, a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State.[93]

The Court then continued:

> Third, the practical effect of the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation. Generally speaking, the Commerce Clause protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State.[94]

Initially, cases in which the cost of tailoring exceeds the cost of compliance appear to implicate that "practical effects" element of extraterritoriality doctrine. Clearly, should providers of online services overwhelmingly choose to comply with a state law across the board, one might conclude the "practical effects" of that state law have altered transactions outside the state's borders.

Nonetheless, a question exists as to whether the ability to block one's service from a particular state's market, rather than complying with that state's laws, takes state Internet-governance regimes out of the realm of *direct* commercial regulations to which extraterritoriality analysis pertains.

92. Gaylord, *supra* note 78, at 1097.
93. Healy v. Beer Institute, 491 U.S. 324, 336-37 (1989) (internal citations omitted).
94. *Id.*

After all, economies of scale provide a strong incentive to standardize products in *all* industries—not just online ones—and a great many state laws result in similar across-the-board compliance. [95] Are all such laws unconstitutional under the "practical effects" doctrine?

A closer look at the Supreme Court's "practical effects" cases suggests they are not. Specifically, the facts of those cases indicate that the Commerce Clause is concerned with laws that have the practical effect of subjecting wholly out-of-state transactions to *potential enforcement*—not merely those with which private parties choose to comply on an across-the-board basis for economic reasons. For example, in what some have called the "fount" of extraterritoriality jurisprudence,[96] *Edgar v. MITE Corp*., the Supreme Court struck down an Illinois corporate takeover law that governed any offers for firms in which "any two of the following three conditions are met: the corporation has its principal executive office in Illinois, is organized under the laws of Illinois, or has at least 10% of its stated capital and paid-in surplus represented within the State."[97] As *Pataki* noted, "[i]n striking the law as violative of the Commerce Clause, the [*Edgar*] Court found particularly egregious the fact that the Illinois law on its face would apply to a transaction that would not affect a single Illinois shareholder if a corporation fit within the definition of a 'target company.'"[98] Thus, the important "practical effect" was the law's enforceability against out-of-state transactions.

Similarly, in *Healy*, Connecticut could not possibly apply its price affirmation statute to liquor sellers without projecting its law into neighboring states.[99] By enforcing it at all, Connecticut threatened to penalize liquor sellers specifically on the basis of the terms of transactions occurring wholly outside of Connecticut borders.[100] Again, in *Brown-Forman Distillers v. New York*, the Court struck down a liquor price scheduling law that would have penalized sellers that provided lower-than-scheduled prices in other states without simultaneously lowering the New

95. For a discussion on a similar effect resulting from a California tobacco labeling law, *see* Lorillard Tobacco Co. v. Reilly, 84 F. Supp. 2d 180, 199-200 (D. Mass. 2000) *aff'd in part, rev'd in part sub nom.* Consol. Cigar Corp. v. Reilly, 218 F.3d 30 (1st Cir. 2000) *aff'd in part, rev'd in part sub nom.* Lorillard Tobacco Co. v. Reilly, 533 U.S. 525 (2001) ("In support of their argument that the cigar market requires uniform national regulation, the Cigar Companies point out that a regulation by California requiring a warning on all cigars has resulted in those California warnings appearing on 90% of all cigar packages in the United States and that the addition of other warnings from other states will result in multiple warnings on the same packaging . . . Those business decisions do not take a market of recreational consumer goods typically sold in local stores and automatically turn that market into one requiring national uniformity in regulation. The Cigar Warnings are not invalid on the basis of Southern Pacific or its progeny.")

96. *See* Goldsmith, *supra* note 109, at 805.

97. Edgar v. MITE Corp., 457 U.S. 624, 627 (1982).

98. *Pataki*, 969 F. Supp. at 174.

99. Healy v. The Beer Institute, 491 U.S. 324 (1989).

100. *Id.*

York price.[101] Because that law had the "practical effect" of regulating prices outside New York, it was invalid under the Commerce Clause.[102]

Before geolocation technology, state Internet regulations suffered from the same constitutional defect. A state could not enforce such laws without projecting them onto transactions in all other states; as one circuit court explained, "because there was no effective way to limit access to online materials by geographic location, a Web site owner operating legally in California would have to comply with New York's law to avoid being subject to liability there."[103] In each of these cases, the troublesome practical effects were the necessary extraterritorial results of the statute's application, *not* mere economic choices by private actors that could have complied within the regulating state wholly independent of their transactions in other states.

Geolocation technologies, therefore, appear to remove from state Internet regulations many of the unconstitutional practical effects on out-of-state commerce. However, those state laws still require that *all* providers implement geolocation technologies in the first place—a mandate that itself looks a lot like direct regulation of extraterritorial conduct, because out-of-state providers of Internet services must utilize the geolocation during transactions with out-of-state consumers in order to distinguish them from in-state ones. Whether this initial geolocation requirement is within a state's constitutional authority will likely depend on the way courts conceptualize extraterritoriality doctrine.

On the one hand, no matter how relatively easy or difficult implementing geolocation may be, *any* direct regulation of conduct occurring outside a state's borders seems to violate extraterritoriality principles. As the *Edgar* Court put it, extraterritoriality doctrine "precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State."[104] From this unqualified language, a state law that enacts a nationwide geolocation mandate appears to be unconstitutional irrespective of the relative difficulty of implementing geolocation because such a law necessarily applies to wholly out-of-state transactions.

On the other hand, some commentators doubt that extraterritoriality doctrine is a complete bar to laws with wholly extraterritorial potential applications. For example, in their Yale Law Journal piece, *The Internet and the Dormant Commerce Clause*, Jack L. Goldsmith and Alan O. Sykes argue that the Supreme Court's extraterritoriality jurisprudence should be viewed as a balancing analysis.[105] On this view, state regulations that result in extraterritorial application of laws are valid unless they impose "a significant

101. 476 U.S. 573 (1986).

102. *Id.*

103. PSINet, Inc. v. Chapman, 362 F.3d 227, 239 (4th Cir. 2004) (citing *Pataki*, 969 F. Supp. at 64).

104. Edgar v. MITE Corp., 457 U.S. 624, 642-43 (1982).

105. Goldsmith, *supra* note 109, at 805.

out-of-state burden on communications between noncitizens [that is] not justified by the meager benefits achieved."[106]

Others are persuaded of extraterritoriality doctrine's demise, viewing a string of recent Supreme Court decisions that avoided extraterritoriality principles as the proverbial writing on the wall for extraterritoriality analysis.[107] In particular, Professor Brannon P. Denning has gone so far as to compose a "post-mortem" for extraterritoriality that purports to chronicle "the lifecycle of constitutional doctrine, from birth to death."[108] Citing to Goldsmith and Sykes' work, Denning argues that extraterritoriality is a poorly-defined and ultimately unworkable doctrine—particularly as it relates to state Internet laws.[109] Similarly, another commentator has predicted that "extraterritoriality analysis of Internet matters will have a brief lifetime under the Dormant Commerce Clause," suggesting that "[j]ust as *ALA v. Pataki* coupled a simple analogy to transportation with broad pronouncements of state incompetence to regulate the Internet, so too did the early [Dormant Commerce Clause] telegraph cases. But the Supreme Court eventually retrenched its analogy in the telegraph context to accommodate state regulatory interests."[110]

Nonetheless, even as some courts reject extraterritoriality analysis in the Internet context, others continue to accept the *Pataki* approach. All things considered, extraterritoriality concerns are worth exploring in challenges to state Internet laws, but judicial receptiveness to that argument has been haphazard at best. To maximize chances of success, an extraterritoriality challenge might include two specific arguments.

First, the challenge might explore the ambiguity in the "practical effects" cases by suggesting that regulations are invalid if the cost of tailoring greatly exceeds the cost of compliance. Consider that in *Southern Pacific*, the Supreme Court characterized the *economic infeasibility* of tailoring one's compliance on state-by-state basis as an invalid practical effect of Arizona's law:

> Frequently it is not feasible to operate a newly assembled train from the New Mexico yard nearest to Arizona, with the result that the Arizona limitation governs the flow of traffic as far east as El Paso, Texas. For similar reasons the Arizona law often controls the length of passenger trains all the way from Los

106. *Id.*

107. Brannon P. Denning, *Extraterritoriality and the Dormant Commerce Clause: A Doctrinal Post-Mortem*, 73 LA. L. REV. 979 (2013). For support, Denning offers State Farm Mutual Automobile Insurance Company v. Campbell, 538 U.S. 408 (2003), along with Phillip Morris, U.S.A. v. Williams 549 U.S. 346 (2007). Both cases employed Due Process, rather than extraterritoriality, as the appropriate analysis in cases seemingly ripe for extraterritoriality analysis.

108. *Id.* at 184.

109. *Id.*

110. Gaylord, *supra* note 108, at 1117.

> Angeles to El Paso. If one state may regulate train lengths, so may all the others, and they need not prescribe the same maximum limitation. The practical effect of such regulation is to control train operations beyond the boundaries of the state exacting it because of the necessity of breaking up and reassembling long trains at the nearest terminal points before entering and after leaving the regulating state.[111]

Likewise, it may be economically infeasible for providers to implement differential treatment of web traffic based on geolocation data, and a challenge to a law enacting such a mandate might argue that its practical effect is therefore to control the provider's behavior in all states, rendering the law unconstitutional. At least one federal court has recently adopted this approach in the privacy context. In evaluating a state requirement that businesses disclose when they record customer support calls, the court reasoned that the dispositive issue was "whether [the defendant] could feasibly comply with California law without altering its conduct with regard to non-California clients."[112]

Secondly, an extraterritoriality challenge to a state Internet law might attack the mandate that providers in all states implement geolocation technology for all interactions to identify the users subject to the state's law. Unlike laws that have extraterritorial effects only because of a business' economic decision to comply across the board, a geolocation mandate *does* directly regulate wholly extraterritorial conduct by threatening potential liability for out-of-state providers—even if most interactions in which those providers engage involve out-of-state users. If the court takes a stringent view of extraterritoriality doctrine that regards as invalid *any* direct regulation of transactions wholly outside state borders, geolocation mandates may well be unconstitutional.

Ultimately, given the wide divergence between courts, predictions as to the application of extraterritoriality analysis to a given Internet regulation are largely speculative. It is, therefore, likely that the Dormant Commerce Clause's other facets will supply the more consistently promising grounds for constitutional challenges to state Internet regulations—particularly in the data privacy context.

B. Pike Balancing: Common State Data Privacy Laws Are Unconstitutional Because Their Underwhelming Local Benefits Cannot Justify the Burden of Location-Based User Filtering.

Pike balancing represents a more fertile ground for Dormant Commerce Clause challenges because the doctrine is more settled than extraterritoriality, so potential plaintiffs can get a better idea of a court's likely reaction to such challenges. In evaluating the implications of

111. *Southern Pacific Co.*, 325 U.S. at 775-76.

112. Ades v. Omni Hotels Mgmt. Corp., 46 F. Supp. 3d 999, 1015-16 (C.D. Cal. 2014).

geolocation for *Pike* balancing, the particular state interest asserted becomes especially important; indeed, *Pike* balancing explicitly evaluates that state interest in the first step of the analysis.[113] Accordingly, a generic category of "state Internet regulations" is insufficient to inform the *Pike* inquiry because the state interests at issue may vary dramatically.

This Section will focus on the state interest in protecting general data privacy, particularly with regard to data commonly considered "personally identifiable information," or PII.[114] As yet, there is little jurisprudence regarding the state interest in data privacy under the Dormant Commerce Clause analysis.[115] This Section attempts to provide a framework for evaluating that interest in a *Pike* balancing context.

To begin, consider how other asserted state interests have fared under *Pike*. The first, and easiest, hurdle that a challenged regulation must clear is that the asserted state interest must be a legitimate matter of local concern.[116] In the realm of Internet commerce, federal courts have weighed the states' interests in protecting children from obscenity;[117] in regulating online pharmacies;[118] in controlling the terms of online sales and online loans to resident consumers; [119] and in dictating website audible accessibility standards.[120] Additionally, state courts have addressed the state's interest in restricting online gambling.[121] Each time, the court accepted the asserted interest as a legitimate one without prolonged analysis.

Perhaps the closest courts have come to evaluating the legitimacy of a state's interest in data privacy is a string of cases addressing state regulation

113. *Pike*, 397 U.S. at 145.

114. There is no universally accepted definition of PII, but generally, any information that might reasonably be associated with a specific person or small group of people qualifies as PII.

115. *See, e.g.*, King, *supra* note 117, at 63 ("[T]he law has reacted inadequately to [geolocation] 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."). Moreover, states may have stronger interest in preserving their citizens' data privacy in some areas, such as health information, than in others, like shopping habits.

116. *Pike*, 397 U.S. at 142 ("Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits.").

117. *See, e.g.*, *Pataki*, 969 F. Supp. at 163; Am. Booksellers Found. v. Dean, 342 F.3d 96, 103 (2d Cir. 2003); PSINet, Inc. v. Chapman, 362 F.3d 227, 240 (4th Cir. 2004); Am. Civil Liberties Union v. Johnson, 194 F.3d 1149, 1161 (10th Cir. 1999); Cyberspace Commc'ns, Inc. v. Engler, 55 F. Supp. 2d 737, 751 (E.D. Mich. 1999), *aff'd & remanded*, 238 F.3d 420 (6th Cir. 2000).

118. Knoll Pharm. Co. v. Sherman, 57 F. Supp. 2d 615, 623 (N.D. Ill. 1999).

119. *See, e.g.*, Ford Motor Co. v. Texas Dep't of Transp., 264 F.3d 493, 500 (5th Cir. 2001); Quik Payday, Inc. v. Stork, 549 F.3d 1302, 1305 (10th Cir. 2008).

120. Nat'l Fed'n of the Blind v. Target Corp., 452 F. Supp. 2d 946, 958 (N.D. Cal. 2006).

121. Rousso v. State, 170 Wash. 2d 70, 82, 239 P.3d 1084, 1090 (2010).

of unsolicited commercial emails ("spam").[122] There too, a federal court accepted that "the Act served the 'legitimate local purpose' of banning the cost-shifting inherent in the sending of deceptive spam."[123] Although the concerns addressed by anti-spam laws—like fraud and annoyance—are different from those inherent in data privacy, there also exist conceptual similarities: the desire for anonymity in consumption, the "right to be let alone,"[124] and the ability to exclude unwanted kinds of correspondence.[125]

Taken together, these cases suggest that courts give state legislatures wide latitude in evaluating the legitimacy of asserted interests. In any event, it seems improbable that a state interest in the data privacy is substantially less legitimate than curtailing unsolicited emails or ensuring audible accessibility for websites. Accordingly, for *Pike* balancing purposes, a state's interest in data privacy will likely be a legitimate one.

However, that does not end the judicial evaluation of a state interest under *Pike*. After ascertaining that a state interest is legitimate, courts must then weigh the gravity of that legitimate interest against the burden thereby imposed on interstate commerce.[126] The common theme at this stage in Internet cases, which could factor prominently in a challenge to a state data privacy law, is that the real weight of a state interest appears to depend less on its importance as a societal goal than on its likelihood of being achieved through the challenged regulation.

Thus, in *PSINet, Inc. v. Chapman*[127] and *American Civil Liberties Union v. Johnson*[128] the Fourth and Tenth Circuits struck down statutes criminalizing transmission of obscene-for-minors material to minors. Even if courts permitted states to apply such statutes against out-of-state actors within the United States, the Tenth Circuit reasoned, "[p]ornography from, say, Amsterdam will be no less appealing to a child on the Internet than pornography from [Albuquerque], and residents of Amsterdam have little incentive to comply with [the statute]."[129] Those courts concluded that the regulation would fail significantly to affect the availability of such materials

---

122. *See* Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 535 (D. Md. 2006); State v. Heckel, 143 Wash. 2d 824, 840 (2001); MaryCLE, LLC v. First Choice Internet, Inc., 166 Md. App. 481, 519 (2006). *See also* Free Speech Coal., Inc. v. Shurtleff, 2:05CV949DAK, 2007 WL 922247 (D. Utah 2007). *Shurtleff*, however, is of limited use for data privacy purposes because the statute at issue permitted the court to evaluate the state interest as protecting minors from obscenity, not merely protecting some form of inbox privacy.

123. *Keynetics*, 422 F. Supp. 2d at 534 (quoting *Heckel*, 143 Wash. 2d at 836).

124. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

125. One might consider the protections embodied in the "Do-not-call" registry, at 47 C.F.R. § 64.1200, as expressions of this ability.

126. *Pike*, 397 U.S. at 143-44.

127. *PSINet*, 362 F.3d 227 (4th Cir. 2004).

128. *Johnson*, 194 F.3d 1149 (10th Cir. 1999).

129. *Id.* at 1162 (quoting ACLU v. Reno, 929 F.Supp. 824, 882 (E.D.Pa.1996), *aff'd*, 521 U.S. 844 (1997) (second and third alterations in the original)).

to minors within the regulating state. The state interest in its enforcement was, therefore, *de minimis*.

By contrast, in *Ford Motor Co. v. Texas*,[130] the Fifth Circuit upheld the application of Texas' ban on manufacturer-owned auto dealerships to Ford's online used vehicle market. In that case, the state's interest was "to prevent vertically integrated companies from taking advantage of their incongruous market position."[131] Noting that Ford had previously unloaded its used vehicles through closed auctions to dealers before discontinuing the practice in order to sell them through its own online dealership, the court concluded that "there is certainly evidence from which a reasonable legislator could believe [the statute] would further the State's legitimate interest in preventing manufacturers from utilizing their superior market position to compete against dealers."[132] That is, unlike harmful-to-minors content originating from overseas sources beyond any state's control, Texas is quite capable of enforcing its economic favoritism for cars bought and sold within its own boundaries. Accordingly, despite the initially strange result that statutes enacted for the protection of minors were invalidated, while others supported only by economic protectionism were upheld, the probable efficacy of a state's law in addressing its asserted interest would explain these outcomes.[133]

The implications for data privacy laws are significant. Consider a hypothetical law that would create a presumption of harm if a defendant shares personal information without obtaining the data subject's prior opt-in.[134] The law would allow consumers to bring actions against businesses that transfer such data without consumer consent.[135] While a state may be able to enforce such a law against domestic firms, under current Dormant Commerce Clause jurisprudence, the ubiquitous collection and sale of such information among foreign providers of websites and applications may preclude the state from actually achieving its interest in protecting its citizens' privacy.

---

130. Ford Motor Co. v. Texas Dep't of Transp., 264 F.3d 493 (5th Cir. 2001).

131. *Id.* at 503.

132. *Id.* at 504.

133. *See also* Greater Los Angeles Agency on Deafness, Inc. v. CNN, Inc., 742 F.3d 414 (9th Cir. 2014) (upholding against summary judgment a California statute mandating video closed captioning). Although the analysis is exceedingly brief, the result is informative as an illustration: presumably, California's interest in "providing hearing-impaired citizens equal access to online news videos," *Id.* at 433, is likely to be substantially realized through domestic enforcement alone, given consumers' relatively greater demand for United States news compared to foreign news.

134. *See* Julian D. Perlman, *Opening The Flood Gates? California Voters May Create Presumption Of Harm In Privacy Breach Cases*, MONDAQ (Oct. 2013), http://www.mondaq.com/unitedstates/x/266604/Data+Protection+Privacy/Opening+The+Flood+Gates+California+Voters+May+Create+Presumption+Of+Harm+In+Privacy+Breach+Cases.

135. *Id.*

Against that underwhelming state interest, courts must weigh the burden a challenged law places on interstate commerce.[136] Several commentators suggest that modern geolocation capabilities lower the burden that state laws place on interstate commerce by enabling them to block citizens of states in which they do not wish to do business,[137] although precedent supportive of this proposition remains sparse.[138] Even so, commentators have observed that "server-side geolocation tools cost thousands of dollars per year and client-side tools still involve non-trivial implementation costs as well."[139] Those expenses may dissuade companies from launching new online services.[140]

Alternatively, a court might conceptualize the burden as the actual cost of bringing a website into compliance—even if geolocation makes it technically possible to block a given jurisdiction. Consider that the statutes in *Bibb* and *Southern Pacific Co.* were both invalid even though "the truck driver or train engineer . . . can steer around Illinois or Arizona, or change the mudguard or train configuration at the state line . . . ."[141] On this view, the burden will likely vary depending on the challenged statute. For example, in the case of data breach notification laws, the burden is (among other things) the cost of contacting all affected parties. Similarly, in the case of California's Online Eraser law, the burden consists of devising a mechanism by which minors may completely remove previous posts from public view.

Along with the technological burden of any given state law—however a court conceptualizes it—comes the additional burden of potentially inconsistent regulations from other states.[142] *Pataki* analyzed the law's

136. *Pike*, 397 U.S. at 143.

137. *See, e.g.*, Goldsmith, *supra* note 109, at 808; Michael W. Loudenslager, *Allowing Another Policeman on the Information Superhighway: State Interests and Federalism on the Internet in the Face of the dormant commerce clause*, 17 BYU J. PUB. L. 191, 243 (2003).

138. To date, the only federal court opinions to have directly addressed the burden associated with implementing geolocation technology as it relates to *Pike* balancing are *Target*, 452 F. Supp. 2d at 962; and *CNN*, 742 F.3d at 433. Both courts reasoned that, because major companies sometimes integrate national-level geolocation technology into their websites, geolocation at the state level must not be a burden. It is unclear whether courts would be as dismissive of the burden if presented by a smaller company, nonprofit, or sole proprietor. Additionally, both cases were decided at pre-trial stages obligating the courts to draw inferences in the plaintiffs' favor. For further analysis, see King, *Personal Jurisdiction*, 21 ALB. L.J. SCI. & TECH. at 91. King acknowledges the possibility that, for *Pike* balancing purposes, some geolocation mandates may be unconstitutionally "disruptive or onerous." *Id.* at 115.

139. *Id.* at 110.

140. *Id.* at 96 ("In theory geolocation tools are available to every Internet site. In practice, however, only some sites can realistically afford to employ them.").

141. *Pataki*, 969 F. Supp. at 183 (citing Bibb, 359 U.S. 520; and Southern Pac. Co., 325 U.S. 761).

142. Goldsmith, *supra* note 109, at 806 ("The inconsistent-regulations cases do not concern inconsistencies in the sense that acts required in one state are prohibited in another. Rather, they concern different regulations across states that heighten compliance costs for multijurisdictional firms.").

susceptibility to inconsistent regulatory schemes as a separate mode of Dormant Commerce Clause analysis, but it is probably best viewed as part of the burden on interstate commerce for Pike balancing purposes. [143] Recall that "the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States."[144] In the data privacy sphere, this is a very real concern; for example, some states may require that businesses destroy data that is no longer in use, while others could require them to save the same records for law enforcement purposes.

Thus, there are several key arguments that a challenge to a state privacy law might include with respect to *Pike* balancing. First, the challenge might evaluate the law's prospects for successfully implementing the state's asserted interest, especially considering any unreachable foreign contributions to the putative problem. Second, the challenge might argue that implementing geolocation is itself a substantial burden—many times a prohibitively costly one. Third, the challenge might detail the possibilities for inconsistent regulations, highlighting the frequency with which data changes physical location in the modern economy. Important principles that might inform these analyses include the presence or absence of sales of physical goods within the state[145] and the relative burden to collect information, including whether a provider presently collects location information.[146] The more burdensome a state data privacy regulation, the more vulnerable it will be to the *Pike* test.

V. CONCLUSION

State data privacy laws currently face significant constitutional hurdles. Geolocation technology may alter the Dormant Commerce Clause analysis, but it is unlikely to mitigate the constitutional difficulties in all, or even most, cases. Challenges to modern data privacy laws, therefore, have

143. Gaylord, *supra* note 108, at 1116 ("The court's third mode of analysis, the potential for inconsistent regulation, is not an independent constitutional test. Rather, it represents "double-dipping" in the Commerce Clause pot."); William Lee Biddle, *State Regulation of the Internet: Where Does the Balance of Federalist Power Lie?*, 37 CAL. W. L. REV. 161, 167 (2000) ("As has been noted by other commentators, these first two reasons given by the court actually represent "double dipping" from the same line of Commerce Clause cases.").

144. *Healy*, 491 U.S. at 336-37.

145. *Compare Target*, 452 F. Supp. 2d 946 and *Ford*, 264 F.3d 493 (upholding challenged laws involving sales of physical goods), *with*, *PSINet*, 362 F.3d 227 and *Johnson*, 194 F.3d 1149 (striking challenged laws involving commerce in digital goods).

146. *Target*, 452 F. Supp. 2d at 961 ("Websites can determine the location of a user from information they provide, such as a credit card number . . . ."). *See also* Michael W. Loudenslager, *Allowing Another Policeman on the Information Superhighway: State Interests and Federalism on the Internet in the Face of the Dormant Commerce Clause*, 17 BYU J. PUB. L. 191, 245 (2003) ("Web sites on which users may download software or receive information or services, such as legal advice or other professional services, do not have the same opportunity to verify the location of the site user . . . .").

several lines of attack at their disposal. Among those arguments are extraterritoriality analyses, focusing on the practical economic effects of the law in question as well as its implicit geolocation mandate. Also available are *Pike* balancing arguments, including the likelihood that a law will achieve the asserted state interest, the costs of implementing unwanted geolocation technology, and the potential for inconsistent state regulations. At bottom, data privacy laws affect far more commerce than any obscenity statute or car dealership regulation ever has because privacy laws impact businesses of all shapes and sizes. Thus, the Dormant Commerce Clause likely has a significant role to play in protecting state comity in this important sector.