Regulatory Transparency Project

Unlocking Innovation & Opportunity

Potential Constitutional Conflicts in State and Local Data Privacy Regulations

Cyber and Privacy

Jennifer Huddleston

Ian Adams

This paper was the work of multiple authors. No assumption should be made that any or all of the views expressed are held by any individual author. In addition, the views expressed are those of the authors in their personal capacities and not in their official/professional capacities.

To cite this paper: Jennifer Huddleston and Ian Adams "Potential Constitutional Conflicts in State and Local Data Privacy Regulations", released by the Regulatory Transparency Project of the Federalist Society, December 2, 2019 (https://regproject.org/wp-content/uploads/RTP-Cyber-and-Privacy-Paper-Constitutional-Conflicts-in-Data-Privacy-final.pdf)

3 December 2019

Table of Contents

Introduction

Over the last few years, we have seen a heightened level of focus and debate among policymakers, scholars, and the public over the possible need for--and details and reach of-- a comprehensive data privacy framework in the United States. These debates intensified following the high-profile enactment of the European Union's General Data Protection Regulation (GDPR) alongside growing concerns domestically related to unexpected uses of information, such as the Cambridge Analytica affair. Despite being the subject of intense Congressional consideration, no legislative vehicle has advanced beyond the early stages of consideration. Absent federal legislation, some states have chosen not to wait and instead acted on their own and passed legislation to create bespoke data privacy frameworks.[1]

Before policymakers can have an honest debate about the pros and cons of the particulars of state data privacy legislation, they must first confront the fundamental question of the constitutionality of their actions. These efforts are wasted if their actions are doomed to be struck down in the courts. It is not enough for policymakers to merely desire a particular solution; he or she must also take actions that will pass constitutional muster.

For example, FCC Chairman Dennis Patrick clearly articulated the necessity of public officials analyzing and following the law in his 1987 statement repealing the Internet Fairness Doctrine:

> [T]he record in this proceeding leads one inescapably to conclude that the fairness doctrine chills free speech, is not narrowly tailored to achieve any substantial government interest, and therefore contravenes the First Amendment and the public interest. As a consequence, we can no longer impose fairness doctrine obligations on broadcasters and simultaneously honor our oath of office. By this action, we honor that oath, and, we believe, we promote the public interest.[2]

Concerns about the costs, benefits, and collateral consequences of data privacy laws are relevant in the context of both federal and state legislation, but sub-national (i.e. state or local) data privacy laws face additional concerns and scrutiny because, as has been noted in other policy contexts, the internet requires a uniform system of regulation. The internet's uniquely global nature inherently

[1] *See* Jennifer Huddleston, *Preventing Privacy Policy from Becoming a Series of Unfortunate Events*, American Action Forum, Jan. 14, 2019, https://www.americanactionforum.org/print/?url=https://www.americanactionforum.org/research/preventing-privacy-policy-from-becoming-a-series-of-unfortunate-events/.

[2] In re Syracuse Peace Council, 64 Rad. Reg. 2d (P & F) 1073 (1987) (Statement of Chairman Patrick, quoted in "Fairness held Unfair," Broadcasting, August 10, 1987, at 27.

cannot be dealt with in a fractured manner and, for this very reason, presents constitutional concerns.[3]

State and local data privacy laws run afoul of the constitution in at least three ways: first, the Dormant Commerce Clause, second, the First Amendment, and, third, conflicts with existing federal law. Given these concerns, before following the lead of California, Nevada, and Maine, policymakers should carefully consider not only the likely technological and competitive consequences of a patchwork of laws, but also the possibility that such laws may be deemed unconstitutional — and thereby nullified.

I. The Current State and Potential Impact of State Consumer Privacy Regulation

In August 2018, California passed the California Consumer Privacy Act (CCPA). The Golden State's framework is set to become effective on January 1, 2020 and enforceable on July 1, 2020. Other states, including Nevada and Maine, have likewise passed consumer data privacy laws, and more still are considering such legislation.[4] Many of these bills (and, potentially, executive orders) use California's legislation as a model, but they are far from uniform. Generally, such laws signal a shift from the American approach to data governance—largely permissionless innovation with a post hoc regulatory response to concrete harms—to a European-style approach with the precautionary principle at its center.

While these laws purport to apply only inside each state's borders, they burden an inherently interstate — indeed, global — media, and the direct and indirect costs and effects of state laws and regulations are significant. A recent regulatory impact assessment from the California Department of Justice concluded that the CCPA would cost California firms — to say nothing of firms outside California — $55 billion in compliance costs up front and $16.5 billion over the next 10 years.[5] Notably, the CCPA's costs impact not only companies in the technology sector but a wide range of industries: from retail and entertainment to construction and mining. This would affect up to 570,000 California businesses.[6]

---

[3] Graham Owens, *Federal Preemption, the Dormant Commerce Clause & State Regulation of Broadband: Why State Attempts to Impose Net Neutrality Obligations on Internet Service Providers Will Likely Fail*, Tech Freedom White Paper, Aug. 8, 2018, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3216665.

[4] Mitchell Nordyke, *US State Comprehensive Privacy Law Comparison*, IAPP, Apr. 18, 2019, https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/.

[5] Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, August 2019, http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

[6] *Id.*

While these internal regulatory compliance costs alone may be high, they fail to capture secondary economic losses such as potential lost advertising revenues of up to$60 billion.[7] Nor do they count the costs to non-resident firms that will be impacted by the law's requirements. Given the scope of its covered entities and its definition of who may invoke rights under the law, the CCPA is broad enough to capture many smaller businesses that have a limited number of California IP addresses in their web traffic and/or draw the bulk of their users or data from other states.[8]

Privacy regulation is not cost-free, and regulations in populous and economically significant states such as California may have particularly dramatic effects far beyond their borders. Already, one large technology firm, Microsoft, has signaled its intention to enforce CCPA's requirements nationwide.[9] But even smaller states considering similar laws would effectively subject both resident and non-resident businesses to sizeable compliance costs and lost revenue. In either case, as both large and small states act, businesses will encounter an ever-increasing compliance burden as seemingly minor differences compel the development, deployment and maintenance of state-specific systems to handle conflicting laws.[10] As a result, while some states may be more likely to give rise to compliance challenges, constitutional concerns and risks of a potential patchwork exist regardless of the size and economic power of the state.

The impact of greater compliance burdens, from one state or many, would be two-fold and informed directly by recent experiences with GDPR's enactment. First, significantly higher compliance costs will make firms hesitate to invest in smaller companies less equipped to handle compliance and to avoid enforcement actions, even one of which could be fatal to a firm, given the public relations sensitivity of "privacy."[11] Second, market leaders such as Google and Facebook would be better protected from new competition as they are more capable of building out compliance infrastructure to address regulatory challenges, while newer and smaller players may struggle with increased barriers to entry from such requirements.[12]

Conversely, the potential benefits of these laws are not readily calculable as an empirical matter and are, as a result, more difficult to discern. This is not to say that there are no benefits to consumer privacy legislation, but the value of such benefits is far more dependent on personal preferences. For

---

[7] Roslyn Layton, *The Costs of California's Online Privacy Rules Far Exceed the Benefits*, AEI Ideas, March 22, 2019, https://www.aei.org/technology-and-innovation/the-costs-of-californias-online-privacy-rules-far-exceed-the-benefits/.

[8] Daniel Castro & Alan McQuinn, Comments regarding The California Consumer Privacy Act, Assembly Bill 375, Rulemaking Process, Mar. 8, 2019, http://www2.itif.org/2019-comments-ccpa.pdf.

[9] Brill, Julie. "Microsoft will honor California's new privacy rights throughout the United States." Nov. 11, 2019. https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/

[10] Jennifer Huddleston, *The Problem of Patchwork Privacy*, Aug. 23, 2018, https://www.mercatus.org/bridge/commentary/problem-patchwork-privacy.

[11] *See* Jian Jia et al., *The Short Run Effects of GDPR on Technology Venture Investment*, Jan. 7, 2019, https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment.

[12] *See* Bjorn Grelf, *Study: Google is the Biggest Beneficiary of the GDPR*, Cliqz, Oct. 10, 2018, https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.

example, various analyses have noted potential unintended consequences of overly precautionary privacy laws as well as the comparably low benefits based on consumers' willingness to pay.[13]

These negative effects are compounded by the uncertainty created for covered entities, possible inconsistencies in enforcement between states,[14]and overly broad definitions of germane terms (particularly "personal information") Even slight inconsistencies among states are likely to frustrate consumer expectations,[15] as well as the companies subject to them, by introducing confusion about what rights exist and what rules apply when trying to comply.[16]

Ultimately, while these proposals may be well-intentioned attempts by state lawmakers to provide a solution in the absence of federal action, sub-national data privacy laws have the potential to create a disruptive mesh of inconsistent, but always applicable, standards that splinter the internet and raise costs.[17]

II. State and local data privacy regulation may violate the Dormant Commerce Clause

The internet knows no borders, and society is better for it. A patchwork of state privacy laws could put up barriers to the conduct of commerce and, in the process, the free flow of digital information as firms attempt to insulate themselves from exposure to particular regulatory regimes. Even if such laws initially appear consistent with one another, they will still likely fail the constitutional test of the Dormant Commerce Clause.

The Dormant Commerce Clause is a doctrine that the U.S. Supreme Court inferred from Article I of the Constitution, holding that state and local laws may not unduly burden commerce between the states, and thereby preventing states from regulating beyond their borders. The extent of this prohibition is a subject of constant debate, but, as articulated in the Court's existing precedent, it encompasses both intentional impacts and incidental cross-jurisdictional impacts, provided the burden on commerce is clearly excessive compared to the claimed local benefits.[18]

---

[13] *See* Layton, *supra* note 7.

[14] *E.g.*, Alec Stapp, *10 Reasons Why the California Consumer Privacy Act (CCPA) is Going to Be a Dumpster Fire*, Truth on the Market, Jul. 10, 2019 https://truthonthemarket.com/2019/07/01/10-reasons-why-the-california-consumer-privacy-act-ccpa-is-going-to-be-a-dumpster-fire/.

[15] *See, e.g.*, Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)*, Santa Clara Univ. Legal Studies Research Paper, Jun. 14, 2019, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013; Jennifer Huddleston, *Preserving Permissionless Innovation in Federal Data Privacy Policy*, 22(12) J. OF INTERNET L. 1 (2019).

[16] *See, e.g.*, Cathy McMoris Rodgers, *4 Warnings About What a Patchwork of State Privacy Laws Could Mean for You*, Morning Consult, May 3, 2019, https://morningconsult.com/opinions/4-warnings-about-what-a-patchwork-of-state-privacy-laws-could-mean-for-you/.

[17] *See, e.g.*, Huddleston, *supra* note 10.

[18] Pike v. Bruce Church, 397 U.S. 137 (1970).

A typical Dormant Commerce Clause analysis in the context of data transmission involves two steps:

1. Does the law in question explicitly discriminate against out-of-state actors? For example, does a consumer privacy law treat data obtained or processed by in-state companies differently than that from out-of-state companies? Such behavior would result in the law being per se invalid under the Dormant Commerce Clause. Even if a law does not facially preference in-state companies, it may still have a discriminatory impact on out-of-state parties.

2. Do the in-state benefits of the law outweigh the burden on the out-of-state parties? This balancing test prevents a single state from imposing excessive costs beyond its borders while still recognizing that incidental impacts may occur in some cases.

Regulation of the internet is inherently cross-jurisdictional. The 2015 Open Internet Order, promulgated by the Federal Communications Commission, for example, declared that the internet is inherently an interstate service.[19] Such reasoning is straight-forward: data transmissions do not obey borders and a single online action can involve multiple states even if it involves only a single individual. On this basis, state laws purporting to regulate the internet should — as a matter of course — trigger Dormant Commerce Clause scrutiny.

Precedent concerning state laws intended to regulate the transmission of information online resulted in courts finding that such regulations violate the Dormant Commerce Clause due to their extraterritorial impact and inability to distinguish between intrastate and interstate activities online. For example, in the 1959 case *Bibb v. Navajo Freight Lines*, the Supreme Court struck down an Illinois law that required the use of a particular type of mudguard on freight trucks driven through the state.[20] The Court found that a law which would require truckers to stop and change their guards at a state's border was an unconstitutional burden on interstate commerce even if facially nondiscriminatory against out-of-state transporters.[21]

When it comes to the internet, the extraterritorial nature of interactions makes such analysis and concerns even more relevant. If it is an unconstitutionally large burden to demand truckers to change mudguards at a state's border, levying requirements on online activities to be similarly tailored, given the quantity of content and number of interactions, must be met with extreme scrutiny. Thus, understandably, lower courts have previously recognized this in the online context.

For example, in *American Library Association v. Pataki*, the federal district court for the Southern District of New York found a New York state law that prevented the dissemination of certain material to minors violated the Dormant Commerce Clause, noting that such regulation of online

---

[19] *See* Protecting and Promoting the Open Internet, WC Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5803 ¶ 431 (2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

[20] 359 U.S. 520 (1959).

[21] *Id.* at 524.

content could subject those who operate entirely outside the state to state law.[22] The court also noted that the internet was an area for federal action in which inconsistent state regulation risked walling off the potential benefits of innovation.[23] That decision is no outlier. Throughout the early 2000s, three different federal circuit courts and two additional federal district courts similarly ruled that state online dissemination laws unduly affected interstate commerce and were unconstitutional.[24] The impact of comprehensive data privacy regulations at a state and local level is even larger than the dissemination laws and the potential benefits of such laws are even more difficult to determine. And, even with advances in technology, these concerns and impacts still exist.

State data privacy laws akin to the CCPA in scope would similarly disrupt cross-border data exchanges, particularly commercial exchanges, when enacted by populous states. Consider that a business becomes subject to the heavy compliance requirements of the CCPA merely by having a single California resident amongst its users once it exceeds the law's minimum threshold requirement(s) — even if the firm does not conduct business in California.[25] Such burdens will not be felt only by technology companies but also by a wide array of industries both online and offline that often utilize personal data. On that basis, courts will have to balance the extent of the burden faced by plaintiffs with the benefit to the state associated with the requirement.

Even if all 50 states independently established the same standards, those subject to such laws might still struggle with different standards of enforcement, creating uncertainty for offering similar products across state borders.[26] Thus, as AEI's Daniel Lyons has argued regarding potential state level Net Neutrality laws:

> [E]ven if the court construes these restrictions to apply only to contracts with in-state consumers, such regulations can disrupt the orderly flow of interstate traffic. Permissible network management practices would differ from state to state, depending on whether and how each state chose to regulate. Even if all states adopted facially identical statutes, fragmentation is likely to occur over time as fifty different sovereigns may reasonably disagree on enforcement.[27]

More likely, even slight differences in state level privacy laws will create Dormant Commerce Clause-triggering undue burdens as out-of-state companies confront the choice to either comply

---

[22] 969 F. Supp. 160 (S.D.N.Y. 1997),

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

[24] Chin Pann, *The Dormant Commerce Clause and State Regulation of the Internet: Are Laws Protecting Minors from Sexual Predators Constitutionally Different Than those Protecting Minors from Sexually Explicit Material?*, 8 DUKE L. & TECH REV. (2005) at *9-11, *available at* https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1128&context=dltr.

[25] Goldman, *supra* note 15.

[26] *See* Daniel A. Lyons, *State Net Neutrality*, Boston College Law School Research Paper 514, Oct. 11, 2019, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3468816 (discussing such in the context of State Net Neutrality laws).

[27] *Id.*

with the most stringent state laws or create individual and less efficient products for each state or local regulation.[28]

III. State and local data privacy regulation may put unnecessary restrictions on First Amendment rights

The American approach to privacy has been fundamentally different from Europe's because, more than anything else, of the First Amendment guarantees in the U.S. Constitution. Data privacy laws restrict the flow of information and thus must carefully balance First Amendment Rights.

Traditionally, U.S. courts have required that the government adhere to heightened requirements when limiting speech. In this way, the government may place restrictions of speech relating to its time, manner, and place so long as it is narrowly tailored, content neutral, and provides alternative channels for the speaker's message.[29] Laws that are not content neutral, or are expressly content based, are presumed to be unconstitutional and are subject to strict scrutiny.[30] As a result, such laws have only been upheld when a compelling government interest exists, such as in the case of child pornography or in the face of a true threat.[31]

Data privacy laws may not, on their face, appear to be content-based but, as Prof. Euguene Volokh has argued, the establishment of laws regulating data privacy inevitably also implicates the information available within that data, as well as the ability to share it.[32] When viewed through the prism of the First Amendment jurisprudence, limiting the availability and alienability of specific types of information inevitably risks the government silencing speakers, and thereby burdening the First Amendment rights of both users and providers.[33]

For example, whether enacted by a state or the federal government, a European style "right to be forgotten" would face constitutional scrutiny in the United States under the First Amendment for its potential impact on a free press and its limitations and removal of the otherwise legitimate speech of others.[34] Such restrictions would affect not only individual speech but could also impact free press activity. As the Center for International Media Assistance points out, a right to be forgotten not only potentially endangers and limits the ability to gather useful public information, it could also be used

---

[28] *Id.*
[29] Ward v. Rock Against Racism, 491 U.S. 781 (1989).
[30] David L. Hudson Jr., *Content Based*, The First Amendment Encyclopedia, https://www.mtsu.edu/first-amendment/article/935/content-based.
[31] *Id.*
[32] Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You, 52 Stanford Law Review 1088–89 (2000).
[33] *Id.*
[34] *See* Craig Timberg & Sarah Halzack, *Right to Be Forgotten vs. Free Speech*, WASH. POST, MAY 14, 2014, https://www.washingtonpost.com/business/technology/right-to-be-forgotten-vs-free-speech/2014/05/14/53c9154c-db9d-11e3-bda1-9b46b2066796_story.html; Michael J. Ohia, *Information Not Found: The "Right to Be Forgotten" as an Emerging Threat to Media Freedom in the Digital Age*, Jan. 9, 2018, https://www.cima.ned.org/publication/right-to-be-forgotten-threat-press-freedom-digital-age/.

to increase government censorship of both media sources and individuals.[35] For that reason, some have expressed concerns about how officials could use such a right to remove information from the public record or otherwise engage in content policing.[36]

Other restrictions found in the GDPR or CCPA could still be found unconstitutional, given the heavy preference for speech rights throughout First Amendment jurisprudence and such laws potential restrictions or distinctions based on the type or purpose of the data. While there are some cases where speech restrictions are necessary, these restrictions tend to be extremely limited.[37]

Broad privacy legislation, which may encumber legitimate speech, is unlikely to satisfy the requirements necessary to restrict categories of speech.[38] In general, restrictions on speech are closely associated with established categories of harm, such as incitement to violence and obscenity, or content-neutral restrictions such as time, place, and manner. What's more, merely stating that a law should not inhibit a free press or otherwise impact speech is unlikely to be sufficient to overcome the potential impact or chilling effect on the sharing of information.[39]

The courts have struck down previous laws as unconstitutional when privacy laws enable content-based discrimination in the sharing of information.[40] In *Sorrell*, the courts struck down a Vermont law that limited the sale or disclosure of a doctor's prescription records. As Prof. Jeff Kosseff points out in his analysis of problems with the CCPA, the law's distinction between "sale" and mere analytics or processing could be viewed as a similar content-based distinction.[41]

While broad-based privacy laws have not been addressed by the courts, other restrictions on online speech have, likewise, been met with skepticism as courts have opted to emphasize the importance of the medium as a tool for open access and mass democratization. In fact, this vision of the special attributes of free and open internet unrestrained by geographic boundaries or government interference has been, in part, what allowed the internet to flourish and innovate free from censorship.[42]

---

[35] *See* Ohia, *supra* note 34.
[36] *Id*.
[37] *Bantam Books v. Sullivan*, 372 U.S. 58, 70 (1963)
[38] Christopher Koopman et al., *Informational Injury in FTC Privacy and Data Security Cases*, at 6, https://www.mercatus.org/system/files/koopman-informational-injury-mercatus-pic-v1_1.pdf.
[39] *See* Alexandra Scott, *California Legislature Passes Amendments to Expansive Consumer Privacy Law*, Inside Privacy, Sept. 4, 2018, https://www.insideprivacy.com/united-states/state-legislatures/california-legislature-passes-amendments-to-expansive-consumer-privacy-law/.
[40] Sorrell v. IMS Health, 564 U.S. 552 (2011).
[41] Jeff Kosseff, *Ten Reasons Why California's New Data Protection Law is Unworkable, Burdensome, and Possibly Unconstitutional (Guest Blog Post)*, Technology & Marketing Law Blog, Jul. 9, 2018, https://blog.ericgoldman.org/archives/2018/07/ten-reasons-why-californias-new-data-protection-law-is-unworkable-burdensome-and-possibly-unconstitutional-guest-blog-post.htm
[42] *See* Chuck Cosson, *Tool Without a Handle: Reflections on 20 Years from Reno v. ACLU*, Center for Internet and Society, https://cyberlaw.stanford.edu/blog/2017/06/%E2%80%9Ctool-without-handle-reflections-20-years-reno-v-aclu%E2%80%9D.

With these precedents in mind, policymakers at all levels must carefully consider the potential First Amendment impact of such laws lest they be found an unconstitutional restriction on speech.

IV. Portions of state data privacy laws may be preempted because of the supremacy of existing federal laws

Despite persistent rumors to the contrary, the United States is not lacking in data privacy law. In fact, federal laws already exist for many areas of sensitive data, including financial information, healthcare information, and children's privacy.[43] Likewise, states have sector-specific privacy laws of their own in areas like insurance. So far, states have sought to clarify that those already subject to these federal regulations are not subject to new state laws or the federal legislation.

However, when broader state-level data protection mandates present conflicts of laws, there is a possibility that preemption analysis will result in the primacy of federal law under the Supremacy Clause. While many federal privacy laws serve as a floor rather than a ceiling, this existing framework could create legal issues if new comprehensive data privacy laws create contradictions with existing federal requirements. In practice, "comprehensive" state privacy laws are unlikely to ever be truly comprehensive.

For instance, if such laws fail to carve out already regulated industries, there could be clear conflicts regarding proper legal requirements and handling for such data. In other cases, state laws may merely create additional compliance burdens for these regulated industries that create confusion for both consumers and industry. In still other instances, state laws could conflict with existing federal requirements and the supremacy of federal law may render at least those portions of the laws preempted.

Some state privacy laws, such as the CCPA, recognize this apparent conflict and explicitly disclaim any intent to cover data uses already covered by existing federal and state regulations, such as Graham-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA). In theory, this should avoid conflicts that prevent compliance with both state and federal regulations. However, ambiguous drafting about covered entities, covered information, or the applicability of new state laws to such already regulated industries could create confusion about compliance and problems for already regulated industries, particularly when the impact on existing regulated industries is not carefully considered. This is particularly true if state laws fail to consider possible contradictions with existing requirements under federal regulations (and existing state laws) that could make compliance with both laws impossible.

[43] *See* Alan McQuinn, *Understanding Data Privacy*, REAL CLEAR POLICY, Oct. 25, 2018, https://www.realclearpolicy.com/articles/2018/10/25/understanding_data_privacy_110877.html.

While it is less likely to be successful, a case could be made that existing findings about the trans-jurisdictional ("interstate") nature of the internet already bar or limit state action.[44] Unfortunately, given the recent ruling regarding the preemption of state Net Neutrality laws, such an argument is less likely to be successful without a federal law or a formal grant of authority by Congress to a federal agency.[45] But note that, in its decision regarding state Net Neutrality laws, the D.C. Circuit Court did not eliminate the possibility of federal preemption of sub-national net neutrality laws; instead, the court held that the FCC's preemption was too sweeping and effectively invited the FCC to try again on the basis that preemption of such sub-national regulation could still occur on a statute-by-statute basis.[46]

Even without express preemption, a new federal data privacy could preempt existing state data privacy laws that conflict with the federal law. Yet even in the absence of such a policy, there are potential conflicts with existing regulations that would preempt at least certain state actions on data privacy.

Conclusion

While the debate about the potential benefits of additional regulation of data continues, the state and local legislation enacted thus far raise clear constitutional concerns. The most straight-forward way to overcome many of these constitutional issues is for a federal privacy framework with preemptive effect to be enacted. Preemption in and of itself will not address the policy concerns surrounding data privacy in the United States, but it will overcome concerns about states regulating beyond their borders and the supremacy of federal law. Given the borderless nature of the internet and the tradeoffs involved in the debate around data privacy, such policy and the debate surrounding the issue is properly had at the federal level.

In the absence of such a framework, not only will state laws fray the internet via a regulatory patchwork, but they will do so at the risk of creating tremendous legal uncertainty in the face of well-founded constitutional challenges. On that basis, policymakers must exercise extreme caution when considering bespoke data privacy standards for their states and consider the potential constitutional issues as well as their desired policy outcomes.

---

[44] *See* Brent Skorup, *Doomed to Fail: "Net Neutrality" State Laws*, Tech Liberation Front, Feb. 20, 2018, https://techliberation.com/2018/02/20/doomed-to-fail-net-neutrality-state-laws/ (discussing a similar scenario regarding net neutrality).

[45] *See* Dell Cameron, *FCC Improperly Blocked States from Passing Net Neutrality Laws, Appeals Court Rules*, Gizmodo, Oct. 1, 2019. https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html

[46] Mozilla v. FCC, No. 18-1051, slip op. at *121-145 (D.C. Cir. Oct. 1, 2019).