A PRIVACY LAW INVASION FROM THE WEST COAST OR NOTHING TO WORRY ABOUT? THE IMPACT OF THE CALIFORNIA CONSUMER PRIVACY ACT IN NORTH DAKOTA

JEREMY STRAUB* & JOSEPH VACEK*

ABSTRACT

The long-arm provisions of the California Consumer Privacy Act ("CCPA") impose restrictions on North Dakota businesses. Businesses can be ensnared by the CCPA even though they don't operate in California or ship goods to the state. While the CCPA is just one state's privacy law, it has significant reach because of its protection of California residents as opposed to governing only activities in California. This article discusses the impact of the CCPA on North Dakota businesses, constitutional problems with the law, and how North Dakota businesses can comply with it.

---

*† Jeremy Straub is an assistant professor at the North Dakota State University and a Challey Institute Faculty Fellow. His research spans the gauntlet from technology law and policy to the development of technical solutions and their commercialization. Straub's prior legal research has focused primarily on aerospace, technology, warfare and privacy law. His work on technology policy has included considerations of rules of technology engagement in war and policing and technological influence warfare. He has published over 50 articles in academic journals and hundreds of conference papers. He is also the first named inventor on two U.S. patents. Recently, Straub has been focusing on issues of privacy related to technology usage and more generally.

*† Joseph J. Vacek, J.D. is an associate professor at UND Aerospace and holds a courtesy appointment at the School of Law. Vacek's primary research relates to UAS (drones) in the field of aviation law. In researching the impact of the CCPA on UAS operations, the broader questions raised by the application of the CCPA in North Dakota became the basis for this article.

I. INTRODUCTION

On September 17, 1787, delegates from the original twelve state signatories to the United States Constitution met to "establish Justice, insure domestic tranquility, provide for the common defence, promote the general welfare, and secure the blessings of liberty."[1] It is unlikely that these delegates could have predicted what the United States could or would become. When they wrote "the Citizens of each State shall be entitled to all Privileges and Immunities of Citizens in the several States,"[2] it seems unlikely that they could have imagined a scenario where an individual was located in one state and committed a crime or civil offense under the laws of another state. How then, could they imagine that by stating "full faith and credit shall be given in each state to the public acts, records, and judicial proceedings of every

1. U.S. CONST. pmbl.
2. U.S. CONST. art. IV, § 2.

other state,"[3] they would be laying the foundation for someone to be tried or sued in one state for acts that were undertaken in another state?

Now, more than 230 years later, North Dakotans and North Dakota businesses face what some might term an invasion. But there are no planes or tanks–nor even the horse-mounted infantry of 1787– just lawyers. The passage of the California Consumer Privacy Act ("CCPA") and its long-arm provisions, which aim to protect the privacy of Californians–and only Californians–everywhere, places a new burden on North Dakota businesses. Businesses now find themselves regulated from the West Coast by legislators that the business's owners and workers had no role in electing and who are not answerable to them in any meaningful way. While it seems unlikely that the Founding Fathers–who themselves had just renounced the rule of a distant king[4]–intended to create such a scenario, it has arisen.

In 2018, when the CCPA was enacted,[5] North Dakota already had basic privacy protections in place.[6] In 2019, several other states enacted various privacy protection statutes designed to curtail the ability of business entities to gather consumer data, provide greater protection and control to consumers about their data, or both.[7] In 2019, North Dakota expanded its privacy protections to include specific protections for payment card information.[8]

This article focuses on the CCPA and ignores other states' similar laws.[9] North Dakota's data protection statute merits its own discussion which the authors address in-depth in a separate article.[10] This article discusses the CCPA and its implications for North Dakotans and North Dakota businesses. It explains why the CCPA may have no effect in North Dakota (or anywhere, for that matter), how the precise implications of the CCPA cannot presently be determined, and full interpretation must await its review by the courts. The implications of the CCPA, assuming its application as written, for the unmanned aerial vehicle ("UAV"), energy, and agriculture sectors are reviewed, and recommendations for North Dakota businesses are presented.

---

3. *Id*. art. IV, § 1.

4. THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776) ("The history of the present King of Great Britain is a history of repeated injuries and usurpations, all having in direct object the establishment of an absolute Tyranny over these States.").

5. CAL. CODE REGS. tit. 1.81.5, §1798 (2018).

6. N.D. CENT. CODE § 12.1-23-11 (2019).

7. *2019 Consumer Data Privacy Legislation*, NAT'L CONF. ST. LEGIS. (Jan. 3, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

8. S.B. 2262, 66th Legis. Assemb., Reg. Sess. (N.D. 2019).

9. For more details about privacy laws in other states passed in 2018, *see 2019 Consumer Data Privacy Legislation*, NAT'L CONF. ST. LEGIS. (Jan. 3, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

10. Jeremy Straub & Joseph Vacek, *Can I Get Your Name Please? Not Unless You Want to go to Jail*, 95 N.D. L. REV. 569 (2020).

II. PRIVACY LAWS AND BROAD REACH

The notion of privacy in the law traces a long history and is again at the forefront in the context of data privacy and protection.[11] While the word "privacy" itself is not in the United States Constitution, nor in the original version of the North Dakota Constitution,[12] the United States Supreme Court has held in numerous cases that there is an implicit right to privacy in several of the Amendments.[13] Additionally, several federal statutes directly related to protecting privacy exist.[14] In North Dakota, the Century Code specifically addresses several privacy related areas, including privacy of medical records,[15] privacy of the physical person,[16] and privacy in communication.[17] While federal law and U.S. Supreme Court precedent applies in all jurisdictions, privacy laws otherwise can be a confusing patchwork of potentially conflicting requirements, even more confusing when sufficient minimum contacts exist, or might exist, with other states to trigger long-arm jurisdiction.

III. LONG-ARM LAWS AND THEIR SCOPE

Long-arm laws are a recurring source of controversy[18] and the growth of the internet has further complicated their application with unanticipated contacts and technically driven considerations.[19] Long-arm jurisdiction found its start in the U.S. Supreme Court's *International Shoe Company v. Washington* decision.[20] Prior to the *International Shoe* decision, states were required by *Pennoyer v. Neff* to gain personal jurisdiction via in-state service.[21] Despite

---

11. For the development of the legal concept of a right to privacy, *see generally* Dorothy J. Glancy, *Invention of the Right to Privacy*, 21 ARIZ. LAW REV. 1 (1979); Samuel D. Warren & Louis D. Brandeis, *Right to Privacy*, 4 HARV. L. REV. 193 (1890).

12. It is not relevant to the scope of this article that "privacy" does appear in N.D. CONST. art. 1, §25(1)(f) (the context of victim's rights or "Marsy's Law").

13. For a discussion of the implicit right of privacy drawn from Constitutional Amendments, *see generally* William M. Beaney, *The Constitutional Right to Privacy in the Supreme Court*, 1962 SUP. CT. REV. 212 (1962); William M. Beaney, *The Right to Privacy and American Law*, 31 L. CONTEMP. PROBS. 253 (1966); Jamal Greene, *The So-Called Right to Privacy*, 43 U.C. DAVIS L. REV. 715 (2009).

14. *E.g.,* Privacy Act of 1974, 5 U.S.C. § 552a (2018); for a list of over 20 federal privacy laws *see Existing Federal Privacy Laws*, CTR. DEMOCRACY & TECH. (Nov. 30, 2008), https://cdt.org/insights/existing-federal-privacy-laws.

15. N.D. CENT. Code § 65-05-32 (2019).

16. N.D. CENT. Code § 12.1-15-06 (2019) (protecting individuals' privacy by banning anyone, such as an employer, parent or agency, from requiring "that an individual have inserted into that individual's body a microchip containing a radio frequency identification device").

17. *Id.* § 12.1-15-02(1).

18. See, e.g., Robert C. Casad, *Long Arm and Convenient Forum*, 20 U. KAN. L. REV. 1 (1971).

19. For a discussion of the issues that the internet has created relative to long arm laws, see generally J. Christopher Gooch, *The Internet, Personal Jurisdiction, and the Federal Long-Arm Statute: Rethinking the Concept of Jurisdiction*, 15 ARIZ. J. INT'L & COMP. L. 635 (1998).

20. Douglas D. McFarland, *Dictum Run Wild: How Long-Arm Statutes Extended to the Limits of Due Process*, 84 B.U. L. REV. 491, 492 (2004).

21. *Id.*

this requirement, a number of ways around it were developed through the creation of "various fictions" to facilitate in-state service of out-of-state entities and individuals.[22] This practice grew between P*ennoyer* and *International Shoe*.[23] *International Shoe* explicitly allowed states to implement long-arm laws, removing the need for these fictitious means of service.[24] In order to have long-arm jurisdiction, states were required to create a long-arm law and respect due process limitations from the Constitution.[25] In 1962, the National Conference of Commissioners on Uniform State Laws created the Uniform Interstate and International Procedure Act as a model for standardizing long-arm statutes across states.[26] An alternate model to the proposed conference language emerged when Rhode Island and California simply extended all of their laws to the boundary of due process.[27] Today, all states have long-arm statutes which either enumerate long-arm provisions or extend all laws to due process limits.[28]

Multiple considerations exist relative to the applicability of long-arm statutes. Watt and Smith, for example, note that a business anywhere in the world that registers to conduct business in Georgia is bound by Georgian "general personal jurisdiction" and can be sued in Georgia over any matter, even if there is no other connection to Georgia whatsoever.[29] Ullian identifies another problem as states revise their long-arm statutes to accommodate new technically-driven considerations, which is whether the laws are retroactive.[30]

With the introduction of the internet, along with crimes and causes of civil action that may extend across numerous–and perhaps all–states, extreme circumstances can apply. The Equifax breach, for example, had approximately 150 million victims,[31] which included victims in all fifty states.[32] In a

---

22. *Id*.

23. *Id*.

24. *Id*. at 492-93.

25. *Id*. at 493.

26. *Id*. at 495.

27. *Id*. at 496 (under the model implemented by California, Rhode Island and others, no specific statutory restrictions on the long-arm laws were developed; instead, jurisdiction is limited only by courts interpretation of Constitutional 'due process' considerations).

28. *Id*.

29. Brian P. Watt & W. Alex Smith, *"At Home" In Georgia: The Hidden Danger of Registering to do Business*, 35 GA. ST. U. L. REV. 1, 5-6 (2019).

30. Dane Reed Ullian, *Retroactive Application of State Long-Arm Statutes*, 65 FLA. L. REV. 1653, 1654-55 (2013) (identifying the issue of whether a long-arm statute must be in place at the time of the act that gives prospective rise to the jurisdiction, when an act which becomes a cause of action occurs, when process service occurs, or if/when personal jurisdiction is challenged).

31. Steve Ragan, *Equifax Says Website Vulnerability Exposed 143 Million US Consumers*, CSO MAG. (Sept. 7, 2017, 2:29 PM), https://www.csoonline.com/article/3223229/equifax-says-website-vulnerability-exposed-143-million-us-consumers.html.

32. *Equifax Breach Victims, by State*, WALL STREET J., https://graphics.wsj.com/table/EQUIFAX (last visited Sep 28, 2020).

circumstance such as this, a perpetrator could conceivably be subject to prosecution in at least fifty-one jurisdictions, all fifty states and federal, just within the United States, and a firm such as Equifax could potentially be subject to lawsuits in this multitude of jurisdictions, as well.[33] This issue has been considered by legal scholars, who have proposed several possible approaches to resolving it. Jimenez and Lodder have suggested a high seas model to characterize this issue.[34] Boldon highlights several recent cases that show the treatment of internet matters by courts continues to evolve.[35] Cleary identifies the fundamental issue in long-arm jurisprudence: it pits "undue hardships on nonresident defendants" against "frustration and inconvenience visited upon plaintiffs" if they cannot sue in a given venue.[36]

For purposes of this article, it is assumed that if a business sells a product or service to a resident of California located in California, the transaction would clearly be subject to California jurisdiction under both the *International Shoe* standard and the California Civil Code.[37] However, businesses that do not engage in direct commerce with Californians or California businesses and simply supply information via their website or participate in other minimal and not inherently commercial transactions become an area of contention. The text of the CCPA prospectively ensnares these businesses, but they may not meet the sufficient minimum contact standards used elsewhere.

IV. THE CALIFORNIA CONSUMER PRIVACY ACT

The CCPA[38] went into effect on January 1, 2020,[39] and enforcement actions were prohibited until July 1, 2020.[40] The law provides protection to personal and consumer household data. A business[41] that operates in

33. Jeremy Straub, *The Inadequacy of Domestic and International Law for Cyberspace Regulation*, 26 INT'L J. COMPUT. THEIR APPLICATIONS 164, 165 (2019).

34. William Guillermo Jiménez & Arno R. Lodder, *Analyzing Approaches to Internet Jurisdiction Based on a Model of Harbors and the High Seas*, 29 INT'L REV. L., COMPUT. & TECH. 266, 266–282 (2015). Under a 'high seas' model, the 'port' of origin, 'port' of destination, both ports or 'the seas traveled' serve as potential forums with jurisdiction over a matter. *Id.* at 271.

35. R. Michelle Boldon, *Long-Arm Statutes and Internet Jurisdiction*, 67 BUS. LAW. 313, 313–320 (2011).

36. Edward W. Cleary, *The Length of the Long Arm*, 9 J. PUB. L. 293, 302 (1960).

37. CAL. CIV. CODE § 1798.40(c) (West 2020).

38. *Id.* § 1798.

39. Lothar Determann, *New California Law against Data Sharing*, 35 COMPUTER & INTERNET LAW. October 2018, at 1.

40. Ronald Camhi, *What Is the California Consumer Privacy Act?*, RISK MGMT. (Oct. 1, 2018), http://www.rmmagazine.com/2018/10/01/what-is-the-california-consumer-privacy-act/.

41. For the purposes of the CCPA, a business is defined as a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information" thus including persons operating sole proprietorships and members of partnerships within its definition. CAL CIV. CODE § 1798.140(c)(1) (West 2020). Note that for the purposes of the

California[42] and meets any one of three threshold levels is covered by the CCPA. The CCPA applies to businesses that generate more than $25 million in revenue, who annually collect data on more than 50 thousand individuals from (or who may be from) California,[43] or who derive more than half its revenue from selling personal data.[44] The law excludes transactions in which "every aspect of [the] commercial conduct" occurs outside of California;[45] however, even minor connections, such as data storage or processing, may cause transactions to be covered by the CCPA.[46] The law has similarities with the European General Data Protection Regulations ("GDPR"),[47] but the two are not identical.[48]

CCPA, a parent or subsidiary of an organization meeting these criteria is also considered to fall under the jurisdiction of the CCPA. *Id*. § 1798.140(c)(2).

42. The CCPA does not define what "does business in the State of California" means or what level of contact or transaction is required, despite this definition being critical to the interpretation of whether an entity is a "business" as defined by California Civil Code section 1798.140(c)(1); CAL. REV. & TAX. CODE § 23101(b) (2012) applies minimum thresholds for an entity to be considered to do business in California, for franchise tax purposes; however, there is no indication that this standard would apply to the CCPA, despite this being an effective way to establish a level of minimum contract required for CCPA application; Jean Murray, *What Does "Doing Business" Mean?*, BALANCE SMALL BUS. (Dec. 7, 2019), https://www.thebalancesmb.com/what-does-doing-business-mean-398226 (suggesting under section 23101(a) any firm that is "actively engaging in any transaction for the purpose of financial or pecuniary gain or profit" in relation to California may be ensnared).

43. *See* CAL CIV. CODE § 1798.140(c)(1)(B) (West 2020) (covering those that "[a]lone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices"). Given this, an individual may end up counting against this limit more than once, particularly if a business has no mechanism to associate user activity across multiple devices.

44. *Id*. § 1798.140(c)(1)(C).

45. *Id*. § 1798.145(a)(6).

46. *Id*. (excluding transactions that "[c]ollect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California."). However, since this would require every business to know every technical detail of an information collection or sale transaction (i.e., internet traffic flows, credit card processing locations, data storage locations, data backup locations), this exception becomes ineffective for most online transactions – or even in-person transactions with an online component or non-cash payment.

47. Colin Tankard, *What the GDPR Means for Businesses*, NETWORK SEC., June 2016 at 5–8.

48. The GDPR took effect on May 25th, 2018. Donald L. Buresh, *A Comparison between the European and the American Approaches to Privacy*, 6 INDON. J. INT'L & COMP. L. 257, 264 (2019). According to Buresh, it is effectively a "European 'bill of privacy rights.'" *Id*. at 267. It has a number of key provisions. *Id*. Like the CCPA, it applies to data based on the European Union individual, it requires firms to provide individuals with the ability to access, correct and delete their data, and it includes data portability requirements. *Id*. at 279. In several ways, it goes beyond CCPA. *Id*. at 278-80. For example, it requires that there be a specific legal basis for data processing. *Id*. at 265. It also requires firms to maintain data processing records, provide data breach notifications and have a data privacy officer. *Id*. at 266. The regulation also imposes restrictions on the transfer of data to non-EU member states and international organizations, requires the use of technical and non-technical

The data collection that would trigger the CCPA includes:

> [I]nformation that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:
>
> (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
>
> . . .
>
> (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
>
> . . .
>
> (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.
>
> . . .
>
> (G) [and] Geolocation data. . . .[49]

The CCPA requires a noticeable opt-out of data sharing option for adults' data,[50] and imposes restrictions on seeking reversal from someone who has opted out of sharing their data within the last twelve months.[51] The law also requires companies to have a CCPA-compliant privacy policy or disclosure,[52] along with a toll-free contact number.[53] It further imposes anti-retaliation provisions,[54] and provides consumers with access, deletion, and data

---

data security protections and implements certain limits on the use of automated decision-making systems. *Id.* at 267-69. Most notably, according to Ausley, it applies to virtually everyone everywhere as, "if a company reaches even one EU customer or employs a single EU citizen, the company must be fully compliant with the GDPR in regard to that person's data." Amber Ausley, *The Prospective Impact of the Global Data Protection Regulation on Entrepreneurship: A Roboadvisor Case Study*, 15 I/S A J. L. POL'Y INFO. SOC'Y 85, 88 (2019).

49. CAL. CIV. CODE § 1798.140(o)(1)(A), (D), (F)-(G) (West 2020).
50. *Id.* § 1798.120(a).
51. *Id.* § 1798.135(a)(5).
52. *Id.* § 1798.130(a)(5).
53. *Id.* § 1798.130(a)(1)(A).
54. *Id.* § 1798.125(a)(1).

portability rights.[55] It allows both the California Attorney General[56] and individual plaintiffs to take action in response to prospective violations.[57]

In addition to these general protections, the CCPA includes a variety of provisions that protect children. Specifically, it requires an explicit parental opt-in to allow the sale of data of children younger than thirteen.[58] It also requires children between thirteen and sixteen to opt-in themselves to allow the sale of their data.[59]

V. CONSTITUTIONAL QUESTIONS AND ACTUAL CCPA APPLICABILITY

Analysis of the text of the CCPA and long-arm precedent does not fully answer the question of how the CCPA will impact North Dakota. There are a variety of broader questions regarding the CCPA that have not been answered by the courts. Assembly Bill 375, which enacted the CCPA, was rapidly constructed by the California Legislature in response to a ballot initiative.[60] If the ballot initiative had passed, amending the statute in the future would have been problematic, as California places limitations on the modification of ballot measure laws.[61] Because of this, the law has several unresolved issues, ranging from typographical and clerical issues to more pronounced problems.[62] Some of these problems have been resolved via a series of subsequent bills.[63] However, perhaps most problematically, the CCPA has a pronounced Equal Protection problem in that the CCPA fails to extend its protections to non-Californians within California.[64] While the laws of a single state would obviously not be expected to protect every person in every location, the CCPA does not provide any protection to non-Californians. This is problematic as the Equal Protection Clause of the United States Constitution prohibits states from denying "to any person within its jurisdiction the equal protection of the laws."[65] Given the Equal Protection Clause considerations, a question remains as to how the law will be handled by the courts. It

55. *Id*. § 1798.100(d).
56. *Id*. § 1798.155(b).
57. *Id*. § 1798.150.
58. *Id*. § 1798.120(c).
59. *Id*.
60. Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States*, 23 J. TECH. L. & POL'Y 68, 73 (2018).
61. *Id*. at 91.
62. Alan Friel, Laura Jehl & Melinda McLellan, *The California Consumer Privacy Act: Frequently Asked Questions*, JD SUPRA (Mar. 28, 2019), https://www.jdsupra.com/legalnews/the-california-consumer-privacy-act-61053.
63. The CCPA Amendments that Survived the California Legislature, JONES DAY (Sept. 2019), https://www.jonesday.com/en/insights/2019/09/the-ccpa-amendments-that-survived.
64. *California Consumer Privacy Act (CCPA)*, CAL. DEP'T JUST. OFF. ATT'Y GEN., https://oag.ca.gov/privacy/ccpa (last visited Aug 16, 2020).
65. U.S. CONST. amend. XIV, § 1.

could be struck down in entirety or in part, or it could be re-written by the courts, a solution that has been used before as an Equal Protection remedy.[66] If a court utilizes a re-writing solution, it is difficult to predict exactly how the law would be changed to become Equal Protection compliant. Similarly, if the law is partially struck down by the courts, the remaining parts would determine what impact the law has. Of course, if the law is struck down in entirety, it would have no effect anywhere.

At present, no attorney general enforcement actions have been filed under the CCPA; however, multiple private suits have been filed.[67] These suits relate to data breaches,[68] and failures of websites to provide required notices.[69] To date, the law itself has not been challenged in the courts; however, it would seem to be only a matter of time until this occurs.[70]

VI. CALIFORNIA CONSUMER PRIVACY ACT IN NORTH DAKOTA

The main point of this article is to analyze the effect of the CCPA in North Dakota. Clearly, the CCPA was broadly drafted to have as much long-arm jurisdictional reach as possible.[71] Functionally, that means any North Dakota entity potentially affected by the CCPA has two options: First, to comply with the requirements of the CCPA, or second, ensure no aspect of its commercial conduct occurs in California or affects a California citizen. If a North Dakota entity has an online presence, compliance with the CCPA is

---

66. *See generally* Tom Campbell, *Severability of Statutes*, 62 HASTINGS L.J. 1495 (2011); Russell W. Galloway, *Basic Equal Protection Analysis*, 29 SANTA CLARA L. REV. 163, 163-64 (1989).

67. A search conducted in September 2020 identified approximately fifty private action suits that are currently pending that cite the CCPA.

68. See, e.g., Complaint at 25, Lopez v. Tandem Diabetes Care, Inc., No. 3:20-cv-00723-LAB-LL(S.D. Cal. April 16, 2020); See, e.g., Complaint at 28, 48, Almeida v. Slickwraps Inc., No. 2:20-at-00256 (E.D. Cal. March 12, 2020); Complaint at 6, 19, 38, Hernandez v. PIH Health, No. 2:20-cv-01662(C.D. Cal. Feb. 20, 2020); Complaint at 3, 15, Barnes v. Andersson, LLC, and Salesforce.Com, Inc., No. 4:20-cv-00812-DMR (N.D. Cal. Feb. 3, 2020); Complaint at 3, 21, Maldonado v. Solara Medical Supplies, LLC, No. 3:19-cv-02284-H-KSC(S.D. Cal. Nov. 29, 2019).

69. *See, e.g.*, Complaint at 9, *G.R. v. TikTok*, No. 2:20-cv-04537 (C.D. Cal. May 20, 2020); Complaint at 21, Sweeney v. Life on Air, No. 3:20-cv-00742 (S.D. Cal. April 17, 2020).

70. Initial letters were sent in July, 2020 which provided 30 days to cure the identified issues. Samuel F. Cullari & Alexis Cocco, *CCPA Enforcement Letters Sent; Supervising Deputy Attorney General Offers Insight*, TECH. L. DISPATCH (July 14, 2020), https://www.technologylawdispatch.com/2020/07/privacy-data-protection/ccpa-enforcement-letters-sent-supervising-deputy-attorney-general-offers-insight/. Presumably one or several of these letters could advance into an enforcement action that could be challenged in court.

71. The CCPA provides benefits to "consumers" who are defined, as "a natural person who is a California resident . . . ." CAL. CIV. CODE § 1798.140(g) (West 2020). The regulation explicitly covers out-of-state businesses (as opposed to only those with presence in California) exempting only activities "[I]f every aspect of that commercial conduct takes place wholly outside of California." *Id.* § 1798.145(a)(6). The definition of this requires that "[T]he business collected [the] information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold." *Id.* Given the amount of internet activity that occurs in California, avoiding ensnarement would be very difficult.

essentially the only reasonable option since there is no feasible method to "screen" website visitors to ensure they are not from California. Since the CCPA only applies[72] to business[73] with more than $25 million in revenue, who collect data on more than 50,000 individuals,[74] or who derive more than half their revenue from selling personal data, it would therefore appear to exclude smaller businesses underneath the threshold. However, a successful business may generate enough web traffic over time that the 50,000 person threshold is met. Although the statute is silent as to the method of counting, the threshold is cumulative annually.[75] Therefore, any data collected from a visitor from California would count towards the threshold. Fifty-thousand web hits, which could potentially be California consumers, could easily occur in a year for a website with even moderate levels of traffic.[76]

The CCPA is clearly intended to address any and all types of consumer tracking used by commercial websites and associated services that use identifiers, such as cookies. Thus, most North Dakota businesses' websites will bring them under the CCPA.

There is but a single exception to the CCPA. The exception states, "[t]his section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information."[77] The exception appears to be applicable only to 'guest'-type online purchases in that it does not require merchants to collect additional information just for CCPA purposes. However, this exception may not actually be applicable in many cases as, even though a merchant's online store application may not collect, retain, or resell personal identifying information ("PII"),

---

72. *See* discussion of parent and subsidiary organizations, *infra* section VII.B.

73. CAL. CIV. CODE § 1798.140(c) (West 2020); *see* discussion of business under CCPA, *supra* section IV.

74. *See* discussion of multiple counting of individuals, *supra* section IV.

75. *See* discussion of multiple counting of individuals, *supra* section IV.

76. Because of the way IP addresses are dynamically assigned by internet service providers, a single household may be assigned several IP addresses for its home internet connection during the course of a year. Additionally, users within the household might have multiple internet-connected devices. A hypothetical example illustrates this point. A family of four might include two adults who use the home internet connection, have mobile devices and access the internet at their workplace. It might also have two children who use the home internet connection, have mobile devices and access the internet at their school. This combination would result in 9 distinct IP addresses. If these addresses changed twice a month (the length of IP address assignment is an arbitrary decision by an internet service provider and could range from a few hours to multiple days), this one family could appear to be 108 distinct users to a website. Without a way to associate the different IP addresses with individuals and the different individuals into a single household, the operator would need to treat all of these accesses as distinct users for CCPA purposes. Under this hypothetical, it would only take 463 households to meet the CCPA threshold.

77. CAL. CIV. CODE § 1798.100(e) (West 2020).

the website may have other software that does collect, retain, or resell PII in a way that triggers the CCPA.

Unless a North Dakota business with an online presence is able to contract with a web hosting service that provides an effective screen and blocks all IP addresses from California, the only realistic option is to comply with the CCPA. Compliance generally requires a number of public, outward facing changes to websites, along with multiple internal data collection procedures.[78] Specific requirements for unique North Dakota business types will be addressed in more detail in Section VII of this article.[79] Generally, an affected business entity must notify consumers at or before collecting their data and create a process to inform consumers about the data collection, allow them to opt out, and to delete their PII.[80] Businesses must also respond to requests for data within specified timeframes.[81] Businesses must also disclose any financial incentive offered in exchange for the consumer's PII.[82]

More sophisticated businesses may already have procedures in place to comply with the European Union's GDPR.[83] However, GDPR compliance does not ensure CCPA compliance, as the CCPA requires more or extra steps in some cases.[84] The cost of compliance with the CCPA can be significant and is entirely born by the affected businesses.[85] Enforcement of the CCPA by the California Attorney General began in July with the issuance of business notification letters for alleged CCPA violators.[86]

---

78. Sarah Jodka, *California's Privacy Law: What It Is And How To Comply (A Step-By-Step Guide)*, DICKINSON WRIGHT (Jul. 12, 2018), https://www.dickinson-wright.com/news-alerts/californias-data-privacy-law.

79. *See* discussion *infra* section VII.

80. CAL. CIV. CODE §§ 1798.100(b), .105(a) (West 2020).

81. *Id*. § 1798.130(a)(2).

82. *Id*. § 1798.125(b).

83. *See* discussion of the GDPR *supra* section IV.

84. *California Consumer Privacy Act Fact Sheet*, CAL. DEP'T JUST., https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf (last visited Oct. 10, 2020).

85. *Id*. Funding is not provided by the CCPA for business expenses occurring due to the regulations. For an estimate of costs to businesses, see generally David Roland-Holst et al., *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, BERKELEY ECONOMIC ADVISING & RESEARCH, LLC (Aug. 2019), https://web.archive.org/web/20201010151603/https://www.tellusventure.com/downloads/privacy/calif_doj_regulatory_impact_assessment_ccpa_14aug2019.pdf (report prepared for the California Department of Justice).

86. Samuel F. Cullari & Alexis Cocco, *CCPA Enforcement Letters Sent; Supervising Deputy Attorney General Offers Insight*, TECH. L. DISPATCH (July 14, 2020), https://www.technologylawdispatch.com/2020/07/privacy-data-protection/ccpa-enforcement-letters-sent-supervising-deputy-attorney-general-offers-insight/. Notably, these letters were sent prior to the final regulations being approved by the California Office of Administrative Law on August 14, 2020. *CCPA Regulations*, CAL. DEP'T JUST. OFF. ATT'Y GEN., https://oag.ca.gov/privacy/ccpa/regs (last visited Aug 17, 2020). At present no attorney general enforcement actions have been filed, see *supra* note 67.

VII. EXAMPLES OF THE IMPACT OF THE CCPA ON NORTH DAKOTA BUSINESSES

This section considers the implications of the CCPA for three particular areas of focus in North Dakota. The potential impact of CCPA for unmanned aerial systems, agriculture, and energy are each discussed.

A. UNMANNED AIRCRAFT SYSTEMS

The proliferation of Unmanned Aircraft Systems ("UAS") in North Dakota and around the United States in the past decade has been well-documented and analyzed.[87] The ability of drones to efficiently gather large amounts of potentially personal identifying information requires special analysis under the CCPA. North Dakota-based businesses offer drone services nationally and the regulations for the operation of drones under the Federal Aviation Regulations apply nationwide.[88]

Two examples are illustrative of the issues drones present. First, the common instance of the airborne capture of a person's image in a public place by a drone would implicate the CCPA, even though in other contexts there exists no specific expectation of privacy in public spaces.[89] Under the CCPA, however, such a photograph would be defined as covered "personal information" even though the CCPA definition of "personal information" states that it does not include "publicly available information."[90] However, due to the narrow definition of "publicly available information," this photograph is not excluded from CCPA coverage. Thus, even though it would seem that a person's presence in public would create "publicly available information," this

---

87. *See Drones: Reporting for Work*, GOLDMAN SACHS, https://www.goldmansachs.com/insights/technology-driving-innovation/drones/ (last visited Aug 17, 2020); Business Insider Intelligence, *Drone Market Outlook: Industry Growth Trends, Market Stats and Forecast*, BUSINESS INSIDER (Mar. 3, 2020, 3:28 PM), https://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts; Tony Murfin, *UAV Reprt: Growth Trends & Opportunities for 2019*, GPS WORLD (Oct. 1, 2018), https://www.gpsworld.com/uav-report-growth-trends-opportunities-for-2019/.

88. The operation of UAVs, in the United States, is governed by the Federal Aviation Regulations, *see* 14 C.F.R. pt. 48 (2015); 14 C.F.R. pt. 101 (2016); and 14 C.F.R. pt. 107 (2016).

89. For a discussion of expectations of privacy in public places, *see generally* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141 (2014).

90. CAL CIV. CODE § 1798.140(o)(2) (West 2020) ("'Personal information' does not include publicly available information."); *Id.* § 1798.140(o)(2) (narrowly defining "publicly available" as "information that is lawfully made available from federal, state, or local government records."); *Id.* § 1798.140(o)(1)(B) (personal information includes "[a]ny categories of personal information described in subdivision (e) of Section 1798.80."); *Id.* § 1798.80(e) ("'Personal information' means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."). A photograph would clearly include "physical characteristics or description" and thus would be considered personal information.

is not the case. For purposes of the CCPA, "publicly available" is narrowly defined as "information that is lawfully made available from federal, state, or local government records."[91] A North Dakota business using drones to gather imagery would be subject to the CCPA if its operations collected information for more than 50,000 consumers,[92] which could easily be the case if the drones were used to survey large geographic areas or large crowds of people. Even though many of those photographed would likely not be Californians, for imagery taken outside of California, the business would have to treat each person that was photographed as potentially a CCPA-protected Californian, as it would likely not have any way of determining or proving that they are not. Since it would not be easily determined who in such images would be residents of California, prudent businesses would treat all images as subject to the CCPA and fall under the CCPA, generally, because of this.

A second example would be a drone used in communications relay or as a wireless access point, perhaps as part of disaster relief. If the business providing the drone services were contracted by a large telecommunications or internet service provider and the provider's branding was included on the drone or as part of any aspect of the service, the data passing through the drone and the operation could be seen as subject to the control of the business temporarily as it is transmitted. This alone might be sufficient to trigger the provisions of the CCPA.[93] Thus, even a small North Dakota drone operator may have to deal with CCPA considerations despite never operating in California.

Both of the foregoing examples show how the CCPA can impose costs on and create logistical impediments to the operations of UAS companies in North Dakota. More generally, these examples also show how a CCPA compliance requirement can stem from multiple areas of a business's operations. Thus, firms must fully assess their operating practices to determine CCPA-applicability and ensure compliance in all areas.

B. AGRICULTURE

Firms that directly market to consumers, maintain frequently accessed websites, have revenues over $25 million, or are the parent or subsidiary of entities that do so, may have CCPA implications.[94] Note that per the

---

91. *Id.* § 1798.140 (o)(1)(K)(2).

92. If one was to take a very strict interpretation, this could also include houses or devices in images in this count as the CCPA combines together "consumers, households, or devices." *See Id.* § 1798.140(c)(1)(B).

93. *Id.* § 1798.140(c)(2) (stating a business is covered by the CCPA if it controls or is controlled by a business that meets section 1798.140(c)(1) and "shares common branding" with or has "the power to exercise a controlling influence over the management of a company" causes the controlled company to be covered by the CCPA).

94. *Id.* § 1798.140(c).

definition of business,[95] large farms, farming co-operatives, grain elevators, and other agricultural businesses could potentially fall under CCPA jurisdiction. Some entities may also fall under CCPA regulations because they are a parent or subsidiary of another firm that meets these criteria.[96]

Two examples are illustrative. First, a firm that makes a packaged food product and sells this product nationwide, despite not having revenues of $25 million, would fall under CCPA jurisdiction if it ran a sweepstakes that collected information for "50,000 or more consumers, households, or devices"[97] during the campaign. Second, a small business restaurant that is a franchisee of a national brand[98] and operates under the "shared name, servicemark, or trademark"[99] of the national franchiser would fall under CCPA jurisdiction if the national franchiser has revenues of $25 million, data for 50,000 individuals, or derived half or more of its revenue from the sale of personal information.[100]

Smaller farmers could also be ensnared by remote access of their website, if they should maintain one. If the website exceeds the 50,000 person access threshold from potential Californians, the business would fall under the CCPA.[101]

C. ENERGY

In the energy sector, firms that are subsidiaries or parents of large firms meeting the $25 million gross revenues, 50,000 individual, or personal

---

95. *Id*. § 1798.140(c)(1) (defining "business" in part as (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. (B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.").

96. *Id*. § 1798.140(c)(2) (defining business to include "[a]ny entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. 'Control' or 'controlled' means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. 'Common branding' means a shared name, servicemark, or trademark").

97. *Id*. § 1798.140(c)(1)(B).

98. It is presumed that the requirement to follow operating directives and policies of the franchiser could meet the definition of "power to exercise a controlling influence over the management of a company." *See id*. § 1798.140(c)(1)(C)(2).

99. *Id*. § 1798.140(c)(2).

100. *Id*. § 1798.140(c)(1)(A)-(C).

101. *See* discussion of website thresholds, *supra* note 71.

information sale threshold would fall under the CCPA.[102] Perhaps even more relevant is the CCPA provision that includes firms in which another qualifying firm has the "power to exercise a controlling influence over" its management, while "shar[ing] common branding" of any kind.[103] This could prospectively ensnare independent drilling companies and similar providers who have relationships with larger qualifying firms. Firms that sell energy directly to consumers and that have over 50,000 customers that are or could be Californians, or even 50,000 unique website visits, would also be ensnared under this provision. A firm that has a limited number of non-consumer customers[104] and does not sell to the public could quickly become subject to CCPA provisions if it experienced a scandal, such as a pipeline leak, that drove significant web traffic in a short period of time.

Two examples are illustrative. First, a corporation that sells electricity to consumers in North Dakota and is the subsidiary of a larger firm that has revenues over $25 million or has information for over 50,000 consumers would fall under CCPA jurisdiction.[105] Second, a small business that sells an energy-saving device indirectly via a third-party website would fall under the CCPA if it has 50,000 unique visits to the website during a year.[106]

Given the foregoing, it seems likely that many North Dakota energy firms may have CCPA compliance requirements. Some firms may attempt to structure their operations or remove all common branding to forestall this. However, given the potential for web visits to trigger a compliance requirement, no firm can be assured that a CCPA avoidance strategy would definitely be successful.

VIII. RECOMMENDATIONS FOR NORTH DAKOTA BUSINESSES

North Dakota businesses, including the industries discussed in greater detail in Section VII, are faced with complying with the CCPA. Because of

---

102. CAL CIV. CODE § 1798.140(c)(1)(A)-(B) (West 2020).

103. *Id.* § 1798.140(c)(2) (including as a covered business "[a]ny entity that controls or is controlled by a business … and that shares common branding with the business").

104. Non-consumer customers are business, non-profit organization and government customers who do not receive the same protections under the CCPA. CAL. CIV. CODE § 1798.140(g) (West 2020) (defining consumer as "a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier"). The CCPA protects consumers, as it defines them, and thus does not extend protections to those that it doesn't include within the definition of consumers (such as businesses, non-profits and governments).

105. CAL. CIV. CODE § 1798.140(c)(1)(A) (West 2020) (including businesses that have "annual gross revenues in excess of twenty-five million dollars"); *Id.* § 1798.140(c)(1)(B) (including any business that "[a]lone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices").

106. CAL. CIV. CODE § 1798.140(c)(1)(B) (West 2020); *see also* the discussion of web hits, *supra* note 76 ("Fifty-thousand web hits, which could potentially be California consumers, could easily occur in a year for a website with even moderate levels of traffic.").

the questionable constitutionality of the CCPA,[107] affected North Dakota businesses may elect to challenge it either on its face or upon expending resources on compliance. To achieve compliance, the CCPA requires affected business entities to notify consumers, allow them to opt out, and to delete their PII.[108] Businesses must also disclose any financial incentive offered in exchange for the consumer's PII and respond to such requests within specified timeframes.[109]

Specifically, North Dakota businesses choosing to continue to do business in California will be required to follow the guidelines provided by the California Administrative Code, which provide greater compliance details to supplement the California Civil Code's statutory requirements.[110] The Administrative Code regulations are numerous, but do provide some help where the Code is ambiguous or silent. For example, in the case of an application that is not directly associated with a specific individual in the business's records, the consumer could be asked to "demonstrate that they are the sole consumer associated with the personal information" or to "respond to a notification sent to their device."[111]

The Administrative Code also provides extensive guidance specific to the timing and presentation of such things as opt-out buttons, links for consumers to select whether the business may sell the consumer's personal information, how to respond to consumer requests for consumer "requests to know," and requests to delete information.[112] Many private practitioners have published additional compliance suggestions on their personal websites or offer legal services to clients specifically focused on CCPA compliance.[113]

IX. CONCLUSION

Despite a firm's location in North Dakota rather than California and even if the firm makes no particular effort to target Californians as customers, any firm that meets the general requirements of the CCPA and has a website or access to analytic information from social media should prepare to deal with CCPA implications.[114] Public interest in a company or product – or a

107. *See* discussion *supra* section V.

108. *See* discussion *supra* section VI.

109. *See* discussion *supra* section VI.

110. *See generally* CAL. CODE REGS. tit. 11, §§ 999.300-999.337 (2020) (CCPA regulations).

111. *Id.* § 999.325(e)(2).

112. *Id.* §§ 999.306, 999.312, 999.315, 999.318.

113. *See California Consumer Privacy Act*, BUCHALTER, https://www.buchalter.com/publication/california-consumer-privacy-act/ (last visited Aug 18, 2020); *California Consumer Privacy Act (CCPA),* KRONENBERGER ROSENFELD, LLP, https://www.krinternetlaw.com/practice-areas/internet-law (follow Website Agreements: California Consumer Privacy Act (CCPA)) (last visited Aug 18, 2020); *California Consumer Privacy Act (CCPA),* REED SMITH, LLP, https://www.reedsmith.com/en/capabilities/services/ip-tech-and-data/data-privacy-and-security/california-consumer-privacy-act-ccpa (last visited Aug 18, 2020).

114. *See* discussion of the definition of a business *supra* section VI.

scandal – could quickly push a company across the 50,000 individual, household, or device threshold to trigger the CCPA. Virtually every business that has an online presence could be taken to do "business in"[115] California and few transactions could have a guarantee of taking place "wholly outside of California."[116] Given this, it would seem that any prudent business with a website should be preparing for CCPA compliance.[117] Some firms, particularly those that only wish to have a minimal informational web presence, may wish to cease having an online presence or contract with a provider that does not maintain or provide them access to logs in order to prevent incidental ensnarement under the CCPA. It is also possible that, as CCPA compliance requirements continue to become better understood, options may emerge to provide technical 'California free' solutions.[118]

In the short term, CCPA compliance becomes a hassle for businesses and those that California defines as businesses, beyond typical definitions,[119] in North Dakota and beyond. Businesses must incur the costs of compliance, such as modifying their website and maintaining the required contact mechanisms and records, or decide not to take these steps and risk enforcement actions and potential fines.

The CCPA illustrates a clear problem with extra-jurisdictional laws which is also raised by the European GDPR. What will become even more problematic is the eventual conflicts between this patchwork of regulations which will leave covered entities scrambling to determine which law among this patchwork of conflicting laws has priority, thereby creating the very real potential for being in a liable-if-you-don't, liable-if-you-do situation.

The U.S. Constitution provides that "Full Faith and Credit shall be given in each State to the public Acts, Records, and judicial Proceedings of every other State"[120] For this reason, North Dakota courts, along with other courts, may be called upon to enforce the CCPA and order the collection of CCPA fines and even the extradition of individuals wanted for the violation of

115. *See* discussion of the definition of doing business in California, *supra* section IV.

116. *See* discussion of out-of-California transactions, supra section IV.

117. Note that, because of the annual definition of 50,000 consumers / households / devices in Section 1798.140(c)(1)(B), a business would appear to be covered for an entire year once they hit this threshold. Because "annually" is not specifically defined, this could be taken to mean up to an entire year before (or after) a spike causing the threshold to be met. Given this, an otherwise ensnared entity cannot necessarily plan to start CCPA compliance activities (particularly maintaining records required therefor) at the point that they reach this threshold, particularly if reaching this threshold was reasonably foreseeable.

118. This would be similar to how some international products are marketed as ITAR free to avoid ensnarement by U.S. International Trafficking in Arms Regulations. P. J. Blount, *The ITAR Treaty and Its Implications for U.S. Space Exploration Policy and the Commercial Space Industry*, 73 J. AIR L. & COM. 705, 713 (2008).

119. *See* discussion of business, *supra* section VII.B.

120. U.S. CONST. art. IV, § 1.

California law.[121] Conversely, California has an equal obligation to respect and give "Full Faith and Credit" to North Dakota's "public acts," such as its laws and regulations.[122] A remote state imposing its laws on North Dakotans and North Dakota businesses operating in North Dakota clearly intrudes on the regulatory domain of the North Dakota state government and thus seems to be an overt failure to provide the requisite due respect.

Invariably, the CCPA will be reviewed by the courts and it seems likely that changes will be made in response to judicial review, enforcement experience, and other factors. Given the potential, if not the likelihood, of the development of other similarly problematic statutes by California and other states, there is a clear role for the U.S. Congress to establish, through legislation, to limit the applicability of one state's laws within other states.[123] After all, it is the federal government's duty to "[p]rotect each [state] against [i]nvasion."[124]

121. N.D. CENT CODE § 28-20.1-01 (2019) (requiring North Dakota courts to enforce foreign court judgements which are "entitled to full faith and credit in this state."); N.D. CENT. CODE ch. 29-30.3 (providing for the extradition of a "requested person" to a "requesting state").

122. *See* U.S. CONST. art. IV, § 1.

123. Since laws in one state that regulate commercial activities in another are inherently dealing with interstate commerce, the U.S. Constitution's Commerce Clause provides a mechanism for federal regulation, *see, e.g.,* U.S. Const. art. 1, § 8 (providing Congress the power to "to regulate commerce … among the several states"); West Lynn Creamery, Inc. v. Healy, 512 U.S. 186, 198-207 (1994) (finding a law that treated out-of-state and in-state entities differently unconstitutionally burdened interstate commerce); The Internet Tax Freedom Act of 1998, Pub. L. No. 105-277, § 151, 112 Stat. 2681 (1998) temporarily banned states from taxing internet access nationwide (except where taxes pre-existed). The Trade Facilitation and Trade Enforcement Act of 2015, Pub. L. No. 114-125, § 922, 130 Stat. 122 (2016) made this ban permanent and required states to stop pre-existing taxation on June 30, 2020.

124. U.S. CONST. art. IV, § 4.