MERCATUS CENTER
George Mason University

TESTIMONY

CONSIDERATIONS FOR NORTH DAKOTA REGARDING CONSUMER DATA PRIVACY POLICY

Jennifer Huddleston
Research Fellow, Fourth Branch Project, Mercatus Center at George Mason University

North Dakota Legislature, Interim Commerce Committee

January 15, 2019

Good afternoon, Chairman Scott Louser, Vice Chairman Shawn Vedaa, and distinguished members of the Interim Commerce Committee.

My name is Jennifer Huddleston, and I am a research fellow at the Mercatus Center at George Mason University, where my research focuses primarily on the intersection of law and technology. This focus includes issues surrounding consumer data privacy. Thank you for this opportunity to discuss such policy matters in relation to the protections, enforcement, and remedies regarding consumers' personal data and the impact of actions taken by other states on this matter.

Within this context I would like to focus on three key points:

1. Existing laws regarding consumer data and the potential tradeoffs to other benefits, including free expression and innovation involved in further regulation of data privacy
2. Potential problems and constitutional concerns from state laws regarding data privacy, including issues under the Dormant Commerce Clause and creation of a disruptive patchwork, that result in the need for a single, federal standard
3. State policy regarding data privacy, which should focus only on the government's own actions or those actions that are solely intrastate

THE CURRENT DATA PRIVACY LANDSCAPE

The United States has traditionally embraced a "permissionless" approach to information technology issues, including issues related to consumer data privacy. The presumption in this approach is that new technology should be allowed to enter the market unless otherwise subject to existing regulation or if regulation would prevent harm or catastrophe that would clearly result from the introduction of the technology or its specific application. In contrast, Europe has taken a much more "precautionary" approach that presumes the potentially risky or harmful impact of technology and instead requires innovators and entrepreneurs to show that such potential risks have been eliminated or minimized. In the same time period, the United States has emerged as a leader in the digital economy, while more heavily regulated jurisdictions such as Europe have produced few tech giants. A shift away from this "permissionless" framework would likely result in tradeoffs that could change the traditional success and leadership the United States has experienced in the digital economy.

For more information or to meet with the scholar, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University, 3434 Washington Blvd., 4th Floor, Arlington, Virginia 22201

Even with this light-touch tradition, the United States is not a Wild West when it comes to data privacy. Instead, the approach has been to identify areas where data are particularly sensitive and where disclosure of information or other potential privacy breaches are likely to result in potential harm. As a result, many types of information, including financial information, healthcare records, educational records, and the data for children under 13 are already subject to additional federal regulations.[1] While these laws may result in tradeoffs that mean certain benefits are forgone or certain innovations are not pursued, the laws represent a much more specific approach, focused on areas where there is particular vulnerability or risk of harm. Additionally, in some cases, these laws also illustrate that even in areas where society highly values privacy, there can be problems and tradeoffs. For example, frustration can ensue when an institution favors privacy out of an abundance of caution for HIPAA requirements and a patient is thus unable to obtain his or her own records.[2] Because all regulation regarding data privacy should be designed to address harms, it should be considered if existing laws already address these harms or could merely be updated to do so.

Concerns are sometimes based less in the day-to-day usage of data and are based more on concerns about data breaches and data security than data privacy. In this area, it is important to note that all 50 states have some kind of data breach notification law, so consumers should receive notification when involved in such an incident.[3] While this state-by-state approach has resulted in notification in all states, the requirements and covered information vary and can create confusion for both consumers and innovators.[4]

This current approach has allowed the expression of a wide range of individual preference when it comes to privacy and data usage. It has also allowed many beneficial services and options for both individuals and society as a whole.[5] Changes to the American approach to data privacy could result in the loss of these benefits and substantially affect individuals, innovation, and the economy.[6]

STATE REGULATION OF CONSUMER DATA PRIVACY PRESENTS ADDITIONAL CONCERNS

Recent headlines and the actions by other jurisdictions, including the European Union's General Data Protection Rule (GDPR), have led American policymakers to question continuing the more hands-off approach to this issue. In the absence of federal legislation, some states have chosen to consider their own legislation rather than wait for a national standard. As of January 2020, California, Maine, and Nevada have enacted additional consumer data privacy regulations and more than 18 other states, including North Dakota, are studying or have considered similar regulation.[7] However, this state-by-state approach has additional innovation-disrupting consequences and raises concerns about potential constitutionality.

Consumer data and the interactions that generate it can involve many states and is difficult to confine to a single state's borders. Ian Adams and I previously noted that "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."[8] As a result, such state laws can have an impact and burden on firms

---

[1] Alan McQuinn, "Understanding Data Privacy," *RealClear Policy*, October 25, 2018
[2] Judith Graham, "In Days of Data Galore, Patients Have Trouble Getting Their Own Records," *Kaiser Health News*, October 25, 2018.
[3] Caleb Skeath and Brooke Kahn, "State Data Breach Notification Laws: 2018 in Review," *Inside Privacy*, December 31, 2018.
[4] Jennifer Huddleston, "The State of State Data Laws, Part 1: Data Breach Notification Laws," *The Bridge*, July 31, 2019.
[5] John Raidt, "7 Great Ways Data Can Benefit Society," *U.S. Chamber of Commerce*, May 23, 2016.
[6] Alan McQuinn and Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law* (Washington, DC: Information Technology and Innovation Foundation, 2019).
[7] National Conference of State Legislatures, "Consumer Data Privacy Legislation," January 3, 2020, http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.
[8] Jennifer Huddleston and Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations* (Washington, DC: Regulatory Transparency Project, 2019).

beyond a state's borders. Given these burdens on nonresident firms and potentially nonresident consumers, these laws may be unconstitutional under the Dormant Commerce Clause.[9]

When analyzing an argument regarding the Dormant Commerce Clause, the courts examine if the state law directly discriminates against out-of-state actors or, if facially neutral with regard to out-of-state actors, indirectly discriminates against them. Current state consumer data privacy laws are not facially discriminatory against out-of-state actors.[10] Their likely effect on out-of-state businesses and consumers, however, raises constitutional issues under the Dormant Commerce Clause, which, among other things, considers whether the burdens on out-of-state parties are disproportionate to the purported in-state benefits.[11] This is where the constitutionality of state consumer data privacy laws could likely be called into question. In *Bibb v. Navajo Freight Lines*, the US Supreme Court struck down a state law that would require a specific type of mudflaps, which would likely result in truck drivers having to change their mudflaps at state borders, as an unconstitutional burden on interstate commerce even if it was not facially discriminatory.[12] Data and the internet are naturally an interstate interaction, and it would be even more difficult to expect a change in data handling to occur at a virtual border for each state's specific requirements.

The Dormant Commerce Clause is not the only potential constitutional concern such laws face. As mentioned earlier, federal regulations exist for certain areas of data. While some of these laws allow for additional state regulation in these areas, state laws could create conflicts that make compliance with both state and federal regulation difficult or incredibly burdensome.[13] The supremacy of federal law could mean that if policymakers do not carefully consider these potential conflicts, allegedly comprehensive privacy laws could be anything but comprehensive as certain sections are preempted by their conflicts with federal laws.[14]

State lawmakers as well as federal lawmakers must also consider the potential conflicts between consumer data privacy and other rights. This is perhaps most obvious in the context of potential burdens on speech that may result from consumer data privacy laws. State data privacy laws may be subject to a high level of scrutiny and found unconstitutional if they discriminate based on the content or purpose of the data.[15] In addition, consideration of requirements such as deletion or a right to be forgotten could silence speakers and impact the availability of important information.[16]

Even aside from these constitutional considerations, a state-by-state approach could have additional negative effects on innovation. Such laws could conflict with one another, interrupting the seamless nature of the internet and information and preventing the same product from being offered in all states. Additionally, this patchwork approach could create confusion for both consumers and companies who are uncertain about what rights they have or what information they should provide. When such uncertainty ensues, mistakes and frustrations may result.

To combat this confusion, innovators might merely choose to comply with the most restrictive requirements, even if other states have more market-friendly approach. For example, Microsoft

---

[9] Huddleston and Adams, *Potential Constitutional Conflicts*.
[10] Huddleston and Adams.
[11] Pike v. Bruce Church, 397 U.S. 137, 142 (1970).
[12] Bibb v. Navajo Freight Lines, Inc., 359 U.S. 520 (1959).
[13] Huddleston and Adams, *Potential Constitutional Conflicts*; US Department of Health and Human Services, "Does the HIPAA Privacy Rule Preempt State Laws?," March 12, 2003, https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html (providing an example of when conflicts may be preempted).
[14] Huddleston and Adams, *Potential Constitutional Conflicts*.
[15] Huddleston and Adams; Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, October 27, 2017).
[16] Huddleston and Adams; Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases."

already stated it would apply the requirements of the California Consumer Privacy Act (CCPA) nationally.[17] Even if all 50 states passed identical or nearly identical legislation, differences in interpretation or enforcement could still result in issues that mean a single state's enforcement decision has an outsized impact.

Such regulations are not costless, and state policymakers should carefully consider the potential economic costs as well as the loss of innovation and investment. California's own study of the potential impact of its CCPA showed it would cost $55 billion to in-state companies. This figure does not include the costs borne by out-of-state companies that will almost certainly be subject to the law.[18] The GDPR also provides an example of the potential costs. One study suggests that, in its first year, the GDPR resulted in a 17.6 percent decrease in weekly venture capital investment and such deals contained less investment than in prior years.[19] As a result of this decreased investment, research suggests that the GDPR could have resulted in 29,000 fewer jobs—jobs that were not created by new innovative companies.[20]

Finally, regulations that prevent certain uses of data could actually deter innovation in privacy and security as well as undermine their end goal. For example, the quick turnaround time for delivering data to legitimate requests can result in mistakes, as seen with the GDPR, such as a fiancé being able to obtain personal information on his betrothed or sending Alexa voice recordings to the wrong recipient.[21] Policymakers should carefully consider whether proposed regulation risks creating new privacy concerns and what its potential effect on data security is.

Keeping these potential constitutional concerns and consequences in mind, in many cases the best action for state policymakers may be no take action at all.

POTENTIAL PROPER ROLE FOR STATES IN ADVANCING DATA PRIVACY

Although I have laid out the potential issues and concerns with state data privacy actions in the preceding sections, there are some actions that states might be able to take within their proper role in the federal system. Largely these will be policies that affect only data actions that the state itself undertakes or that are solely intrastate.

The most notable example of this is a recent Utah law requiring a warrant for various law enforcement access to data.[22] Such an approach is in line with recent Supreme Court precedent regarding the removal of warrantless access to cell service location information.[23] Such laws protect individuals' civil liberties but do not have the same impact beyond state borders as other laws. Such an approach still should recognize that, at times, data are useful and beneficial while also recognizing existing principles and protections from unnecessary government intrusion.

---

[17] Daniel A. Lyons, "State Net Neutrality" (Research Paper No. 514, Boston College Law School, Newton, MA, October 11, 2019) (discussing such in the context of State Net Neutrality laws).
[18] State of California Department of Justice, Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018*, August 2019.
[19] Jian Jia, Ginger Lin, and Liad Wagman, "The Short-Run Effects of GDPR on Technology Venture Capital Investment," Vox (Center for Economic Policy Research), January 7, 2019, https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment.
[20] Jia, Lin, and Wagman, "The Short-Run Effects."
[21] Lorenzo Franceschi-Bicchierai, "Researchers Show How Europe's Data Protection Laws Can Dox People," *Motherboard*, *Vice*, August 8, 2019; Nick Statt, "Amazon Sent 1,700 Alexa Voice Recordings to the Wrong User Following Data Request," *Verge*, December 20, 2018.
[22] Molly Davis, "Utah Just Became a Leader in Digital Privacy," *Wired*, March 22, 2019,
[23] Jennifer Huddleston and Anne Philpot, "Adapting 4th Amendment Standards to Connected Technology," *Law 360*, November 14, 2019; Brent Skorup and Jennifer Huddleston Skees, "Bringing Constitutional Doctrine into the Digital Age," *Washington Times*, July 3, 2018.

Policies at a state or local level should focus only on those actions and data that occur within their borders. Another possible example would be regulations related to the governments' own collection and usage of data. These issues are distinct from the broad consumer privacy laws often proposed and should also reflect specific harms and legal standards.

CONCLUSION

What, if any, additional regulation or enforcement is needed regarding consumer data privacy continues to be a hotly debated issue. However, in many cases a federal framework will be needed rather than the potential disruption caused by a state patchwork. Still, states can play an important role in encouraging action at the federal level and continuing to preserve the benefits of the American approach to innovation. Rather than seeking broad consumer privacy actions, if states feel the need to act, they should look at potential restraints on their own actions or other similar intrastate issues.

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).

MERCATUS CENTER
George Mason University

What GDPR's First Year Says about Data Privacy Regulation

Wednesday, May 29, 2019

Authors: Jennifer Huddleston

Almost a year ago, the European Union's General Data Protection Regulation (GDPR) [1] went into effect. In that year, the United States has been engaging in its own debate about what, if anything, should be done to bolster our data privacy protections. While some have suggested that the United States implement its own GDPR [2] — a comprehensive reform to more tightly regulate the collection, use, and retention of data — we have the advantage of looking at the early consequences of Europe's policy.

As debates about potential federal data privacy legislation continue [3], what can the first year of the GDPR teach us about what such a regime may do in America?

First, the cost of compliance with complicated data regulations is not cheap, and as a result, some companies may choose to leave the market rather than comply. According to a PwC survey [4], more than 40 percent of companies surveyed, including American companies with a data presence in the EU, spent over $10 million preparing to comply with GDPR.

From video game [5] sellers to various news outlets [6] including the Los Angeles Times, some companies found the costs too high to continue doing business in Europe, and removed themselves from the EU. For others that chose to remain, things remain uncertain. In some cases, courts and countries continue to work through interpretations, often with differing results [7].

Now, almost a year later, many of these companies still have not returned to Europe. Some might argue this is not necessarily a bad thing if new, more privacy-sensitive companies take their place. Yet, venture capital investment in startups in Europe post-GDPR is down by over $3 million [8], according to a National Bureau of Economic Research study. As a result, there were likely 3,000 to 30,000 fewer jobs.

Large companies are not immune from the effects of cumbersome regulatory schemes, but policies like the GDPR are more difficult on new entrants [9] struggling to find footing in the market. In the immediate aftermath of GDPR, large players in the targeted advertising space were able to grow or maintain [10] their market share. Newer and smaller players seemed to struggle.

While we shouldn't assume big is bad [11], strict top-down regulations like the GDPR will make it more difficult for new companies and competitors to challenge existing players. In the long-term, we may get a static market in which the "next Google" fails to emerge and improve upon what more established tech giants are doing.

It may be worth it for consumers to have the extra privacy, but are European consumers actually safer than they were before GDPR?

"Opt-in changes [12]" — like the click-throughs where users must approve of web sites' use of cookies before proceeding — do not appear to actually increase consumer decision making regarding privacy. Similarly, when email inboxes were filled with updated privacy policies [13] in the weeks leading up to the GDPR, it did not appear to lead to real changes in their online behavior.

GDPR's requirement that companies respond quickly to user requests for large amounts of data (and harsh penalties for failing to comply), may not always be the silver bullet for portability or transparency. For example, in one incident, Amazon sent 1,700 Alexa recordings [14] to the wrong user.

Laying out some of these consequences is not to say that we shouldn't place a premium on internet privacy. Rather, it's to point out that pursuing privacy is not without tradeoffs with other things that we value or benefit from. There are already a wide variety of options for individuals to make choices about their own privacy, and we hold a wide variety [15] of individual privacy preferences in the first place.

As the United States debates whether or not to implement its own comprehensive, federal privacy law, we should pay attention to the recent lessons of the GDPR. A U.S. GDPR may sound comforting, but perhaps we should simply adapt the more permissionless notice-and-choice approach that has allowed us to lead the world in innovation — and reap tremendous benefits [16]. As a result, we may be able to find more solutions with fewer negative consequences.

Source URL: https://www.mercatus.org/bridge/commentary/what-gdprs-first-year-says-about-data-privacy-regulation

Links
[1] https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018
[2] https://securityboulevard.com/2019/04/equifax-breach-leads-u-s-senate-to-propose-america-draft-its-own-gdpr/
[3] https://www.reuters.com/article/us-usa-privacy-congress/u-s-lawmakers-struggle-to-draft-online-privacy-bill-idUSKCN1S62NA?utm_source=applenews
[4] https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html
[5] https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html
[6] https://gizmodo.com/dozens-of-american-news-sites-blocked-in-europe-as-gdpr-1826319542
[7] https://digiday.com/media/gdpr-regulators-mixed-signals-industry-confusion/
[8] https://www.mediapost.com/publications/article/330185/gdpr-has-chilling-effect-on-eu-tech-funding-study.html
[9] https://www.realclearpolicy.com/articles/2018/06/01/its_not_about_facebook_its_about_the_next_facebook_110654.html
[10] https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr
[11] https://reason.com/2019/04/09/why-tyler-cowen-loves-big-tech-and-think/
[12] https://www.americanactionforum.org/insight/opt-in-mandates-shouldnt-be-included-in-privacy-laws/
[13] https://slate.com/technology/2018/05/heres-what-you-should-actually-do-with-all-those-privacy-policy-emails-dont-delete-them-yet.html
[14] https://www.theverge.com/2018/12/20/18150531/amazon-alexa-voice-recordings-wrong-user-gdpr-privacy-ai
[15] https://niskanencenter.org/blog/against-privacy-fundamentalism-in-the-united-states/
[16] https://www.mercatus.org/publications/entrepreneurship/technological-innovation-and-economic-growth

https://www.mercatus.org

THE HILL

Should Congress be concerne about California's data privacy

BY JENNIFER HUDDLESTON, OPINION CONTRIBUTOR — 12/03/19 04:30 PM EST
THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

Just In...

Sanders hits Facebook, GOP in response to alleged Russian hack of Ukrainian gas company
TECHNOLOGY — 7M 51S AGO

Democracy wins again — now Trump should set China straight on Taiwan
OPINION — 10M 18S AGO

McConnell knocks call for additional impeachment witnesses
SENATE — 10M 40S AGO

Shepard Smith talking to MSNBC about primetime spot as network eyes Chuck Todd move: report
MEDIA — 11M 39S AGO

Panel: Who will win and lose at tonight's debate?
RISING — 13M 29S AGO

Panel debates should Bernie Sanders confront Elizabeth Warren at the debate
RISING — 15M 1S AGO

'Homeland' star accuses Trump of trying to 'have it both ways' on intelligence
IN THE KNOW — 15M 34S AGO

Rural Iowa Dem reveals which 2020

© The Hill photo illustration

As 2019 comes to a close, the debate over a potential federal data privacy framework continues. The Senate Commerce Committee is set for a Dec. 4 hearing examining potential legislative proposals for protecting consumer privacy, and Senate Democrats recently listed a set of principles they desire in any federal data privacy legislation. But with little overall movement on the federal level, states including Nevada, California, and Maine have passed their own policies that are or will soon be effective.

These state laws will have a national effect. Some technology companies, including Microsoft, already plan on honoring the California Consumer Privacy Act (CCPA) nationwide. Indeed, because of its structure and application to California residents the CCPA will have an outsized impact, even outside of the state. California firms are expected to spend nearly $55 billion in compliance costs the first year alone, and many more firms based outside of the state will also be subject to requirements that could easily have six-figure compliance costs if they wish to continue doing business there.

In addition to worrying about the ability of one large state to influence — and potentially stifle — innovative industries from coast to coast, we should explore whether this development could affect the constitutional framework of federalism. Namely, such laws could trigger questions about potential unconstitutional burdens on interstate commerce.

presidential candidate is winning farm country
RISING — 16M 1S AGO

VIEW ALL

View Latest Opinions >>

Laws like CCPA may not directly discriminate against out-of-state companies, but the costs and burdens associated with compliance — as well as the potential national impact on consumer choice, decisions regarding privacy and data, and free expression and innovation — raise doubts. Should the purported in-state benefits of a law outweigh the burdens it creates for out-of-state parties?

Such burdens raise concerns about constitutionality under the Dormant Commerce Clause. They will only grow as other states follow California's example and create a patchwork of state and local data privacy laws that could provide significant disruption to one of America's key industries.

Some people argue that the benefits of privacy legislation are worth some reduction in economic activity or innovation, but it's important to recognize that these things are difficult to measure and compare. The incalculable benefits of privacy legislation also involve tradeoffs to other intangible values — such as free expression — and should be carefully considered. For example, privacy laws often result in free speech concerns either due to content-based restrictions on commercial speech or deletion requirements, such as a "right to be forgotten," that silence other speakers.

At times, the requirements of data privacy laws may even undermine the privacy they seek to protect. This can happen when companies are incentivized to respond to a request rapidly rather than carefully. One researcher was able to gain significant access to his fiancé's online data by requesting it from companies under the EU's new General Data Protection Regulation.

Even large companies make mistakes under expansive, evolving data protection frameworks and the incentives to act they create, like when Amazon sent 1,700 Alexa recordings to the wrong person following a GDPR request. Dealing with a patchwork of state laws with different timelines and enforcement requirements makes similar mistakes practically inevitable.

Many Americans are confused or concerned about their data these days. The state-by-state, patchwork approach starting with the CCPA is only likely to further that confusion for both consumers and innovators. The internet by its very nature is an interstate tool, and a single interaction can easily involve multiple states. In some cases, the most stringent laws will simply trump the more permissive ones. In others it may be impossible to comply with both laws if, for example, one state requires users to opt-in to data collection while the other requires that users have the ability to opt-out.

The CCPA is set to go into effect on Jan. 1 and become enforceable on July 1. As the clock ticks towards 2020, the potential consequences become more of a reality. It's not the end of the debate over data privacy, but rather a reminder of the risks and disruptions that a state-driven approach will have on consumers and innovation.

Without federal preemption, the U.S. approach to data privacy may see its changes come from Sacramento rather than Washington.

With significant costs and other consequences for both consumers and innovators, policymakers should carefully consider what such a shift might mean before rushing to follow California and Europe's lead.

Jennifer Huddleston is a research fellow with the Mercatus Center at George Mason University. She has a JD from the University of Alabama School of Law and a BA in political science from Wellesley College.

TAGS CALIFORNIA DATA PRIVACY PRIVACY LAW DATA SECURITY DIGITAL RIGHTS CALIFORNIA CONSUMER PRIVACY ACT GENERAL DATA PROTECTION REGULATION CONSUMER PRIVACY

MERCATUS CENTER
George Mason University

The State of State Data Laws, Part 1: Data Breach Notification Laws

Wednesday, July 31, 2019

Authors: Jennifer Huddleston

A few weeks ago, Equifax settled with federal and state regulators to pay up to $700 million [1] in damages and penalties from the 2017 data breach involving the personal information of millions of Americans.

This is far from the only time data security and privacy have been in the news. Just this week, Capital One announced a major breach [2] that exposed the data of 106 million customers and applicants. From privacy for social media and search to security for government organization and infrastructure, it seems hardly a week goes by without a data-related scandal.

While Congressional lawmakers debate possible federal legislation on data privacy and security, some states are pursuing their own new policy actions. Lacking a federal law, the current patchwork of state laws has both benefits and shortcomings.

This piece, focusing on data breach notification laws, is the first in a series examining state actions and debates on data issues, as well as the potential benefits or consequences (or both) of a state-level approach to these issues. Future essays will consider state-level general consumer data privacy laws, state policies concerning specific types of information such as biometrics, and regulations concerning government data security and use of data.

The news of Equifax-like breaches often worry customers about adverse financial consequences such as identity theft. Some legal scholars argue that *any [3]* breach harms users [3], regardless of whether the exposed data are abused by malicious actors or not. Either way, data breach notification laws that require companies to tell customers when data have been exposed are intended to enable consumers to make choices about what to do when such events happen and protect themselves if their information was compromised.

Beginning with California in 2003, all 50 states [4] have enacted some form of data breach notification laws. This approach means consumers will be notified in the event that certain information is wrongly exposed. However, these laws vary significantly [5] on important factors including: who is covered, what data are covered, how notifications should occur, and how long the breached entity has to provide that notification. In general, however, these laws are an important step in empowering consumers to take appropriate action based on their own level of concern following a breach.

While these laws help provide awareness for affected consumers, they are not without their own potentially adverse consequences. For example, as Andrea O'Sullivan has pointed out [6], basing notification windows on when a company learns of a hack could actually discourage better

cybersecurity by dissuading the use of more active monitoring techniques that might make a company aware of a hack sooner.

Additionally, if consumers continually get notifications about breaches, fatigue [7] may set in and consumers may become complacent about best practices after a breach, such as changing passwords or checking their credit reports.

The patchwork approach also has its own unique consequences for innovators and consumers. Companies subject to multiple state laws may find it easiest to comply with the most restrictive law rather than develop different [8] systems or standards for each variation. Consumers may also be uncertain regarding their rights under different statutes [9].

Attempts to create a federal data breach law to harmonize this patchwork have been unsuccessful. State policymakers or enforcers [10] often wish to retain and expand the specifics of their own policy rather than succumb to federal preemption. States that are more restrictive rarely want to agree to a solution that would reduce what they view as necessary protections. A poor federal policy could, in fact, make things worse by accidentally creating a mosaic of the worst elements of different policies in an effort to protect various states' interests.

The current state-by-state approach to data breaches illustrates that while a patchwork may provide a solution, it can also create additional problems for both consumers and covered entities. Still, states have successfully provided notification requirements so that all consumers can determine appropriate next steps.

While a federal approach might be preferable in providing certainty and uniformity, it might also exacerbate unintended consequences for cybersecurity, consumers, and innovators. Policies at any level need to consider how to balance the needs and choices of consumers with the incentives and realities of innovators subjected to these regulations.

Photo credit: Drew Angerer [11]/Getty Images.

Links
[1] https://www.cnn.com/2019/07/22/tech/equifax-hack-ftc/index.html
[2] https://www.wsj.com/articles/capital-one-breach-casts-shadow-over-cloud-security-11564516541
[3] https://www.lawfareblog.com/standing-data-breach-actions-injury-fact
[4] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[5] https://www.jacksonlewis.com/publication/state-data-breach-notification-laws-overview-patchwork
[6] https://reason.com/2017/09/26/would-data-breach-notification-laws-real/
[7] https://www.abc.net.au/news/science/2018-07-06/data-breach-fatigue-ticketmaster-ticketfly-linkedin/9943720
[8] https://www.americanactionforum.org/research/preventing-privacy-policy-from-becoming-a-series-of-unfortunate-events/
[9] https://iapp.org/news/a/if-not-all-data-breaches-are-created-equal-why-are-all-data-breach-notifications-treated-the-same/
[10] https://jolt.law.harvard.edu/digest/coalition-of-32-state-ags-outline-opposition-to-federal-

preemption-of-state-data-breach-notification-laws
[11] https://www.gettyimages.com/search/photographer?family=editorial&photographer=Drew+Angerer

https://www.mercatus.org

MERCATUS CENTER
George Mason University

The State of State Data Laws, Part 2: Consumer Data Privacy Legislation

Tuesday, August 6, 2019

Authors: Jennifer Huddleston

Many states are not waiting for the federal government to take action on data privacy. California was the first to take matters into its own hands by passing the California Consumer Privacy Act (CCPA) [1], which is set to go into effect in January 2020 and will become enforceable later that year. In their 2019 legislative sessions, Nevada and Maine also passed consumer data privacy legislation, and numerous other states have considered similar laws [2].

The first piece [3] in this series discussed how states have created a patchwork of data breach notification laws as a next best alternative to a federal solution. However, another emerging patchwork [4] of broader CCPA-like data regulations would introduce more problems and disruptions. Such an approach could fail to solve actual problems and instead could balkanize the internet and undermine many of the benefits of its borderless nature.

Most of the consumer privacy bills introduced so far are modeled after the CCPA. Yet, these proposals do not just copy and paste the text of the CCPA, and the differences are significant.

For example, Maine's legislation [5] only applies to internet service providers. Other state proposals [2] have gone so far as to seek to regulate the collection of consumer data, but most only focus on the saleor breach of information, or outline what rights individuals have over their data.

Many of these state proposals reflect a shift from an American approach to technology regulation to a more European one. Traditionally, the US has taken a light-touch regulatory stance towards the internet, which largely fueled the Silicon Valley-led digital revolution. These new state laws look more like the EU's General Data Protection Regulation (GDPR), which is typical of the precautionary European posture towards emerging technologies.

Compliance with stringent data requirements is costly for large firms [6]. But for small companies, these regulatory requirements can further hamper their ability to compete and can keep new competitors out.

For example, an economic study [7] found that in the aftermath of the GDPR, venture funding decreased for small and micro companies. This lower investment level likely cost thousands of jobs as well as the potential benefits of innovation.

Following GDPR [8], small advertising players saw their market share shrink. By shrinking, the number of competitors and making it more difficult for new entrants, strict regulation can further enshrine the market power of large players while emerging players struggle to comply or choose to exit the market. Recently, a study by Daniel Castro and Alan McQuinn [9] estimated that imposing a restrictive federal data privacy policy similar to the GDPR or CCPA would cost the US economy $122 billion per year.

The compliance burden of many of these policies would not be limited to tech companies. The CCPA, for example, would apply to many brick-and-mortar business practices such as letting diners make restaurant reservations [10] online due to its definition of household information and data storage.

A state-by-state approach to top-down data regulations would likely impose similar costs and consequences as the GDPR, but in an even more complicated way.

As Federal Trade Commission (FTC) commissioner Christine S. Wilson pointed out in a May 2019 congressional testimony [11], state laws could not only create a patchwork with different requirements, but requirements could be so contradictory that it would be impossible to comply with every state. In some situations, state laws could stifle innovation by making it impossible for the same technology to operate in all 50 states, or by requiring costly state-specific versions that may or may not be interoperable with one another.

This concern is already starting to be realized. For example, the Maine law has an opt-in framework while California and Nevada are opt-out. These laws have different defaults for consumers meaning that innovators would have to develop to different systems to be able to operate in all states. (For a more in-depth discussion of the problem with opt-in frameworks, see Will Rinehart's piece [12] on this issue.)

Not only could these laws create a patchwork that might limit innovation, state laws might be constitutionally problematic. As I discussed with my colleagues Adam Thierer, Andrea O'Sullivan, and Chris Koopman in comments to the FTC [13] on information harms, broad definitions of harm can create friction between privacy and First Amendment-protected speech.

This can occur no matter what level of government implements policies. Informational harm cases should be carefully limited, and the resulting policies as narrowly tailored as possible.

In some cases, privacy regulations risk either favoring privacy over the speech of another individual or regulating the speech inherent in decisions about what information to carry. The potential impact on First Amendment protected speech should be a consideration in any data privacy regulation, whether at a state or federal level.

State and local level data privacy regulations also raise unique constitutional concerns when it comes to the potential disruption of interstate commerce. State data privacy laws like the CCPA could violate the dormant commerce clause [14] by requiring changes to the system for out-of-state platforms, content creators, and businesses, which places an undue burden on commerce conducted or created by these entities.

The breadth of many of these laws will likely result in regulating the data collection standards for consumers and businesses beyond their borders, either for the ease of compliance or because of the definition of "covered entity." While federal laws would still have to interact and compete with a global regulatory marketplace, it would not raise the same constitutional concerns when it comes to the regulation of interstate commerce.

The CCPA and other potential state laws are driving much of the debate around a possible federal data privacy law. As the effective dates of those laws approach, the concerns about potential disruption grows.

A patchwork of different data policies could create a quagmire that deters innovation and services both within and beyond state borders. These spillover effects are more likely to be seen in broader-reaching approaches, such as the CCPA. While often well-intentioned, the borderless nature of the internet means state regulations could be counterproductive when it comes to achieving a goal of a better data environment.

In the next section of this series, I will examine some of the ways states are dealing with privacy issues for specific technologies like biometrics.

Photo credit: Justin Sullivan [15]/Getty Images

Links
[1] https://oag.ca.gov/privacy/ccpa
[2] https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/
[3] https://www.mercatus.org/state-of-state-data-part-one-breach-notification
[4] https://techliberation.com/2018/08/15/the-problem-of-patchwork-privacy/
[5] http://www.mainelegislature.org/legis/bills/display_ps.asp?ld=946&PID=1456&snum=129
[6] https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law
[7] https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment
[8] https://techcrunch.com/2018/10/09/gdpr-has-cut-ad-trackers-in-europe-but-helped-google-study-suggests/
[9] https://www.itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law?mc_cid=4014b20ad2&mc_eid=db8ecd6bc8
[10] https://www.nrn.com/operations/get-ready-consumer-privacy-mandates-are-coming
[11] https://loadtest.ftc.gov/system/files/documents/public_statements/1519254/commissioner_wilson_may_2019_ec_opening.pdf
[12] https://www.americanactionforum.org/insight/opt-in-mandates-shouldnt-be-included-in-privacy-laws/
[13] https://www.mercatus.org/publications/technology-policy/informational-injury-ftc-privacy-and-data-security-cases
[14] 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
[15] https://www.gettyimages.com/search/photographer?family=editorial&photographer=Justin+Sullivan

MERCATUS CENTER
George Mason University

The State of State Data Laws, Part 3: Biometric Privacy Laws and Facial Recognition Bans

Wednesday, August 7, 2019

Authors: Jennifer Huddleston

Today, you can clock into an office with your fingerprints or unlock your phone with just your face. As such potential applications biometric technologies expand, so do the concerns about how they can be abused, particularly when it comes to privacy.

While federal policy is still at the discussion stage about placing limits on biometric technologies like facial recognition, some state and local governments have already passed rules for biometric data or applications, and others are considering it. Illinois [1], Washington [2], and Texas [3] all have existing laws governing privacy rights for biometric information and its use by private entities. Other states, such as Montana [4], have considered creating similar legislation in the most recent legislative term.

Biometric information is often thought of as particularly sensitive and difficult, if not impossible, to change. Those in favor of regulating such technology often point to the ways in which it could be abused, and call for bans [5] or restrictions [6] on its deployment by certain actors.

However, current biometric privacy laws show that a broad approach to regulating this technology in the name of privacy may have unintended consequences and could remove beneficial uses of the technology as well.

Current state biometric privacy laws have prevented residents from accessing the benefits of certain technologies available in other states. For example, Illinois and Texas residents were unable to use Google Arts & Culture [7]'s "art twin" match. While this may not seem like a real inconvenience, it illustrates how strict interpretation and legal challenge could remove consumers' choice to use benign or beneficial technologies.

Similar applications could help users easily confirm their identity or improve outdated security or attendance systems—that is, unless they live in Illinois or Texas. Innovators may skip those states altogether in favor of a more welcoming regulatory environment.

Discussions of biometric and genetic data privacy can easily conjure dystopian science fiction visions like the film Minority Report [8]. However, focusing on the fears associated with this type of data can lead one to neglect the benefits [9] of these technologies. While critics focus on the potential abuse of this information, technology also has promising private sector applications that could be beneficial as smart door locks that would not require a fumbling for a key or quicker boarding of an airplane.

As with most privacy concerns, consumers have a wide range of preferences when it comes to balancing privacy and the potential benefits of biometrics. In private interactions, different

consumers may make different choices including which companies they are willing to provide information or when allowing access to this data is worth the benefits.

My Mercatus colleague Andrea O'Sullivan discussed [10] how the company Clear tries to provide speedier airport security using biometrics. She observed that some individuals may find the tradeoffs of a more rapid security clearance using biometrics beneficial while others are more privacy-sensitive about giving a private company such information.

Yet, broad laws requiring increasingly formal consent can prevent consumers and businesses from having options and making decisions themselves and innovators may find that it is easier not to offer their product in those states rather than engage in costly compliance.

Recently in Illinois, a court found [11] that it was not necessary under the biometric privacy statute to prove harm had occurred for a lawsuit to proceed against Six Flags for collecting fingerprints from a minor for an annual pass without a parent's consent. Such private rights of action increase liability concerns and could further raise legal costs, particularly for smaller companies.

There are legitimate concerns about the about biometric technologies. Some fear that the state could abuse facial recognition capabilities to further surveillance goals, for instance. This threat is especially acute considering that it has already in some countries with totalitarian regimes [12].

But rather than all-out bans, we should adopt a more targeted approach to address concerns about specific applications that are more prone to abuse. This would avoid many of the unintended consequences discussed earlier.

For example, as Cato scholar Matthew Feeney [13] suggests, governments could consider placing restrictions on things that are the most likely to cause harms to civil liberties or allow state surveillance, like real-time facial recognition tracking. This approach would allow state and local governments to utilize beneficial applications, such as finding missing children with facial recognition, while minimizing potentially abusive applications.

While laws targeting biometrics may appeal to those envisioning a dystopian future, these policies bring adverse spillover effects onto benign applications. As a result, policy makers should carefully consider what limitations on biometric technologies are needed and tailor their policies to address specific concerns.

Photo credit: ERIC PIERMONT [14]/AFP/Getty Images

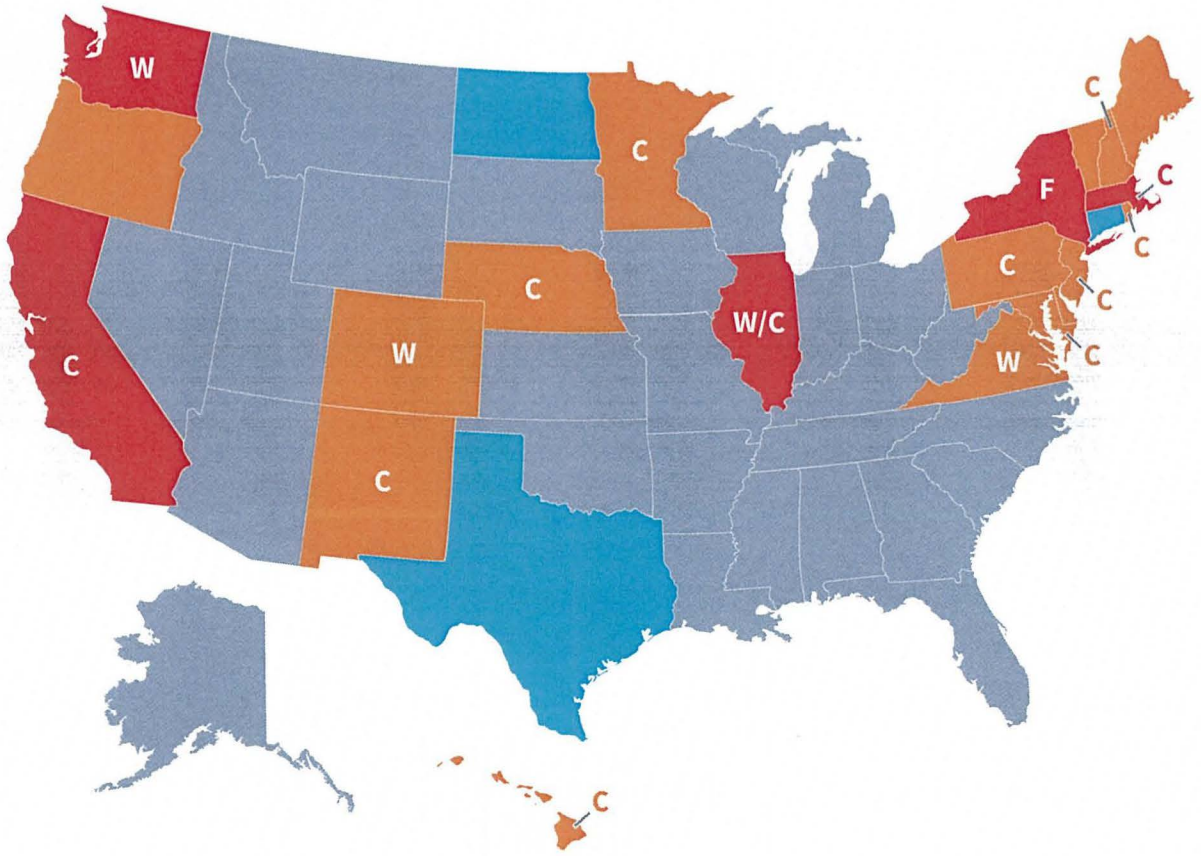
Links
[1] http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57
[2] https://app.leg.wa.gov/RCW/default.aspx?cite=19.375
[3] https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm
[4] https://leg.mt.gov/bills/2019/BillHtml/HB0645.htm
[5] https://ny.curbed.com/2019/7/29/8934279/bill-ban-facial-recognition-public-housing-brooklyn-nyc
[6] https://www.wsj.com/articles/workers-push-back-as-companies-gather-fingerprints-and-retina-scans-11553698332

[7] https://money.cnn.com/2018/01/17/technology/google-arts-culture-not-working/index.html
[8] https://www.entrepreneur.com/article/251627
[9] https://www.mercatus.org/bridge/commentary/great-facial-recognition-technopanic-2019
[10] https://reason.com/2019/02/05/hate-long-tsa-lines-hate-them-enough-to/
[11] https://iapp.org/news/a/illinois-supreme-court-rules-against-six-flags-in-bipa-case/
[12] https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition
[13] https://www.cato.org/blog/should-police-facial-recognition-be-banned
[14] https://www.gettyimages.com/search/photographer?family=editorial&photographer=ERIC+PIERMONT

https://www.mercatus.org

Chamber Technology Engagement Center (C_TEC)

STATE PRIVACY ACTIVITY IN 2020*



Likely to pass privacy law

Will likely introduce privacy bill

Studying privacy legislation

C California Model

W Washington State Model

F Fiduciary Model

*All information subject to change

2020 Legislative Session Dates

California	*January 6 - August 31*
Colorado	*January 8 - May 6*
Connecticut	*February 5 - May 6*
Delaware	*January 14 - June 30*
Hawaii	*January 15 - May 1*
Illinois	*January 8 - TBD*
Maine	*January 8 - April 15*
Maryland	*January 8 - April 6*
Massachusetts	*January 1 - July 31*
Minnesota	*February 11 - May 18*
Nebraska	*January 8 - April 23*
New Hamphire	*January 8 - June 30*
New Jersey	*January 14 - January 10, 2022*
New Mexico	*January 16 - February 20*
New York	*January 15 - TBD*
North Dakota	*Not meeting in 2020*
Oregon	*February 3 - March 7*
Pennsylvania	*January 7 - December 31*
Rhode Island	*January 1 - TBD*
Texas	*Not meeting in 2020*
Vermont	*January 8 - TBD*
Virginia	*January 8 - March 7*
Washington	*January 13 - March 12*

For more information, please contact:

Jordan Crenshaw

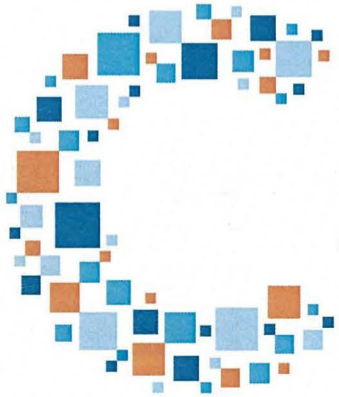
Policy Counsel

Chamber Technology Engagement Center

JCrenshaw@uschamber.com

Chamber Technology Engagement Center (C_TEC)

FEDERAL PRIVACY PROPOSALS



_TEC

U.S. Chamber of Commerce
Technology Engagement Center

For more information, please contact:

Jordan Crenshaw | *Policy Counsel*
Chamber Technology Engagement Center
JCrenshaw@uschamber.com

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Definitions	**Covered Entity**	The term "covered entity" — (A) means any organization, corporation, trust, partnership, estate, cooperative, association, sole proprietorship, unincorporated association, or other entity, over which the [FTC] has authority pursuant to section 5(a)(2) of the FTC Act that processes covered information; (B) ...Common Carriers; and (C)...any nonprofit organization...	The term "controller" means a person that, on its own or jointly with other entities, determines the purposes and means of processing sensitive personal information."	(A)The term "covered entity" means a person who (i) intentionally collects, processes, or maintains personal information; and (ii) sends or receives such personal information over the internet or a similar communications network. (B) EXCLUSION.—The term "covered entity" does not include a natural person, except to the extent such person is engaged in a commercial activity that is more than de minimis.	Any natural person who operates in or affects interstate or foreign commerce.	Any entity or person that is subject to the FTC Act and process or transfers covered data. Covered entity includes any entity or person that controls, is controlled by, is under common control with, or shares common branding with a covered entity.
	Covered Information	The term ""covered information""— (i) means any information about an individual possessed by a covered entity that is linked or reasonably linkable to a specific individual **[or consumer device]** and (ii) does not include (I) information that is processed solely for the purpose of employment by the individual's employer, including any information regarding an individual that pertains to such individual in his or her capacity as an owner, director, or employee of a partnership, corporation, trust, estate, cooperative, association, or other type of entity; (II) deidentified information; **[(III) information that is rendered unusable, unreadable, or indecipherable.]**	Sensitive Personal Information and Non-Sensitive Personal Information	(A) The term "personal information" means any information maintained by a covered entity that is linked or reasonably linkable to a specific individual or a specific device, including de-identified personal information and the means to behavioral personalization created or linked to a "specific" individual. (B) EXCLUSIONS.—The term "personal information" does not include (i) publicly available information related to an individual or (ii) information derived or inferred from personal information, if the derived or inferred information is not linked or reasonably linkable to a specific individual.	• The term "covered data" means information that identifies or is linked or reasonably linkable to an individual or a device that is linked or reasonably linkable to an individual. • Excluded are aggregated data, de-identified data; employee data; and publicly available data.	"Covered Data" means information that identifies, or is linked or reasonably linkable to an individual or a consumer device, including derived data. Excluded are de-identified data, employee data, and public records.
	Sensitive Information		(A) The term "sensitive personal information" means information relating to an identified or identifiable individual, including the following: i. Financial account information. ii. Health information. iii. Genetic data. iv. Information pertaining to children under 13 years of age. v. Social Security numbers. vi. Unique government-issued identifiers. vii. Authentication credentials, such as a username and password. viii. Precise geolocation information. ix. Content of a wire communication, oral communication, or electronic communications with respect to any entity that is not the intended recipient of the communication. x. Call detail records. xi. Web browsing history, application usage history, and the functional equivalent of either. xii. Biometric information. xiii. Sexual orientation. xiv. Religious beliefs. (B) The term "sensitive personal information" does not include (I) de-identified information...(ii) information related to employment; or (iii) publicly available information.	No	• Covered data that describes or reveals the diagnosis or treatment of past, present, or future physical health, mental health, or disability of an individual. • A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account. • Biometric information. • Contents of Private Communications • Account log-in credentials such as user name or email address, in combination with password or security questions to would permit access. • Covered data revealing racial or ethnic origin, or a religion in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information. • Covered data revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information. • Online activities related to sensitive information defined by the Act. • Calendar, address book, phone or text logs, photos or vides on an individual's device. • Categories designated in rulemaking by FTC.	"Sensitive Covered Data" means the following forms of covered data: • A government-issued identifier, such as a Social Security number, passport number, or driver's license number. • Any information that describes or reveals the past, present, or future physical health, mental health, disability, or diagnosis of an individual. • A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account. • Biometric information. • Precise geolocation information that that reveals the past or present actual physical location of an individual or device. • The content or metadata of an individual's private communications. • An email address, telephone number, or account log-in credentials. • Information revealing an individual's race, ethnicity, national origin, religion, or union membership in a manner inconsistent with the individual's reasonable expectation regarding disclosure. • Information revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding disclosure. • Information revealing online activities over time and across third-party website or online services. • Calendar, address book, phone or text logs, photos, or videos maintained on an individual's device. • A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual. • Any other covered data process or transferred for the purpose of identifying sensitive data defined by Act. • Information determined by FTC rulemaking to be sensitive.

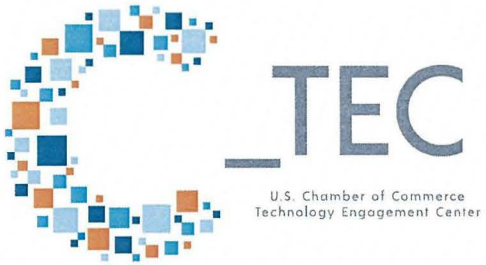
		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Obligations, Consumer Rights and Prohibitions	**Transparency**	Yes	Yes	Yes	Yes	Yes
	Access	Yes	No	Yes (Categories of Personal Information and Content of Communications)	Yes	Yes
	Correction	Yes	No	Yes	Yes	Yes
	Deletion	Yes	No	Yes	Yes	Yes
	Portability	No	No	Yes	Yes	Yes
	Fiduciary Duty	No	No	No	No	Yes
	AI Specific or Right to Human Review of Automated Decision Making	No	No	Right to Human Review	Study	Required Impact Assessment for algorithmic decision-making for housing, education, employment or credit.
	Reasonable Basis	No	No	Required for collection, processing, disclosure and maintenance of personal information	No	No
	Opt-In	Data Processing Not Consistent with Reasonable Expectations	Any functionality that involves the collection, storage, processing, sale, sharing, or other use of sensitive personal information	• Behavioral Personalization • Data Retention • Disclosure or Sale • Collection, Processing, Maintenance, and Disclosure personal information that creates or increases the risk of foreseeable privacy harms	Processing of and Transferring of Sensitive Covered Data to Third Party	Processing and Transfer of Sensitive Covered Data
	Opt Out	First Party Marketing	Any collection, storage, processing, selling, sharing, or other use of non-sensitive personal information	No	No	Transfer of Data to Third Parties

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Obligations, Consumer Rights and Prohibitions (continued)	**Misc. Prohibited Practices**	• Collection Under False Pretenses • Processing of Biometrics • Processing of Attribution of Devices to Individuals with Probabilistic Methods • Processing of Covered Information obtained through microphone or camera • Processing of Contents of Communications • Processing of Health Information	No	• Disclosing Personal Information with intent to threaten, intimidate, or harass any person, incite or facilitate the commission of a crime of violence, or place any person in reasonable fear of death or serious bodily injury • Disclosure to entities not subject to United States jurisdiction or not Compliant with the Act • Reidentifying personal information • Deceptive Notice and Consent Processes and Privacy Policies • Collection, Processing, Maintenance, or Disclosure of Genetic Information subject to exceptions • Collection, Processing, and Disclosure of Contents of Communications	No	No
	Data Minimization	No longer than reasonably necessary for purposes information originally processed	No	• A covered entity shall not maintain personal information for more time than expressly consented to by an individual whose personal information is being maintained • Covered entities may not collect, process, disclose, or maintain personal information for more than reasonably necessary	Entities Shall not Collect, Process, or Transfer covered data beyond what is reasonably necessary, proportionate, and limited to provide or improve a produce, service or a communication about a product or service, including what is reasonably necessary, proportionate and limited to provide a product or service specifically requested by an individual or reasonably anticipated within the context of the covered entity's ongoing relationship with an individual; OR What is reasonably necessary, proportionate, or limited to otherwise process or transfer covered data in a manner that is described in the required privacy policy	A covered entity shall not process or transfer covered data beyond what is reasonably necessary, proportionate and limited to specific processing purposes and transfers described in required privacy policy, where the covered entity has affirmative express consent or explicitly excepted by the Act
	Discrimination	Race, color, religion, national origin, sex, age or disability	No	No processing of personal information or contents of communication for advertising, marketing soliciting, offering, selling, leasing, licensing, renting or otherwise commercially contracting for employment, finance, health, credit, insurance, house, or education opportunities that discriminates against a protected class.	No	A covered entity shall not process or transfer covered data on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income or disability for advertising, marketing, soliciting, offering, selling, leasing, licensing, renting or commercially contract for housing, employment, credit, or education opportunity in a manner that unlawfully discriminates or segregates or discriminates place of public accommodation

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Obligations, Consumer Rights and Prohibitions *(continued)*	**Pricing and Service Differences**	Prohibition on Take-It-Or-Leave it and Financial Incentives	No	No	Covered entities may not deny goods or services because of the exercising of privacy rights	Generally, Covered entities cannot condition provision of service or product to an individual on the individual's agreement to waive privacy rights with some exceptions
Accountability	**Privacy Program**	Yes	No	No	Yes	Yes
	Audit Requirement	No	Yes	No	Required Privacy Impact Assessment	No
	Privacy/ Security Officer Requirement	Both	No	No	Both	Both
Security	**Data Security**	Requires reasonable administrative, technical and physical security measures, polices, practices and procedures.	No	• Covered entities must establish and implement reasonable information security policies, practices, and procedures for the protection of personal information collected, processed, maintained, or disclosed. • Must notify Agency within 72 hours of awareness of data breach or data sharing abuse.	Covered entities must establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect against risk to the confidentiality, security, and integrity of sensitive covered data	A covered entity shall establish, implement, and maintain reasonable data security practices to protect the confidentiality, integrity, and accessibility of covered data. Such data security practices shall be appropriate to the volume and nature of the covered data at issues. Practices should include a vulnerabilities assessments, information retention and disposal, and training
Misc. Industries	**Service Providers and Processors**	Covered entities may only disclose covered information to processors with a written agreement limiting processing	Service Provider with contract limiting processing not considered a third party	Service providers are not third parties if they have a contract limiting processing, do not directly collect personal information, and only derive revenue form processing for covered entities, do not disclose personal information to third parties, do not provide targeting, and do not link information from covered entity to another source.	• Service Providers are Not Third Parties • Service providers are exempt from access, deletion, correction, and portability rights.	• Service Providers are not third parties so long as their processing or transferal relates to the performance of service on behalf or direction of covered entity. • Service Providers are exempt from access, transparency, deletion, correction and individual control rights.
	Data Brokers	Public identification as data broker, auditing, and FTC registry	No	No	Registration with FTC	No

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Misc. Industries *(continued)*	**Small Business Relief**	Small businesses that have an **[annual gross revenue or less]**, process covered information of fewer than **[50,000]** individuals, **[and derives less than 50 percent of its annual revenues from selling consumers' personal information]** alone or in a group may apply to the FTC for self-regulatory safe harbors.	Audit exemption of controllers who collect, store, process, sell, share, or otherwise use sensitive personal information relation to 5,000 or fewer individuals	Small businesses are defined as covered entities that do not earn revenue from the sale of personal information; earn less than half of annual revenues from the processing of personal information; have not maintained over the last six month personal information of over 250,000 individuals; have fewer than 200 employees; and receive less than $25M in annual revenue. Small businesses are exempted from access, correction, portability requirements and can follow approved safe harbor programs for larger companies.	Small businesses that in the previous three years did not exceed a gross revenue of $25M, or process covered data of 100,000 more individuals or devices, or derive 50 percent or more of their revenues from data sales are exempted from access, correction, deletion, minimization, and portability rights.	Small businesses which over the past three calendar years that do not maintain annual average gross revenues exceeding $25M, annually process the covered data of an average of 100,000 or more individuals, h households or devices; AND derive 50 percent or more of their annual revenue from transferring individuals' covered data are exempted from the Act.
	Children's Privacy	**Bracketed**	Information pertaining to children under 13 considered sensitive personal information	No	No	No
Enforcement Issues and Effective Date	**Enforcement Agency**	FTC with new Bureau of Privacy	FTC with additional 50 full-time staff and $35M in appropriations	United States Digital Privacy Agency led by appointed Director	FTC	FTC with new privacy bureau
	Safe Harbor	See Small Business Relief	No	• Safe harbor program for disclosing personal information to entities outside United States jurisdiction • Disclosure of Contents of Communications for Service Providers • Genetic Information Processing and Disclosure for Service Providers • Agency-approved "notice and consent" safe harbor	FTC-approved certification programs create deemed compliance	
	Expanded Penalty Authority	Civil Penalties	No	• Criminal penalties for disclosure with intent to harm (fine or 5 years in prison) • Civil Penalties with Maximums • Rescission or Reformation of Contracts • Refund of Moneys • Restitution • Disgorgement • Damages • Limits on Activities • Public Notice of Violations	No	No
	State AG Enforcement	Yes	Yes	Yes	Yes	Yes
	Rulemaking	Yes	Yes	Yes	Yes	Yes

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Enforcement Issues and Effective Date *(continued)*	**Private Right of Action**	**Bracketed**	No	Injunctive Relief and Damages	No	Yes
	Effective Date	**Bracketed**	180 days after enactment	1 year after enactment	2 years after enactment	180 days after enactment



For more information, please contact:

Jordan Crenshaw | *Policy Counsel*
Chamber Technology Engagement Center
JCrenshaw@uschamber.com

Gabby Reed, Manager
State Government Affairs – Rocky Mountain Region

RELX Group

Elsevier
LexisNexis Legal & Professional
LexisNexis Risk Solutions
Reed Exhibitions

January 13, 2020

The Honorable Scott Louser
North Dakota State Capitol
600 East Boulevard
Bismarck, ND 58505-0360

Re: the study of protections, enforcement, and remedies regarding the disclosure of consumers' personal data

Dear Chairman Louser:

I am writing on behalf of RELX and LexisNexis to outline some critically important items for consideration as the Interim Commerce Committee moves forward with the study of protections, enforcement and remedies regarding the disclosure of consumers' personal information. The subject of consumer data privacy is extremely complex and RELX/LexisNexis commends the committee for attempting to tackle this complicated and multi-faceted issue.

LexisNexis is a division of RELX and is recognized as a leading provider of authoritative legal, public records, and business information which helps our customers make informed and accurate decisions. LexisNexis is the nation's leading provider of credential verification and identification services for Fortune 1000 businesses, government and law enforcement agencies, and the property and casualty insurance industry. LexisNexis plays a vital role in supporting government, law enforcement, and business customers who use our information services for important uses including: detecting and preventing identity theft and fraud, finding deadbeat parents or missing children, locating suspects, and preventing and investigating criminal and terrorist activities.

This letter only includes substantive feedback on HB 1485, as originally proposed during the 66th legislative session. If any other proposal was to be considered for approval by the committee, RELX would require an opportunity to evaluate that language and provide specific feedback as well. Thus far, no state, except for California, has passed an omnibus consumer data privacy bill which indicates the difficulty and complexity of the topic. At this time, the final impact of the California law remains unknown as businesses await final regulations from the Attorney General's Office and the outcome of a newly filed ballot initiative that would implement even further changes to the 2018 law. Not accounting for final regulations and the new ballot initiative, the estimated cost of implementation is over $65 billion. Also, important to note are the difficult negotiations that continue to take place in Washington regarding provisions of an omnibus privacy bill. HB 1485, as originally proposed during the 66th legislative session, was based on a Washington draft that is no longer the primary vehicle being considered. Furthermore, the federal government has made meaningful progress on consumer data privacy with the introduction of two bills in the U.S. House and U.S. Senate which share more commonalities than differences. North Dakota has a unique opportunity to observe how consumer data privacy efforts, both at the federal and state level, move forward in 2020 and delay consideration of a specific proposal until the 2021 legislative session with these efforts in mind. RELX encourages the committee to take this course of action and remains committed to assisting the committee on this critically important topic.

***

RELX Inc. Denver, Colorado Telephone: 202.403.7893 Gabby.Reed@relx.com
www.relx.com

Overall, any legislation concerning consumer data privacy will have a material impact on entities that collect and process personal data both within the state and across state borders. For this reason, please consider the following issue that must be addressed before passing and implementing a comprehensive consumer data privacy law:

Adequate Provisions to Retain the Ability to Combat Waste, Fraud, Abuse, and Identity Theft:

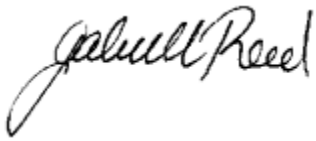
As drafted and proposed during the 66th legislative session, House Bill 1485 will incentivize would-be criminals and identity thieves to restrict their personal data from being processed which will have significant downstream effects because personal data on these individuals will no longer be provided to law enforcement agencies, government agencies, and other entities that utilize third-party products and solutions to identify fraudulent activity.

Although unintended, House Bill 1485 will likely result in increased instances of identity fraud. Once a consumer has objected to a controller processing their personal data, a fraudster will have an easier time fraudulently using such consumer's identity to obtain goods and services, as merchants will no longer be able to use identity verification tools effectively to confirm that the purchaser is who they say they are. Although HB 1485 contains an exemption for controller's or processor's to "Prevent or detect identity theft, fraud, or other criminal activity or verify identities", the exemption does not extend to third party companies that provide essential information to law enforcement, government agencies, or other parties for their efforts to comply with the law or prevent fraud or other criminal activity. As an example, RELX would not be able to share information with banks for anti-money laundering purposes where a consumer has objected to processing, because it is the bank's (controller's) legal obligation that is covered by the exemption and not a third party. Under this scenario, banks themselves do not possess all the data needed to comply with "know your customer" rules without third party data for comparison. Additionally, many programs and services have eligibility and verification requirements that government entities must comply with before providing funds or services or they will be in violation of federal and state regulations. In many instances, third parties often provide the data necessary for staff to authenticate identities to help ensure program integrity within the prescribed rules and regulations.

***

Thank you for your consideration of RELX's comments as the committee continues the study of protections, enforcement and remedies regarding the disclosure of consumers' personal information. Should you have any questions, please do not hesitate to contact me either via e-mail at gabby.reed@relx.com or at 202-403-7893.

Sincerely,



Gabby Reed
Manager, State Government Affairs - Rocky Mountain Region
RELX Group

CC: Senator Shawn Vedaa, Vice Chairman, Interim Commerce Committee
Senator Randy Burckhard, Member, Interim Commerce Committee
Senator Jim Dotzenrod, Member, Interim Commerce Committee

Gabby Reed, Manager
State Government Affairs – Rocky Mountain Region

Elsevier
LexisNexis Legal & Professional
LexisNexis Risk Solutions
Reed Exhibitions

Senator Scott Meyer, Member, Interim Commerce Committee
Senator Ronald Sorvaag, Member, Interim Commerce Committee
Representative Pamela Anderson, Member, Interim Commerce Committee
Representative Thomas Beadle, Member, Interim Commerce Committee
Representative Claire Cory, Member, Interim Commerce Committee
Representative Terry Jones, Member, Interim Commerce Committee
Representative Jim Kasper, Member, Interim Commerce Committee
Representative Jeffery Magrum, Member, Interim Commerce Committee
Representative Corey Mock, Member, Interim Commerce Committee
Representative Mike Nathe, Member, Interim Commerce Committee
Representative Emily O'Brien, Member, Interim Commerce Committee
Representative Shannon Roers Jones, Member, Interim Commerce Committee
Representative Randy Schobinger, Member, Interim Commerce Committee
Representative Denton Zubke, Member, Interim Commerce Committee

RELX Inc. Denver, Colorado Telephone: 202.403.7893 Gabby.Reed@relx.com
www.relx.com

American Property Casualty Insurance Association
INSURING AMERICA apci.org

Privacy

Executive Summary

State legislatures and Congress are rushing to consider comprehensive privacy bills based on the California Consumer Privacy Protection Act (CCPA) and the European Union's General Data Protection Regulation (GDPR). Insurers are already subject to robust state and federal sector-specific privacy regulations However, insurers would be swept into most of the proposed reforms, potentially losing long-standing exemptions for legitimate business activities.

Ideally, insurers want to create a partnership with their customers based on trust and collaboration. Through collaboration insurers get information to perform legitimate and necessary business functions and customers benefit from better products and services. To facilitate this ideal, workable privacy and data security standards are critical. Insurers also want to retain our current exceptions in existing privacy laws and limit enforcement and liability to actions by our state insurance regulators.

Current Realities & Future Challenges

Insurance companies rely on data to execute core business functions, i.e. risk-based underwriting and ratemaking decisions, claims handling, fraud prevention, marketing, litigation management, and consumer product development. Insurers often work with affiliates and third-party vendors to perform these legitimate functions. Historically, the United States has taken a sectoral approach to privacy. However, recent adoption of the GDPR and CCPA along with high profile privacy scandals – in particular, at relatively unregulated technology firms – have led to the introduction of comprehensive privacy bills by states more broadly.

At that same time that privacy activists are advocating comprehensive legislation, numerous business trade associations are seeking federal legislation to override the developing patchwork of state laws. Responding to these concerns, comprehensive and uniform privacy rules have also become a priority for the current Congress and Administration. Similarly, insurers prioritize the need for uniform laws, because focusing on detailed nuances and competing obligations compromises the very security that legislatures intend to protect and distracts from developing solutions for the real privacy concerns. It is important to note that the uniform standard must be a workable standard that appropriately balances legitimate and necessary business functions with consumer protection.

For more information, please contact Steve Schneider 312.782.7720 steve.schneider@apci.org

7.10.2019