SIIA ISSUE BRIEF

Preemption and Privacy:
Primer on Legal and Policy Considerations

DEVELOPED BY THE PUBLIC POLICY DIVISION OF THE
SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

Contents

Executive Summary

In the late 19th century, Samuel Warren and Louis Brandeis published the "Right to Privacy," articulating for the first time in the United States a privacy right, defining it as the "right to be let alone." Over the next nearly 130 years, U.S. law on privacy continued to develop through common law torts, constitutional interpretation, the implementation of the Fair Information Practice Principles, and the development of federal and state sectoral privacy law. Despite being a global leader on privacy, however, the U.S. never developed a comprehensive federal privacy law to regulate the commercial use of information, or data; instead enacting laws to protect particularly sensitive personal data privacy, such as financial, health, and children's information. The rest of the world, in contrast, began regulating information privacy as a comprehensive national concern. This national-level comprehensive approach corresponded with the enormous growth of the global digital economy, spearheaded by the commercial Internet and unprecedented global connectivity. Suddenly, data, which lacks any intrinsic value, became valuable based on how it could be processed to generate value. Now, data is integral to our national economy, the global economy, and trade.

The Software Information & Industry Association (SIIA) has joined the call for robust privacy legislation that harmonizes U.S. privacy law and provides meaningful consumer protections and individual rights (such as the rights to notice, access, control, correction, portability, and in some instances, deletion). This Issue Brief focuses on one aspect of the national information privacy debate, which is why a law that harmonizes the U.S. approach to information privacy is critical to our global leadership, the promotion of our national economy and the global economy, and to ensure equal and strong consumer protections. The brief is organized as follows:

First, the brief analyzes why the regulation of personal data is a matter of national and global economic concern due to unprecedented global connectivity, the value of cross-border data flows, and its implications for digital trade. The brief then narrows in on the national economic impact because federal privacy legislation will regulate beyond tech, impacting traditional businesses and small- and medium-sized enterprises (SMEs). This section illustrates the incontrovertible impact of data on our national economy and the global economy. It concludes by:

- urging Congress to counteract potential harms to SMEs and the global economy and our national economy by enacting a harmonized data privacy standard for the benefit of our economy, consumers, and innovation.

Second, and against the backdrop described above, the brief discusses why federal privacy law should preempt state law. The preemption doctrine is generally used to provide uniform rules for areas of national (and international) import, and it is critical that policymakers consider preemption when drafting legislation, even if they do not concede their support for preemption until a bill is ready for vote. A well-crafted preemption provision can ensure that the federal privacy law provides equal protections for all consumers, irrespective of their state of residence, while leaving intact state laws which regulate personal data (directly or indirectly) that have a uniquely local concern and execute the state police powers. The brief concludes by:

- identifying the types of state laws a federal privacy law should exclude from preemption (including consumer protection laws except to the extent they are enforced to regulate personal data; criminal laws; laws relating to wiretapping, the protection of Social Security numbers, identity protection, or student privacy; and state constitution, contract, and tort laws), and the expectation that any preemption provision will retain the federal sectoral model, including some state laws that are permitted by the savings and preemption clauses of those federal sectoral laws; and

- discussing the unique concerns that children's and students' privacy present, with the Children's Online Privacy Protection Act's express preemption provision and the uniquely local concerns surrounding student privacy.

Finally, we conclude the brief with an in-depth and technical analysis of language Congress can use to pinpoint its preemption intention through a combination of express preemption and savings clauses. This section draws on preemption and savings provisions included in two legislative proposals: the Information Transparency & Personal Data Control Act (H.R. 2013) and the Intel Privacy Bill. Using these proposals, along with research recently released by the Congressional Research Service, we explain how these models leave significant room for state regulation while harmonizing information privacy generally. Although broadly agreeing with the provisions articulated by these legislative proposals, the brief suggests:

- how Congress may further clarify the provisions to ensure the law (1) excludes from preemption all state and local consumer protection laws (except to the extent they regulate personal data collection and processing), (2) unambiguously saves state constitutional, trespass, contract, or tort law except to the degree the law is enforced to govern personal data collection and processing, and (3) protects state laws

banning revenge pornography (unless the federal privacy law includes a provision regulating this at the federal level).

- that Congress consider inserting an expanded savings clause to clarify its intent that the federal privacy law does not supersede the federal sectoral privacy laws, as well as other privacy laws relating to how public entities (such as government agencies) collect and process personal data.

Introduction

In *McCulloch v. Maryland,* Justice Marshall wrote of the Supremacy Clause: "If any one proposition could command the universal assent of mankind, we might expect it would be this – that the Government of the Union, though limited in its powers, is supreme within its sphere of action. . . It is the Government of all; its powers are delegated by all; it represents all, and acts for all."[1] These words form the basis of the constitutional doctrine of preemption, which has evolved over time to address American federalism and the growth of our national economy. Under the modern doctrine, the intent of Congress to preempt is preeminent. Congress may displace state laws at will, provided that it is acting within one of its constitutionally enumerated powers, such as the constitutional authority for Congress to regulate interstate commerce to protect and unify our national marketplace.

As one mechanism of organizing our federalist system, preemption exists "against a backdrop of shared assumptions," one of which is that "'our economic unit is the Nation.'"[2] Nevertheless, questions of preemption, including the judicial review of Congress's legislative intent to preempt, are rarely easy. Preemption questions must also be balanced against other legitimate concerns, including how to adhere to our foundational federalist principles, the policy objectives and strength of the federal legislation at hand, political ideology, the careful balancing and trade-offs of competing policy objectives, and canons of statutory construction.

All of these issues are in play as the 116th Congress considers the federal personal information privacy question and whether a federal framework can and should preempt state law. As we reach consensus amongst most stakeholders on the need for baseline federal legislation, the remaining divergences are primarily focused on the details of the legislation itself, including the role of the states after Congress acts. On one side of the debate are stakeholders and policymakers who fear that preemptive federal legislation will quash stronger state information privacy standards and individual remedies. On the other side, are those who foresee the balkanization of state privacy standards, and the unintended consequences that flow therefrom, including: disparate and unequal protections for

[1] *Id.*, 17 U.S. 316, 406 (1819).
[2] Thomas W. Merrill, *Preemption and Institutional Choice*, 102 Nw. U. L. Rev. 727, 745 (2008) (quoting *H.P. Hood & Sons, Inc. v. DuMond*, 336 U.S. 525, 537 (1940)). Merrill identifies three other assumptions, including that (1) "state governments are the locus of general sovereignty in the American federal system," (2) "Congress is the critical institution in determining whether to activate federal authority," and (3) "federal power, once activated, is paramount to the authority of the states." *Id.* at 745-46.

Americans, contradictory regulatory standards, economically infeasible compliance costs, regulatory barriers to entry and competition, disincentives for innovation and growth, and state-level regulation of the national and international data market, including cross-border data flows and the resulting need for interoperability.

This Issue Brief weighs in on the critical importance of Congress passing comprehensive federal privacy legislation that sets a ceiling standard for the commercial collection and processing of personal data. Our views are premised on the assumption that such legislation will set forth strong regulatory requirements. Provided Congress can identify and agree on these maximum standards for information privacy, preemption of the field is the only viable choice to ensure equality, uniformity, and the protection of our economy.

We begin this Issue Brief by explaining why the regulation of personal information privacy is a national and global market concern, and thus, demands preemptive action by Congress. Next, we provide an overview of the modern preemption doctrine, the importance of express congressional intent, and why Congress should expressly preempt state information privacy laws. Last, we set forth recommended considerations for Congress for an express preemption provision, drawing from an excellent primer on preemption recently published by the Congressional Research Service, and using legislation and a draft industry bill as models for discussion.

Information Privacy Regulation Is a National and Global Market Concern

Personal data is one component of the "knowledge economy," which "has been recognized for years as a critical driver of economic growth and productivity."[3]

Although the decision to preempt rests within the discretion of Congress, whether to exercise that discretion (and when it is appropriate to do so) often turns on whether regulatory uniformity is critical to our national economy. We start, therefore, by examining the intersection of information privacy regulation with our national economy and the global economy, and assessing the importance of commercial data practices to trade and continued

[3] Silja Baller, Soumitra Dutta, and Bruno Lanvin (Eds.), *The Global Information Technology Report 2016: Innovating in the Digital Economy* (Sept. 3, 2019, 2:50 PM), p. 39, http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf.

economic growth. Of particular concern are the impacts on trade and cross-border data flows, our national economy, and small- and medium- sized enterprises (SMEs).

Trade and Cross-Border Data Flows: The Global Economic Impact

How the U.S. regulates information privacy will directly impact the global economy. Cross-border data flows, which information privacy regulation can restrict or promote,[4] "drive about 22 percent of global economic output and will add up to US $11 trillion to global GDP by 2025."[5] This economic growth is driven by unprecedented global connectivity, with "'more than 4 billion Internet users across the planet . . . . generat[ing] close to 2.5 quintillion bytes of data – a figure expected to increase ten-fold in the next five years alone.'"[6] As James Sullivan, the Acting Assistant Secretary for Industry & Analysis at the Department of Commerce, recently noted: "Cross-border data flows are indispensable – not just for big, multinational technology companies, but for traditional industries, and for small- and medium-sized businesses as well."[7] Regulating data through information privacy laws, therefore, is simply not a local concern, but a national concern with global import.

A recent OECD Trade Policy Paper echoes this, noting that the connections between trade and production are inescapable, with both "heavily dependent on moving, storing, and using digital information (data) increasingly across borders."[8] Thus, "while regulations related to privacy and security are not traditionally associated with trade, they *can* have

[4] Casalini, F. and J. López-González (2019-01-23), "Trade and Cross-Border Data Flows," *OECD Trade Policy Papers*, No. 220, p. 8, OECD Publishing, Paris. https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_b2023a47-en.

[5] Lou Mastria, *Summit Snapshot 19L: DC I U.S. Dept. of Commerce Assistant Secretary for Industry & Analysis Sullivan Seeks to Keep Open Global Data Flows with Trading Partners in Privacy-First Age* (Sept. 3, 2019, 2:45 PM), https://digitaladvertisingalliance.org/blog/summit-snapshot-19dc-us-dept-commerce-assistant-secretary-industry-analysis-sullivan-seeks-keep.

[6] *Id.* Other recent reports analyzing historical cross-border data flow statistics further drive home their importance to the U.S. and global economy. In 2016, the World Economic Forum reported that in 2011 digital trade alone was credited with increasing the US GPD to 4.8% from 3.4% and with the creation of 2.4 million jobs, with cross-border Internet traffic increasing 18-fold from 2005 to 2012. *See* fn. 3, at 39-40. More recently, in December 2018, Francesca Casalini and J. López-González reported in an OECD Trade Policy Paper that cross-border data transfers increased 45 times between 2005 and 2014. Casalini and López-González at 9. According to their paper, this translated "into an estimated contribution of USD 2.8 trillion to global economic activity, or 3.5% of global GDP." *Id.* These numbers are slated to only grow in the coming years as "the size of the internet economy is expected to more than double for G20 economies, with even faster growth rates for developing economies." *Id.*

[7] Mastria, fn. 4.

[8] Casalini and López-González at 8.

trade consequences, when, for instance, they affect the movement of data that is critical for the coordination of global value chains or for an SME to trade."[9]

United States trade policy recognizes the national and global impact of digital trade, including cross-border data flows, through trade agreements and support for mechanisms that seek to facilitate data flows across nations with disparate privacy regimes. For instance, the U.S. is one of eight participating economies in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR).[10] The APEC CBPR is a system for facilitating transborder data flows by requiring "participating business to implement data privacy policies consistent with the APEC Privacy Framework."[11] The U.S. also is committed to administering and enforcing the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, which are designed to permit European and American companies "with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce."[12] With respect to trade agreements, the United States-Mexico-Canada Agreement (USMCA) includes a negotiated chapter on digital trade that provides for a binding cross-border data flow obligation, and specifically recognizes the APEC CBPR as a valid mechanism for data flows.[13]

We cannot afford for state privacy regimes to undercut U.S. trade policy and commitments. Privacy regulations directly impact digital trade and cross-border data flows, which are vital to our economic interests and the global economy. When the U.S. government and businesses engage globally, they enter a globally balkanized regulatory field and Internet.[14] This is because we do not have one international standard or answer to information privacy. For the U.S. to compete effectively on a global scale, therefore, we need to operate as one integrated digital economy, not as 50 separate state economies. The European Union recognized the importance of a harmonized information privacy standard when it implemented the General Data Protection Regulation, which preempted unique

---

[9] *Id.* In 2016, for instance, the Global Information Technology Report noted that "61 percent (US$387.7 billion) of total US service exports were digitally delivered in 2012, and 53 percent of total US imports were digitally delivered," with the rates even higher in the European Union. *See* Baller, *et al.* at 39.
[10] CROSS BORDER PRIVACY RULES SYSTEM, http://cbprs.org/.
[11] *Id.*
[12] PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview.
[13] Joshua Harris, *Why CPBR recognition in the USMCA is a significant development for privacy,* IAPP Privacy Perspectives (Oct. 10, 2018), https://iapp.org/news/a/why-cbpr-recognition-in-the-usmca-is-a-significant-development-for-privacy/
[14] *See* fn. 4.

Member State approaches to data privacy regulation under the 1995 Privacy Directive.[15] Moreover, national legislation can ensure that our standard is interoperable with the information privacy frameworks of our most important trading partners and other countries critical to our national industries.

The National Economic Impact

Even looking at the issue from a solely non-trade national perspective, the answer to the data privacy question is critical for continued growth in digital activity generally, and to promote the "emergence of new industries as well as the accelerated development of traditional sectors."[16] Estimates show that massive growth of the global economy, due in large part to the Internet, "impacts all facets of national economies, not just their budding technology sectors" with "an estimated 75 percent of the Internet's benefit [] captured by companies in traditional industries."[17] Even when looking at it through the lens of "big data" alone, the economic impacts are massive. In 2015, for example, an industry study estimated that consumer data collection was a $16.9 billion industry.[18]

The regulation of information privacy – whether at the state or federal level – will impact these national economic concerns because it sets rules of the road for how companies collect and use personal data. Comprehensive regulation of information privacy should govern personal data collection and use across industries and technologies, and thus provide standards for personal data whether the business primarily operates online or offline. In practice, this means that information privacy regulation is not merely the regulation of tech. It also is the regulation of traditional businesses, SMEs, startups, and individual entrepreneurs, all of which rely on the collection and processing of personal data for fulfillment, the flow of supply chains, improvements to products and services, and the innovative development of new technologies. It is unavoidable, therefore, that information privacy regulation will impact businesses that provide Americans with everyday necessities and luxuries, including groceries, coffee, insurance coverage, and medical care.

---

[15] Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (hereinafter GDPR)

[16] Baller, *et al.*, at 39.

[17] *Id.*

[18] Tony Glosson, *Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws*, 67 Fed. Comm. L. J. 409, 411 (Dec. 2015) (citation omitted).

The Economic Impact on SMEs

A recent OECD Trade Policy Paper finds that cross-border data transfers enable "the creation of a new breed of [SMEs], the micro-multinational, which is 'born global' and is constantly connected."[19] The ability to engage in cross-border data transfers, which, as discussed below, is impacted by privacy regulation, benefits the growth of these micro-multinationals because they provide access to services (i.e. cloud computing), reducing the need for costly infrastructure expenditures to support a profitable business model.[20] In addition, this access to data allows SMEs to overcome entrenched hurdles by "reducing barriers to engaging in international trade and allowing them to more readily compete with larger firms."[21]

As our national digital economy and the global economy continues to grow, the question of how to effectively regulate SMEs, particularly those that are "born global," in the privacy space is particularly acute. Information privacy regulation inevitably affects SMEs disproportionately, and a patchwork regulatory model exacerbates this. This is because SMEs, unlike large and established national and international companies, often do not have the resources to hire legal counsel to ensure compliance programs that are effective and adaptable across a patchwork of national privacy regulation.

The costs associated with complying with patchwork regulation are not minor, nor borne entirely by large national and multi-national companies. The IAPP estimates, for instance, that the California Consumer Privacy Act (CCPA) will regulate more than 500,000 businesses, the vast majority of which are SMEs, when it implements next year.[22] The compliance costs associated are high, and will continue to rise as new states enter the regulatory field. For compliance with the CCPA alone, a TrustArc survey of 250 US privacy professionals reveals that the vast majority anticipate spending at least $100,000 on CCPA compliance, with 39% anticipating the costs as high as $500,0000 and 19% expecting to

[19] Casalini and López-González at 14.
[20] *Id.*
[21] *Id.*
[22] Rita Heims and Sam Pfeifle, *New California privacy law to affect more than half a million US companies*, The Privacy Advisor (July 2, 2018), https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/.

spend more than $1 million.[23] These costs, even on the low end, will be difficult for SMEs, including those born global, to bear and run profitably.[24]

Compliance with the CCPA is complex, difficult, and expensive because it will require companies to build tools to map and match data across disparate systems, as well as engage in vendor management to ensure data is compliantly handled downstream.[25] U.S. companies that operate in Europe have a competitive advantage, having engaged in this process as the GDPR was implemented. For all other U.S. companies and particularly for SMEs, however, the compliance costs and processes for the CCPA will scale high. As other states enact comprehensive privacy laws, these companies will have to incur these costs again to comply with the specific requirements in each state and address conflicts between the laws.[26]

Congress can counteract this compliance knot through a unified national law setting forth harmonized standards that balance how to bring SMEs within its scope. It is vital that the United States arrive at a harmonized answer to the data privacy question, rather than relying on patchwork regulation at the state and local levels. Information privacy simply is not a "local" matter.[27]

---

[23] TrustArc, *CCPA and GDPR Compliance Report* (2019), https://download.trustarc.com/dload.php/?f=7OFEDLUL-784

[24] We note that even when state laws intend to exclude SMEs, how to do so has proven illusory. The CCPA is a cautionary tale. There, legislators intended to exempt SMEs from the law's scope, and did so by assigning three thresholds for the Act's coverage: (1) a minimum annual gross revenue amount, (2) a minimum percentage of gross revenues based on selling customers' information, or a (3) minimum annual data threshold for buying, receiving, selling, or sharing the personal information of 50,000 or more consumers, households, or devices. Given the breadth of triggering mechanisms in the last category, along with ongoing ambiguity about how the Act defines "selling," it is unclear how SMEs should calculate their data collection points to determine coverage by the CCPA. What is clear, however, is that a business will fall under the scope of the act with an average of just 136 transactions per day. In addition, this arbitrary and yet ineffective line in the sand will disincentivize business growth, as the costs of the 50,001 data point will bring with it substantial compliance costs.

[25] Jeff Kosseff, *Hamiltonian Cybersecurity*, 54 Wake Forest L. Rev. 155, 183 (2019) (although focusing on the need for a harmonized approach to cybersecurity, Kosseff notes that the CCPA will require many companies "to entirely revamp their data storage and security comply with the new law.")

[26] For a summary of the compliance challenges that companies, big and small, face as the CCPA deadline looms, *see* Patience Haggin, *Businesses Across the Board Scramble to Meet California Data-Privacy Deadline,* The Wall Street Journal (Sept. 8, 2019, 9:00 AM), https://www.wsj.com/articles/businesses-across-the-board-scramble-to-comply-with-california-data-privacy-law-11567947602.

[27] Notably, California recognized the importance of a unified law when the state amended the CCPA to preempt a growing patchwork of local privacy laws. *See* John Stephens, *California Consumer Privacy Act*, American Bar Association (July 2, 2019),

Federal Information Privacy Law Should Preempt State Law

The Hamiltonian concerns about regulations do not arise from them being too onerous; the objections relate to the ability of a single state to regulate out-of-state commerce.[28]

What Is Preemption?

The doctrine of preemption is grounded in the Constitution's Supremacy Clause, which declares federal law as the supreme law of the land.[29] Under the modern doctrine, whether federal law displaces, or preempts, state law turns on congressional intent.[30] In other words, it is within the discretion of Congress to determine the scope of its legislation. In practice, however, the courts are often called on to resolve questions of whether Congress intended to displace state law.[31]

The Supreme Court has developed "two primary branches of preemption – express and implied preemption."[32] Express preemption applies when Congress directly addresses the issue of preemption in federal legislation, either through a provision stating which state laws Congress deems preempted, a savings clause identifying the state laws Congress does not intend to preempt, or both.[33] Implied preemption, in contrast, applies to displace state law when the federal law's "structure and purpose implicitly reflect Congress's preemptive intent."[34] Notably, "the presence of an express preemption clause in a federal statute does not preclude implied preemption analysis."[35]

The Court applies two types of implied preemption – field and conflict preemption. "Field preemption arises when the intent or effect of federal law is to occupy the entire field in an area of law, so as to leave no room for any state regulation in the area."[36] Conflict

---

https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.

[28] Kosseff at 190 (in an article arguing for the need for a national standard for cybersecurity).

[29] Merrill at 733 (citation omitted); Steven Ferrey, *The Supreme Court's Constitutional 'Bright Line': Preempting Authority of 47 of 50 States*, 10 Ne. U. L. Rev. 143, 153-54 (Spring 2018) (citations omitted); Mary J. Davis, *Unmasking the Presumption Against Preemption*, 53 S. C. L. Rev. 963, 973-74 (2002).

[30] Merrill at 740 (noting that the first maxim of modern preemption is that "'[t]he purpose of Congress is the ultimate touchstone' in every preemption case."); citing *Retail Clerks Int'l Ass'n, Local 1625 v. Schermerhorn*, 375 U.S. 96, 103 (1963)). *See also Wyeth v. Levine*, 555 U.S. 555, 565 (2009).

[31] For an excellent primer on the preemption doctrine, *see also* Jay B. Sykes and Nicole Vanatko, CONG. RESEARCH. SERV., R45825, FEDERAL PREEMPTION: A LEGAL PRIMER (2018).

[32] Jesse Merriam, *Preemption as a Consistency Doctrine,* 25 Wm. & Mary Bill Rts. J. 981, 988 (March 2017) (citing *Geier v. Am. Honda Motor Co.*, 529 U.S. 861, 884 (2000)).

[33] *Id.* (citing *Cipollone v. Liggett Grp., Inc.*, 505 U.S. 504, 517 (1992)). *See also* Merrill at 738 (citations omitted).

[34] Sykes and Vanatko at 2.

[35] *Id.* (citing *Geier v. American Hondo Motor Co.*, 529 U.S. 861, 881-82 (2000)).

[36] Merriam at 989 (citing *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947)).

preemption is divided into two parts. The Court finds conflict preemption when either (1) state law directly conflicts with federal law rendering compliance with both laws impossible ("impossibility preemption"), or (2) "state law 'stands as an obstacle' to the accomplishment of federal objectives, and therefore, must yield" ("obstacle preemption").[37]

When resolving questions of preemption, the Court also applies a presumption against preemption.[38] This presumption, which dates back to the Court's 1947 decision in *Rice v. Santa Elevator Corp.*, requires the courts to "start with the assumption that the historic police powers of the States [are] not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress."[39] Scholars note, however, that the Supreme Court has inconsistently applied the presumption against preemption when determining Whether federal law displaces state law.[40] The presumption against preemption, moreover, does not apply in cases involving express preemption.[41]

Why Should Congress Consider Preemption When Drafting Information Privacy Legislation?

Whether Congress should expressly preempt state law is a difficult decision influenced by a number of factors, from political ideology to the quality of the legislation at hand. Members of Congress need not decide their position on preemption until legislation is drafted and ready for vote. Nevertheless, negotiating with preemption on the table is crucial, even if acceptance is not yet conceded. It is the only way to ensure that federal legislation codifies standards strong enough to justify preemption and identifies which state laws should be preempted.

The inherent complexity of information privacy law, and the breadth of state laws relating to privacy, render judicial challenges to the preemptive effect of a comprehensive

---

[37] *Id.* (citing *Wyeth v. Levine,* 555 U.S. 555, 589-90 (2009)) (other citations omitted); Davis at 969-70 (citations omitted).
[38] Davis at 968, fn. 2.

[39] *Id.*, 331 U.S. 218, 230 (1947).
[40] Merrill at 762 (citing *Engine Mfrs. Ass'n v. S. Coast Airl Quality Mgmt Dist.*, 541 U.S. 246 (2004); *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525 (2001); *Buckman Co. v. Plaintiff's Legal Comm.*, 531 U.S. 341 (2001)); S. Candice Hoke, *Preemption Pathologies and Civil Republican Values*, 71 B.U. L. rev. 685, 733, n. 59 (1991)); Davis at 968 (arguing that the Court's presumption against preemption actually operates as a presumption *in favor* of preemption); Merriam at 989-90 (arguing that the preemption doctrine is messy). *See also* Sykes and Vanatko at 3-4 ("The Court regularly appealed to [the presumption against preemption] in the 1980s and 1990s, but has invoked it inconsistently in recent cases.") (citations omitted).
[41] Sykes and Vanatko at 4 (citing *Puerto Rico v. Franklin Cal. Tax-Free Trust*, 136 S. Ct. 1938, 1946 (2016)).

federal privacy law a virtual certainty. With judicial review inevitable, the most effective way for Congress to influence the outcome through precise and explicit statutory language.

Although the Supreme Court's maxims of adhering to congressional intent and applying a presumption against preemption may provide some assurances that a judicial finding of preemption is unlikely without an express statement to preempt in the legislation, review of the case law shows otherwise. As noted above, for instance, an express preemption clause does not foreclose an implied preemption analysis.[42] At a minimum, therefore, Congress must consider that its laws may impliedly preempt state law, even if Congress expressly states its intentions with respect to the preemptive effect of the legislation.[43] Moreover, and as recognized by several scholars, the Court has applied the presumption against preemption inconsistently,[44] and has found congressional intent to preempt state law even when the federal statute contained a savings clause stating otherwise.[45] At least one scholar has argued that in practice the Supreme Court's case law reveals that the Court applies a presumption *in favor* of preemption.[46]

Judicial interpretation of congressional intent can also prove tricky. Although Congress' intent is the "ultimate touchstone" of the Court's preemption doctrine,[47] the Court may look beyond the statute's text when assessing the scope of the intention.[48] Legislative clarity, therefore, is critical when Congress is considering the question of preemption.

This is even more true in the context of information privacy laws, which involve a complex interplay of federal, state, and local sectoral privacy laws, and the growing trend of comprehensive state privacy laws. The federal sectoral laws present unique challenges on their own, with each handling preemption differently. Some set minimum regulatory floors,

---

[42] *Geier v. Am. Honda Motor Co.*, 529 U.S. 681 (2000).
[43] Sykes and Vanatko at 3.
[44] Merrill at 739, 741 (noting that this maxim "is honored as much in breach as in observance."); Davis at 968, fn. 2.
[45] *Id.* (noting that the "Court has insisted that 'the existence of conflict cognizable under the Supremacy Clause does not depend on express congressional recognition that federal and state law may conflict.'") (quoting *Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 388 (2000) (citing, *Buckman v. Plaintiffs' Legal Comm*, 531 U.S. 341, 348, 352 (2001); *Geier*).
[46] Davis at 968 (arguing that the presumption against preemption is not functional and that "[i]t is inescapable: there is a presumption in favor of preemption.").
[47] Sykes and Vanatko at 3 (citing *Wyeth v. Levine*, 555 U.S. 555, 565 (2009) (quoting *Retail Clerks v. Schermerhorn*, 375 U.S. 96, 103 (1963)).
[48] *Id.* (noting that "the Court has also noted the importance of statutory structure and purpose in determining how Congress intended specific federal regulatory schemes to interact with related state laws.") (citing *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 486 (1996); *Wyeth* at 583 (Thomas, J. concurring in the judgment)).

which allow the states to fill in the gaps with stricter standards provided they are not inconsistent with the federal standard (*i.e.* the Gramm-Leach-Bliley Act (GLBA), the Driver's Privacy Protection Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Video Privacy Protection Act). Other laws include express preemption provisions, like the Children's Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act (FCRA), and the CAN-SPAM Act. Adding to this complexity is the range of state and local laws that touch upon privacy, but do not solely address the commercial data privacy questions that we expect federal legislation to cover. These include wiretap laws, consumer protection laws, tort law, and contract law.[49] As Peter Swire notes: "to avoid unintended consequences on other areas of law, a federal privacy preemption provision will need to contemplate interactions with a much larger range of laws than many have realized."[50]

Why Is It Critical that a Comprehensive Federal Privacy Law Preempt State Law?

Information privacy regulation is inherently complex, requiring policymakers to balance the values of individual privacy interests and necessary consumer protections against constitutional principles (like freedom of speech), the interests of our national economy (a large component of which is the digital economy that relies on collection and processing of personal data), our trade obligations and other international agreements, and the ability of U.S. companies to compete globally. It also is inherently a matter of interstate commerce. Congress is uniquely situated to weigh all of these value judgments to arrive at a maximum standard for information privacy that equally protects individuals across the United States, and promotes and protects our national economy and international interests.

National and Global Economic Implications

Let's begin with the national economy and trade interests inherent in the information privacy debate. As explained at the outset of this Issue Brief, the regulation of personal data is incontrovertibly a national and global economy issue. Companies of all sizes, shapes, and sophistication – from true "mom and pop shops" to SMEs to large multinational companies – rely on the ability to collect and process personal data for direct customer service (like fulfillment of goods and service) to backend operations relating to supply chains and the improvement of goods and services.[51] The ability of SMEs to enter the market and compete

[49] Peter Swire, *US federal privacy preemption part 2: Examining preemption proposals* (Jan. 10, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-2-examining-preemption-proposals/.
[50] *Id.*
[51] *See* Baller, *et al.* at 41 (noting that the Business Roundtable identified "at least six different areas of activity whereby firms may transmit data across national borders to support business operations. These include interconnected machinery, big data analytics, back-office consolidation, supply-chain automation, digital collaboration, and cloud scalability.").

with entrenched players is directly correlated to the SMEs' ability to leverage external infrastructure sources, like cloud computing, which rely on the ability to collect and process data within the United States and internationally.[52] Disparate and conflicting information privacy standards at the state level will disrupt these economic activities domestically and internationally.

Relatedly, information privacy regulation impacts trade, as the OECD Trade Policy Paper has pointed out, when the regulation impacts the movement of data. Cross-border data flows are necessary to realize the full economic potential of data-driven innovation and the global economy. As one measurement, the McKinsey Global Institute estimated that in 2014, global data flows raised the global GDP by $2.8 trillion.[53] The ability for companies to transfer data across national borders depends on the interoperability of information privacy regulation between countries. Currently, Europe is leading the charge in setting the information privacy standard through the GDPR, and countries are aligning their privacy laws with it. The result is restrictive adequacy standards for cross-border data flows that complicate how U.S. companies engage around the world.[54] A national federal information privacy standard can, therefore, help the U.S. meet adequacy standards for cross-border data flows with critical trading partners around the world. Moreover, a U.S. federal law would set a powerful example for other countries, many of which currently are relying on the GDPR as a guide.

Consumer Protection Implications

Disparate state regulation of comprehensive information privacy legislation also risks consumer confusion and unequal privacy standards for consumers. Allowing 50 or

[52] Casalini and López-González at 14 ("Data flows allow SMEs to access IT services, such as cloud computing, reducing the need for costly upfront investment in digital infrastructure. This allows them to be more nimble, scaling-up IT functions in response to changes in demand. Better and faster access to critical knowledge and information also helps SMEs overcome information disadvantages, notably with respect to larger firms, reducing barriers to engaging in international trade and allowing them more readily to compete with larger firms.")

[53] SIIA, *Data Flow Promotion in International Agreements and International Law*, ISSUE BRIEF, 2 (November 2018), http://www.siia.net/Portals/0/pdf/Policy/Data%20Flow%20Promotion%20in%20International%20Agreements%20and%20National%20Laws%20SIIA%20Issue%20Brief.pdf?ver=2018-11-14-101028-167.

[54] Matthew Humerick, *The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up To Rising Global Standards?*, 27 Cath. U. J. L. & Tech. 77, 81-82 (2018) ("The European Union is the global standard for international privacy law, and is continuously developing, while the United States continues to embrace an antiquated, ineffective approach. Additionally, with the United States' view towards international cooperation shifting, negotiations will likely become more tense and result in significant delays. For companies, this means that international data transfers and trade will continue to take place without the security of agreements that bridge the gap between internal data privacy laws.") (citations omitted).

more state standards to develop, some of which will inevitably conflict, will result in individual privacy rights changing as consumers travel and interact with businesses in other states. This is unacceptable, particularly when information privacy is not a local concern requiring regulation that is tailored to the customs or preferences of a particular state. Instead, the standards for information privacy are value judgments based on the need for robust consumer protection (which should apply to everyone equally across the United States) and the recognition that data collection and processing is inherently good and integral to our national economy. The only way to balance our national economic interests and need for innovative growth while ensuring robust and meaningful consumer protections to prevent and remedy privacy harms is through a national law setting forth a harmonized standard that applies irrespective of an individual's state of residence or location when engaging in commercial activities that involve their personal data.

What State Laws Should Federal Privacy Law Preempt?

Federal information privacy law should set forth a national standard to regulate the collection and processing of personal data, while retaining important state laws that fall under core police powers and local interests that may directly or indirectly touch on data privacy. The state laws that should be retained include consumer protection laws (except to the extent they are used to regulate personal information privacy practices); criminal laws; laws relating to wiretapping, the protection of Social Security numbers, identity protection, or student privacy; and state constitutional, contract, and tort laws.

Whether a federal law should preempt state laws regulating information privacy issues relating to sensitive health data, financial data, and children's data, depends entirely on the scope of the federal law. If, as we expect, federal information privacy law acts a gap filler to the current federal sectoral model in these areas, then the federal law should not preempt state laws to the extent they are permitted under the preemption and savings clauses of the relevant federal sectoral laws; namely, HIPAA and GLBA.

Children's and students' privacy present unique concerns that federal information privacy law may address. Both are currently regulated by a mixture of federal and state law, but for different reasons. COPPA, for instance, expressly preempts state law. The scope of COPPA, however, is the protection of online privacy for children under the age of 13. Although COPPA preempts inconsistent state law, this left room for states to regulate children's privacy outside COPPA's scope. In other words, COPPA has not been interpreted, at least by its regulatory authority (the Federal Trade Commission), as an implied field preemption statute. Whether policymakers should preempt state laws

governing children's privacy will depend how the federal privacy law addresses children's privacy.

The Family Educational Rights and Privacy Act (FERPA), in contrast, does not preempt state law. As a result, student privacy is subject to numerous regulations at the state and local levels. Notably, this comports with our country's tradition of treating education as a matter of local control. Because of this localization, student privacy regulation generally does not implicate the global market concerns we have noted in the general information privacy sector, even if it has some impact on our national market. In general, therefore, we expect that federal information privacy legislation will not preempt state and local student privacy regulations.

Analysis of Model Preemption Provisions and Recommendations

The ultimate question in each case . . . is one of Congress's intent, as revealed by the text, structure, purposes, and subject matter of the statutes involved.[55]

As we have explained in detail above, preemption in the federal privacy context is complex due to the interplay of federal sectoral privacy laws, state and local privacy regulations, and a range of other federal and state laws that touch upon the privacy. It is important, therefore, that policymakers consider the following questions as they examine the question of preemption in federal information privacy legislation:

1. Which state laws regulating data must Congress preempt to achieve the goal of strong and uniform federal regulation over the information market? As part of this question, policymakers should ask whether there are any state laws relating to information privacy that federal legislation could inadvertently supersede with either an express preemption provision or through an implied field or obstacle preemption analysis by the courts. For example, could the courts interpret a preemption provision to expressly or impliedly preempt state consumer protection laws?[56] If so, policymakers need to consider if this is the policy balance they want to achieve, and whether a savings clause is necessary to express congressional intent to prevent an inadvertent displacement of certain state laws.

[55] *Cipollone*, 505 U.S. at 545 (Scalia, A., concurring in part).

[56] Jay B. Sykes and Nicola Vanatko, Cong. Research Serv., R45825, Federal Preemption: A Legal Primer (2019), pp. 8-9 (discussing how the Airline Deregulation Act was interpreted by the Court to preempt state consumer protection statutes to the extent they prohibited deceptive airline fare advertisements).

2. How can Congress ensure that privacy legislation preempts state laws only to the extent necessary to ensure harmonization of the law? To answer this question, policymakers will need to consider how to describe the scope of the preemption provision and whether a savings clause excluding certain state laws can helpfully evidence congressional intent regarding the scope of preemption.

3. How should a preemption provision in federal privacy legislation address federal sectoral privacy laws? Going on the assumption that such legislation will fill the gaps in the federal sectoral model rather than displace it, how could a preemption provision impact state laws that exist in parallel to the federal sectoral laws?

Even if federal information privacy law includes a preemption provision, significant room remains for the states to legislate on other privacy and data issues, particularly those of a local concern. For example, and as described in this brief, federal information privacy legislation is not expected to preempt state law addressing student privacy, which is an area that the U.S. has traditionally treated as subject to local regulation. Federal legislation also is not expected to preempt state laws governing how local law enforcement and other government agencies collect and use personal data for purposes of executing their state police powers, another area customarily of local concern. Lastly, unless federal information privacy law is broad enough to supersede federal sectoral privacy law, we expect that it will not displace the preemption provisions of those sectoral laws that set federal floors rather than ceilings for information privacy standards.

As policymakers draft and debate federal information privacy legislation, we note that two legislative proposals address these preemption questions: the **Information Transparency & Personal Data Control Act**[57] ("ITPDCA") and the **Intel Privacy Bill**.[58] Each contains a preemption provision that focuses on civil laws to the extent they cover the data collection and processing practices covered by the draft law, and a series of savings clauses to address the unique risks associated with preemption in the privacy context. Below we analyze these provisions, with the aim of helping policymakers decide whether they should adopt these proposals in total or partially.

We rely on the ITPDCA and the Intel Privacy Bill for the purposes of applying preemptive analysis to information privacy law only. Our analysis is not an endorsement of

[57] H.R. 2013, 116th Congress (2019).
[58] Intel, Legislation, https://usprivacybill.intel.com/legislation/.

the substantive provisions and protections proposed by either proposal. We have reprinted the relevant ITPDCA and Intel Privacy Bill provisions in appendices A and B, respectively.

Before delving into that, however, we begin with an analysis of statutory language for express preemption provisions, and how the Court has interpreted such language.

Statutory Language for Express Preemption Provisions

A recent CRS report on federal preemption identifies four categories of language most commonly used in express preemption clauses, and how that language has been interpreted by the Supreme Court and lower federal courts: those that preempt all state laws that are (1) "related to" a specific matter, (2) "covered by" federal laws and regulations, (3) "in addition to, or different than" federal requirements, and (4) "concerning subjects" of federal regulatory concern.[59] Each category brings pros and cons that should be evaluated when drafting an express preemption provision.

First, some federal statutes expressly preempt "all state laws that are 'related to' a specific matter of federal regulatory concern.[60] Examples of federal statutes employing preemption with a similar scope are the Employee Retirement Income Security Act (ERISA), the Airline Deregulation Act, and the Federal Aviation Administration Authorization Act (Federal Aviation Act)).[61]

Although the Supreme Court has cautioned against literal interpretation of these provisions, the Court also considers them to be "deliberatively expansive" and "conspicuous for [their] breadth."[62] The Court "has consistently held that state laws 'relate to' matters of federal regulatory concern when they have a 'connection with' or contain a 'reference to' such matters.[63] State laws generally "have an impermissible 'connection with' matters of federal concern when they prescribe rules specifically directed at the same subject as the relevant federal regulatory scheme, or when their indirect effects on the federal scheme are particularly acute."[64] This is in contrast to "state laws having only 'tenuous, remote, or peripheral' effects on an issue of federal concern," which "are not sufficiently

[59] *See generally* Sykes and Vanatko.
[60] *Id.* at 6-10.
[61] *Id.* at 7.
[62] *Id.* (citing *FMC Corp. v. Holliday*, 498 U.S. 52, 58 (1990)).
[63] *Id.* at 10 (citing *Rowe v. N.H. Motor Transport. Ass'n*, 552 U.S. 364, 370 (2008); *Morales v. Trans World Airlines, Inc.*, 504 U.S. 34, 383 (1992); *Shaw v. Delta Airlines, Inc.*, 463 U.S. 85, 96 (1983)).
[64] *Id.* (citing *Egelhoff v. Egelhoff ex rel. Breiner*, 532 U.S. 141, 148 (2001); *NY State Conf. of Blue Cross & Blue Shield Plans v. Travelers Ins. Co.*, 514 U.S. 645, 668 (1995)).

'related to' the issue to warrant preemption."[65] Qualifying language in the preemption provision, however, risks the courts interpreting a narrow preemptive scope.[66] This is exemplified by the Federal Aviation Act, which significantly limited the breadth of its preemption provision through the inclusion of "with respect to," which the courts interpreted as limited qualifying language.[67]

Second, some laws preempt state laws "covered by" federal laws and regulations.[68] The Supreme Court has held that "'covering' is a 'more restrictive term' than 'related to' and that federal law will accordingly 'cover' the subject matter of a state law only if it 'substantially subsume[s]' that subject."[69] As a result, "the Court has made clear that 'covering' preemption clauses . . . have a narrower effect than 'related to' clauses."[70] The "specific determinations that federal law 'covers' a subject," however, "will depend heavily on the details of particular regulatory schemes."[71]

Third, other statutes supersede state laws that are "'in addition to, or different than' federal requirements," which the Supreme Court has interpreted as preempting state law even when compliance with both does not create a conflict.[72] Thus, with these provisions, when a state law is different from a federal law, the state law is preempted. State laws that are identical, or parallel, to the federal law, however, are not displaced.[73] To be deemed identical and survive preemption, the state law does not need to explicitly incorporate the federal law or provide the same remedies.[74] The case law in this area is still developing, with one lower court finding that a state law is identical (or parallel) and not displaced if it is "generally equivalent" to the federal standards, and another court finding that state law is not generally equivalent to the federal law "if a defendant could violate state law without having violated federal law."[75]

---

[65] *Id.* (citing *Shaw*, 463 U.S. at 100 n. 21).
[66] *Id.* (citing Dan's City Used Cars, Inc. v. Pelkey, 569 U.S. 251, 261 (2013)).
[67] *Id.* at 9-10.
[68] *Id.* at 10-11.
[69] *Id.* at 10 (quoting *CSX Transp., Inc. v. Easterwood*, 507 U.S. 658, 664 (1993)).
[70] *Id.* at 11.
[71] *Id.*
[72] *Id*. at 11 (citing *National Meat Assn. v. Harris*, 565 U.S. 452, 455 (2012)).
[73] *Id.* at 12 (citing *Bates v. Dow Agrosciences LLC*, 544 US. 431, 446 (2005); *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 494-97 (1996)).
[74] *Id.* (citing *Bates*, 544 U.S. at 447-48).
[75] *Id.* (citing *Bates* at 454; *McMullen v. Medrronic, Inc.*, 421 F.3d 482, 489 (7th Cir. 2005)).

Fourth, and finally, federal laws "frequently preempt state 'requirements,' 'laws,' 'regulations,' and/or 'standards' concerning subjects of federal regulatory concern."[76] This leaves to judicial interpretation whether the preemptive reach extends to state common law.[77] The Supreme Court has ruled that absent evidence of a contrary intention, the reference to state "requirements" reaches state common law.[78] Another case, however, indicates that reference to "laws" or "regulations" alone does not evidence an intention to preempt state common law, particularly when there is a savings clause for state common law claims.[79]

Examining Express Preemption Through the Lens of the ITPDCA and the Intel Privacy Bill

Assuming Congress agrees on strong information privacy legislation that is comprehensive and technology-neutral, the legislation should preempt all civil laws at the state level within the same regulatory scope. To achieve this, Congress will need to draft an express preemption provision that reaches the state laws necessary to ensure one national standard for the federal information privacy interests addressed by the federal law. This is critically important because including an express preemption provision does not preclude judicial interpretation of the implied preemptive scope of a federal law.[80] Moreover, when there is an express presumption provision, the courts do not apply the maxim of a presumption against preemption.[81]

The Intel Privacy Bill and the ITPDCA seek to achieve this baseline goal through their express preemption provisions.[82] Each includes express preemption language to supersede civil state laws (or civil laws of any political subdivision of the state) "to the degree the law is focused on the *reduction of privacy risk*." The Intel Privacy Bill focuses its preemptive scope from there on the regulatory reach of the model bill, which addresses the "regulation of personal data collection and processing activities." The ITPDCA similarly focuses the scope of its preemption provision, though it is scaled according to that

[76] *Id.* at 12-13.
[77] *Id.* at 12.
[78] *Id.*
[79] *Id.* at 12-13 (citing *Sprietsma v. Mercury Marine*, 505 U.S. 504, 521 (1992)).
[80]Sykes and Vanatko at 2-3 (citing *Geier v. American Hondo Motor Co*., 529 U.S. 861, 881-82 (2000) (explaining that an express preemption provision "does not preclude implied preemption analysis")).
[81] *See* fn. 3-4, *supra*.
[82] *See* appendices A and B for the model statutory language.

legislation's narrower focus on the collection and processing of sensitive personal information. The specific preemptive language of each bill is as follows:

- **Intel Privacy Bill**: "For a covered entity subject to this Act, the provisions of this Act shall preempt any civil provisions of the law of any State or political subdivision of a State to the degree they are focused on the reduction of privacy risk through the regulation of personal data collection and processing activities."

- **ITDPCA**: "For a controller that is subject to this Act, or any regulation promulgated pursuant to this Act, the provisions of this Act, or any such regulation, shall preempt any civil provision of the law of any State or political subdivision of a State to the degree the law is focused on the reduction of privacy risk through the regulation of the collection of sensitive personal information and the collection, storage, processing, sale, sharing with third parties, or other use of such information."

These model provisions incorporate two important points that policymakers should include in federal data privacy legislation. *First*, for information privacy legislation, a preemption provision should generally limit its reach to civil laws, which avoids inadvertently displacing state criminal laws that touch on data privacy issues. These laws can include state laws prohibiting the distribution of revenge pornography or outlawing identity theft. These model provisions account for this by expressly preempting ***civil*** laws focused on the reduction of privacy risk. Policymakers, however, may want to consider adding language to clarify that this tailoring is not intended to leave in place state laws seeking to criminalize the data collection and processing activities regulated by the federal law. If the federal government passes comprehensive privacy legislation that sets a ceiling for collection and processing activities, then state laws criminalizing the same conduct should not circumvent Congress' preemptive intent.

Second, any preemption provision should focus on displacing state laws addressing the regulation of personal data collection and use. State and local consumer protection laws (such as the little FTC Acts prohibiting unfair and deceptive acts and practices) should not, therefore, be impliedly displaced on judicial review, except to the extent they are used to regulate privacy standards. The Intel Privacy Bill's provision accounts for this by expressly limiting the bill's preemptive reach to laws focused on the reduction of privacy risk through the regulation of personal data collection and processing activities. The ITPDCA differently, but similarly, limits its preemptive reach to the sensitive information addressed by the law.

Policymakers may also want to consider adopting some of the most commonly used preemption language, as identified by recent CRS research (which is discussed in detail above). Doing so helps policymakers predict the potential reach or limitation of a preemption provision when subject to judicial review.

Notably, neither the ITPDCA nor the Intel Privacy Bill uses the preemption language that CRS identifies as the most common. They do not, for instance, supersede state laws that "relate to" or "cover" a particular federal regulatory concern. Neither do their preemption provisions permit state laws "in addition to, or different than" their regulatory scope, nor preempt state "requirements," "laws," "regulations," and/or "standards." Instead, they preempt state laws "to the degree they ***are focused on***" the regulatory concern of each proposed law. Our research has not uncovered another preemptive statute using the language "focused on" or any resulting judicial interpretation of the preemptive effect of a statute using this language.

To ensure predictable judicial interpretation, policymakers may want to draw from the most commonly used preemption language identified by the CRS, rather than breaking the mold with untested language. We suggest using the key words "relate to," which case law suggests will be interpreted to displace state laws that govern or interfere with the core areas of concern to the federal statute, as opposed to laws that indirectly affect it.[83]

Examining Savings Clauses Through the Lens of the ITPDCA and the Intel Privacy Bill

Congress, to clearly demonstrate its preemption intent, can also include savings clauses to work in tandem with express preemption provisions and restrict the preemptive scope of the federal law. Including a savings clause, particularly in a regulatory area as complex as information privacy, can help courts determine the intended preemptive effect of the statute by identifying specific state laws or categories of state law that Congress does not intend to displace. This is particularly important because "[t]he law regarding savings clause 'is not especially well developed,' and cases involving such clauses 'turn very much on the precise wording of the statutes at issue.'"[84]

The ITDPCA and the Intel Privacy Bill include savings clauses that serve to clarify the intended preemptive scope of their express preemption provisions.[85] With respect to

[83] Sykes and Vanatko at 7-8 (discussing ERISA) and 10 (citations omitted).
[84] Sykes and Vanatko at 13 (quoting Alan Untereiner, *The Preemption Defense in Tort Actions: Law Strategy and Practice* 204-05 (2008)).
[85] *See* appendices A and B.

state laws, the two models are nearly identical. The Intel Privacy Bill model, however, goes beyond the ITDPCA to include provisions preserving the authority of the FTC under other provisions of law, the FCC pursuant to the Communications Act of 1934, and the treatment of covered entities by enumerated federal sectoral privacy laws (*i.e.*, HIPAA, FERPA, and the GLBA).

These legislative proposals accomplish an important goal: ensuring a national information privacy standard, while retaining important federal sectoral laws and state laws that fall under core police powers and local interests that may directly or indirectly touch on data privacy. The state laws include consumer protection laws (such as the little FTC Acts); criminal laws; laws relating to wiretapping; the protection of Social Security numbers, identity protection, and student privacy; and state constitutional, contract, and tort laws.

Should policymakers follow this approach, they may want to consider refining these models in the following ways:

First, policymakers could clarify the scope of the savings clause for consumer protection laws. Both models include a preemption carve-out for the enforcement pursuant of any state consumer protection law by an attorney general of the state, other than to the extent such laws regulate personal data collection and processing. Policymakers may want to clarify this provision in federal legislation by expanding the savings clause to enforcement actions brought by other State or local law enforcement authorities as authorized by state law. Doing so recognizes that while most states prosecute consumer protection violations through their Office of Attorney General, not all do. It also recognizes that consumer protection enforcement often occurs on the local city and county level.[86]

Second, the ITPDCA and the Intel Privacy Bill include a separate savings clause that saves certain laws from preemption: (1) the constitutional, trespass, contract, data breach notification, or tort law of any state, other than to the degree such laws are substantially intended to cover government personal data collection and processing; (2) any other state law to the extent that the law relates to acts of fraud, wiretapping, or the protection of Social Security numbers; (3) any state law to the extent it provides additional provisions to specifically regulate the covered entities as defined in HIPAA, FERPA, or the GLBA; and (4) private contracts based on any state law that require a party to provide additional or greater

[86] In general, courts find that savings clauses apply to local laws from their very terms absent a clear statement to the contrary. *See* Sykes and Vanatko at 16. Nevertheless, Congress may choose to include this for legislative clarity.

personal data privacy or data security protections to an individual than does this Act. We suggest that policymakers consider two clarifications to this:

(1) The first provision listed above specifies that the savings clause is intended to save state constitutional, trespass, contract, or tort law only to the extent those laws are ***not substantially intended*** to govern personal data collection and processing. The language "substantially intended" results in some ambiguity. Policymakers may want to clarify the savings clause by stating the federal law should not be construed to preempt any state constitution, trespass, contract, data breach notification, or tort law, other than ***to the degree such law regulates or is enforced to govern*** the collection and processing of personal data. Alternatively, and to potentially rely on the case law interpreting preemption provisions, the savings clause could be redrafted to save those enumerated laws other than ***to the extent the law regulates or is enforced to address acts and practices relating to*** the collection and processing of personal data.[87]

(2) The second provision may be clarified to exclude from preemption those state laws relating to nonconsensual pornography. Unless the federal information privacy legislation specifically covers this particularly pernicious use of personal information, an express savings clause can ensure that existing state laws barring it are not displaced. To date, 46 states, the District of Columbia, and one territory have enacted laws to bar revenge pornography.[88]

Last, and although not technically a preemption issue, policymakers may want to consider a provision similar to the one included in the Intel Privacy Bill to address how comprehensive federal privacy legislation is intended to work with existing federal sectoral privacy laws. Our presumption is that even if federal legislation fills some of the gaps between these laws, it will not replace them. If that is the case, a provision explicitly stating that the federal privacy law does not modify, limit, or supersede the existing sectoral frameworks may be beneficial. Another legislative proposal is instructive here, the Privacy Bill of Rights Act.[89] Policymakers may want to consider an amalgam provision of the provisions in the Intel Privacy Bill and the Privacy Bill of Rights Act. This could help ensure that comprehensive federal privacy legislation can fill the gaps of the federal sectoral framework, while leaving important national privacy laws intact.

[87] *See* fn. 59-79, *supra*.
[88] Cyber Civil Rights Initiative, https://www.cybercivilrights.org/revenge-porn-laws/.
[89] S. 1214, 116th Cong. (2019), § 18.

Conclusion

It is true that in American federalism one of the bases for concurrent state and federal regulation is to enable the states to act as the "laboratories of democracy,"[90] testing out new and innovative regulatory frameworks. The intention of this division of powers, however, cannot justify splintering a regulatory matter of national and global importance to the detriment of our national economy, the global economy, and American consumers. Congress can, and should, honor state ingenuity through a federal information privacy standard that draws on their regulatory lessons while harmonizing U.S. data privacy for the benefit of consumers, industry, and economy.

[90] *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, dissenting).

Appendix A: Information Transparency & Control Personal Data Act

Sec. 9. NATIONAL STANDARD

(a) PREEMPTION. – For a controller that is subject to this Act, or any regulation promulgated pursuant to this Act, the provisions of this Act, or any such regulation, shall preempt any civil provision of the law of any State or political subdivision of a State to the degree the law is focused on the reduction of privacy risk through the regulation of the collection of sensitive personal information and the collection, storage, processing, sale, sharing with third parties, or other use of such information.

(b) CONSUMER PROTECTION LAWS. – Except as provided in subsection (a), this section may not be construed to limit the enforcement, or the bringing of a claim pursuant to any State consumer protection law by an attorney general of a State, other than the extent to which any such law regulates the collection of sensitive personal information and the collection, storage, processing, sale, sharing with third parties, or other use of such information.

(c) PROTECTION OF CERTAIN STATE LAW. – Nothing in this Act may be construed to preempt the applicability of any of the following:

(1) State constitutional, trespass, contract, data breach notification, or tort law, other than to the degree such law is substantially intended to govern the collection of sensitive personal information and the collection, storage, processing, sale, sharing with third parties, or other use of such information.
(2) Any other State law to the extent that the law relates to acts of fraud, wiretapping, or the protection of social security numbers.
(3) Any State law to the extent the law provides additional provisions to specifically regulate the covered entities as defined for purposes of the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), section 444 of the General Education Provisions Act (commonly known as the Family Educational Rights and Privacy Act of 1974) (20 U.S.C. 1232g), the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or the Gramm-Leach-Bliley Act (15 U.S.C. 6701 et seq.).

(4) Any private contract based on a State law that requires a party to provide additional or greater privacy for sensitive personal information or data security protections to an individual than this Act, or any regulation promulgated pursuant to this Act.

Appendix B: Intel Privacy Bill

Section 10. PREEMPTION.

(a) **PREEMPTION.** – For a covered entity subject to this Act, the provisions of this Act shall preempt any civil provisions of the law of any State or political subdivision of a State to the degree they are focused on the reduction of privacy risk through the regulation of personal data collection and processing activities.

(b) **CONSUMER PROTECTION LAWS. –** Except as provided in Section 10(a), this section shall not be construed to limit the enforcement or bringing of a claim pursuant to any State consumer protection law by an attorney general of a State, other than the extent to which those laws regulate personal data collection and processing.

(c) **PROTECTION OF CERTAIN STATE LAW.** – Nothing in this Act shall be construed to preempt the applicability of –

(1) the constitutional, trespass, contract, data breach notification or tort law of any state, other than to the degree such laws are substantially intended to govern personal data collection and processing;
(2) any other state law to the extent that the law relates to acts of fraud, wiretapping, or the protection of social security numbers;
(3) any state law to the extent it provides additional provisions to specifically regulate the covered entities as defined in the Health Insurance Portability and Accountability Act of 1996 (Pub.L. 104-191), the Family Educational Rights and Privacy Act (Pub.L. 93-380), the Fair Credit Reporting Act (Pub.L. 91-508) or the Financial Services Modernization Act of 1999 (Pub.L. 106-102); or
(4) private contracts based on any state law that require a party to provide additional or greater personal data privacy or data security protections to an individual than does this Act.

(d) **PRESERVATION OF COMMISSION AUTHORITY**. – Nothing in this Act may be construed to in any way limit the authority of the Commission under any other provision of law.

(e) **FCC AUTHORITY.** – Insofar as any provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.), including but not limited to Section 222 of the Communications Act of 1934 (47 U.S.C. 222), or any regulations promulgated under such Act apply to any person subject to this Act with respect to privacy policies, terms of service, and practices covered by this Act, such provision of the Communications Act of 1935 or such regulations shall have no force or effect, unless such regulations pertain to emergency services.

(f) **TREATMENT OF COVERED ENTITIES GOVERNED BY OTHER FEDERAL LAW.** – Covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (Pub.L. 104-191), the Family Educational Rights and Privacy Act (Pub. L. 93-380), the Fair Credit Reporting Act (Pub.L. 91-508) or the Financial Services Modernization Act of 1999 (Pub.L. 106-102), are excluded from the provisions of this Act to the degree specific uses of personal data are covered by the privacy provisions of those laws.

The Software & Information Industry Association (SIIA) is the principal trade association for the software and digital content industry. SIIA provides global services in government relations, business development, corporate education, and intellectual property protection to the leading companies that are setting the pace for the digital age.

For more information, visit siia.net

SIIA Public Policy
Software & Information Industry Association
1090 Vermont Avenue NW
Sixth Floor
Washington, DC 20005