Congressional Research Service
Informing the legislative debate since 1914

Preemption and Privacy Law

August 29, 2025

Congressional Research Service
https://crsreports.congress.gov
R48667

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Preemption and Privacy Law

SUMMARY

R48667

August 29, 2025

Chris D. Linebaugh
Legislative Attorney

Under the U.S. Constitution's Supremacy Clause, Congress may displace state law when it is acting within its enumerated constitutional powers. In the realm of consumer privacy, Congress has largely chosen to leave state laws in place. Rather than adopting a single comprehensive consumer privacy law, Congress has enacted various privacy statutes that apply to particular industries and subcategories of data. These laws, which are often described as "sectoral" privacy laws, apply to health data, financial data, children's data, telecommunications data, and credit reports, among other areas. These federal sectoral privacy laws generally leave room for states to supplement the federal requirements with their own standards.

States, consequently, have increasingly adopted their own privacy laws. Many of these laws either build on the federal sectoral privacy laws or apply to new industries or types of data not covered by the federal laws. For example, some states have adopted laws that provide additional protections for genetic data, biometric data, or reproductive health data; some states have passed laws requiring online platforms to configure their settings to better protect children's privacy; and some states have passed laws aimed at entities like data brokers, who compile and sell consumer data. An increasing number of states have taken the step of adopting comprehensive privacy laws that apply to nearly all forms of personal data within their jurisdictions. Between 2018 and the time of this writing, at least 19 states have adopted comprehensive consumer privacy laws. These laws generally provide a similar set of consumer rights (e.g., the right for consumers to request that businesses provide a copy of their personal data or to correct or delete their data) and business obligations (e.g., the obligation to give consumers the opportunity to opt out of the sale of their data or the use of their data for targeted advertising).

With the burgeoning landscape of state privacy law, preemption will be a key question in any future federal privacy legislation. Any new federal privacy law will either displace or maintain state laws, depending on Congress's intent. Congress could choose to preserve state privacy laws unless they directly conflict with the federal law, or it could choose to preempt all or most state privacy laws. Congress could further cabin a law's preemptive scope by including a savings clause that expressly preserves certain types of state laws or remedies. Congress could also delegate preemption decisions to a federal agency. Comprehensive privacy bills introduced in past Congresses have taken varied approaches to preemption, including preserving most state laws, preempting most state laws, and combining a general preemption provision with a detailed savings clause.

Contents

Contacts

Much of American privacy law is state law. While Congress has constitutional authority[1] to preempt states from regulating companies' data privacy practices, it has, for the most part, declined to do so. Congress's approach to data privacy has been described as "sectoral."[2] Rather than adopting one comprehensive privacy law that applies to most consumer data, Congress has enacted various statutes aimed at certain industries and types of data, such as health data, financial data, and children's data.[3] These privacy statutes generally do not displace state laws, thus leaving room for states to supplement the federal requirements with their own standards. As a result, states have the ability to adopt their own privacy laws, and they have increasingly done so. States have enacted sectoral laws that build on existing federal privacy protections and that apply to new industries and categories of data.[4] States have also, more recently, adopted comprehensive privacy laws, regulating nearly all forms of personal data within their jurisdictions.[5]

With the burgeoning landscape of state privacy law, preemption will be a key question in any future federal privacy legislation. Any new federal privacy law will either displace or maintain these laws, depending on Congress's intent. This report assists Congress in navigating such preemption decisions. It first provides a background of key legal principles governing preemption. The report next describes how existing federal privacy laws have approached preemption, particularly the way in which they leave room for states to supplement the federal requirements. The report then reviews state privacy laws. It first surveys various state sectoral privacy laws before taking a closer look at the comprehensive state privacy statutes. The report closes with some considerations for Congress in drafting future preemption provisions, particularly in the context of a comprehensive data privacy bill.

Federal Preemption of State Laws[6]

General Principles

The federal government's preemption of state law derives from the U.S. Constitution's Supremacy Clause. The Supremacy Clause states that the "Constitution, and the Laws of the United States which shall be made in Pursuance thereof," shall be the "supreme Law of the Land," notwithstanding any conflicting state law.[7] Under the Supremacy Clause, Congress may displace state law when it is acting within its enumerated constitutional powers.[8]

[1] Under the U.S. Constitution's Commerce Clause, Congress has the power to "regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes." U.S. CONST. art. I, § 8, cl. 3. The U.S. Supreme Court has said that personal information, when used by entities engaging in interstate commerce, is considered "an article of commerce" and within Congress's authority to regulate under the Commerce Clause. Reno v. Condon, 528 U.S. 141, 671 (2000). When Congress legislates pursuant to its authority under the Commerce Clause, it may preempt inconsistent state law. *See infra* "General Principles" for a discussion of Congress's preemption authority.

[2] *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014) (explaining that "privacy law in the United States is sectoral").

[3] *See infra* "Preemption in Federal Privacy Statutes" for further discussion of these federal privacy statutes.

[4] *See infra* "Sectoral State Privacy Laws" for a discussion of state sectoral privacy laws.

[5] *See infra* "Comprehensive State Privacy Laws" for a discussion of state comprehensive privacy laws.

[6] For a more detailed discussion of federal preemption, see CRS Report R45825, *Federal Preemption: A Legal Primer*, by Bryan L. Adkins, Alexander H. Pepper, and Jay B. Sykes (2023).

[7] U.S. CONST. art. VI, cl. 2; *see* Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 108 (1992).

[8] *See Overview of Supremacy Clause*, CONSTITUTION ANNOTATED, https://constitution.congress.gov/browse/essay/artVI-C2-1/ALDE_00013395/ (last visited Aug. 11, 2025).

The U.S. Supreme Court has identified two general types of preemption: *express* preemption and *implied* preemption.[9] Federal preemption is express when a law contains explicit language preempting state law, and it is implied when a federal law's structure and purpose implicitly reflect Congress's intent to preempt.[10] For both types of preemption, the purpose of Congress is the "ultimate touchstone" that guides a reviewing court's preemption analysis.[11]

In many cases, and in particular when the federal government regulates in an area where states have historically exercised their police powers, the Supreme Court has presumed that a statute does not preempt state law "unless that was the clear and manifest purpose of Congress."[12] The Supreme Court has declined to apply this presumption in certain cases, however, including cases involving (1) express preemption;[13] (2) subjects that the states have not traditionally regulated;[14] and (3) areas in which the federal government traditionally has a "significant" regulatory presence.[15]

Express Preemption

Common Preemption Terms: "Related to" and "Covering"

Express preemption clauses often use terms with settled judicial interpretations. For example, some federal laws expressly preempt state laws that are "related to" a specific subject matter.[16] The Supreme Court has characterized these "related to" provisions as "deliberately expansive" and "conspicuous for [their] breadth."[17] "Related to" provisions generally displace state laws that have "a connection with" or contain a "reference to" the matter of federal concern.[18] The Supreme Court has cautioned, however, that "related to" preemption provisions might not preempt state laws with "tenuous, remote, or peripheral" effects on the matter of federal concern.[19]

Congress may also limit the impact of a "related to" provision by including qualifying language. For instance, in *Dan's City Used Cars v. Pelkey*, the Supreme Court considered a statute that preempted state laws "related to a price, route, or service of any motor carrier . . . with respect to the transportation of property."[20] The Court explained that the qualifier "with respect to"

---

[9] *See Gade*, 505 U.S. at 98 (citing Jones v. Rath Packing Co., 430 U.S. 519, 525 (1977); Shaw v. Delta Air Lines, Inc., 463 U.S. 85, 95 (1983); Fid. Fed. Sav. & Loan Assn. v. De la Cuesta, 458 U.S. 141, 152–53 (1982)).

[10] *Id.*

[11] *Id.* at 96.

[12] Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947).

[13] Puerto Rico v. Franklin Cal. Tax-Free Tr., 579 U.S. 115, 125 (2016).

[14] Buckman Co. v. Plaintiff's Legal Comm., 531 U.S. 341, 347–48 (2001).

[15] United States v. Locke, 529 U.S. 89, 108 (2000).

[16] *See, e.g.*, 29 U.S.C. § 1144(a) (preempting state laws "insofar as they may now or hereafter relate to any employee benefit plan"); 49 U.S.C. § 41713(b)(1) (preempting state laws "related to a price, route, or service of an air carrier"); *id.* § 14501(c)(1) (preempting state laws "related to a price, route, or service of any motor carrier . . . or any motor private carrier, broker, or freight forwarder with respect to the transportation of property").

[17] Morales v. Trans World Airlines, Inc., 504 U.S. 374, 384 (1992) (quoting Pilot Life Ins. Co. v. Dedeaux, 481 U.S. 41, 46 (1987); FMC Corp. v. Holliday, 498 U.S. 52, 58 (1990)).

[18] *See* Shaw v. Delta Air Lines, Inc., 463 U.S. 85, 96–97 (1983) (explaining that "[a] law 'relates to' an employee benefit plan, in the normal sense of the phrase, if it has a connection with or reference to such plan"); *see also* Dan's City Used Cars, Inc. v. Pelkey, 569 U.S. 251, 260 (2013) (explaining that the phrase "related to" in the Federal Aviation Administration Authorization Act of 1994 (FAAAA) "embraces state laws 'having a connection with or reference to' carrier 'rates, routes, or services,' whether directly or indirectly.") (quoting *Morales*, 504 U.S. at 384).

[19] *Shaw*, 463 U.S. at 100, n.21.

[20] *Dan's City*, 569 U.S. at 264.

"massively limited" the statute's preemptive scope.[21] The Court held that the federal law did not preempt a state law regulating the storage and disposal of towed cars because it did not concern the transportation of property.[22] As discussed later in the report, one federal privacy statute—the Fair Credit Reporting Act (FCRA)—similarly uses the phrase "with respect to" in its preemption provision. Citing *Dan's City*, courts have construed FCRA's preemption more narrowly than a typical "related to" provision.[23]

Other federal laws may preempt state laws on a subject matter "covered" by federal law.[24] In the case *CSX Transportation, Inc. v. Easterwood*, the Supreme Court explained that "covering" preemption provisions are more restrictive than "related to" preemption provisions and that a federal law will only "cover" the subject of a state law if it "substantially subsume[s]" that subject.[25] *Easterwood* dealt with preemption under the Federal Railroad Safety Act of 1970, which allowed states to regulate railroad safety "until such time as the Secretary [of Transportation] has adopted a rule, regulation, order, or standard covering the subject matter of such State requirement."[26] The plaintiff in *Easterwood* brought a state law tort action against the owner and operator of a train that struck and killed her husband at a train crossing. The Department of Transportation had adopted regulations that, among other things, (1) required states participating in a federal grant program to use warning devices at train crossings that conformed to standards set out in an agency manual and (2) set maximum train speeds.[27] The Court first held that the requirement for states to follow the agency manual did not "cover" tort liability for inadequate warning devices.[28] The Court explained that the manual mainly described the "proper size, color, and shape of traffic signs and signals" for the benefit of state employees and expressly disavowed any intent to set legal requirements.[29] On the other hand, the Court held that the maximum-speed regulations "covered," and therefore preempted, state tort claims alleging that a train traveled at an unsafe speed.[30] The Court explained that the Secretary adopted these regulations after considering the hazards posed by track conditions and they "must be read as not only establishing a ceiling, but also precluding additional state regulation."[31]

---

[21] *Id.* at 261 (quoting City of Columbus v. Ours Garage & Wrecker Serv., Inc., 536 U.S. 424, 449 (2002)).

[22] *Id.* at 261–65.

[23] *See infra* "Preemption in Federal Privacy Statutes" for a discussion of preemption under the Fair Credit Reporting Act.

[24] *See, e.g.*, 49 U.S.C. § 20106(a)(2).

[25] CSX Transp., Inc. v. Easterwood, 507 U.S. 658, 664 (1993).

[26] *Id.* at 662. Although this preemption provision has since been amended, the current version still retains the same "covering" terminology. *See* 49 U.S.C. § 20106(a)(2).

[27] *Easterwood*, 507 U.S. at 662–63, 666, 673. The regulations contained additional requirements for warning devices constructed using federal funds. *Id.* at 670–71. Under these requirements, federally funded projects to improve the train crossing had to include an automatic gate unless otherwise approved by the federal government. *Id.* These requirements, however, did not apply in *Easterwood* because the federal funds were not used to install the warning devices at the particular crossing at issue. *Id*. at 671–72.

[28] *Id.* at 666–70.

[29] *Id.* at 669. The Court contrasted the agency manual with the regulatory requirements for federally funded warning devices, discussed *supra* note 26. The Court explained that, unlike the manual, these requirements "do establish requirements as to the installation of particular warning devices" and "cover the subject matter of state law which . . . seeks to impose an independent duty on a railroad to identify and/or repair dangerous crossings." *Id.* at 670–71. In a later case, the Court held that these requirements preempted state law claims against a train operator for the alleged inadequacy of warning devices installed using federal funds. Norfolk S. Ry. Co. v. Shanklin, 529 U.S. 344, 358–59 (2000).

[30] *Id.* at 673–75.

[31] *Id.* at 674.

Savings Clauses

When Congress has included an express preemption clause in a law, the clause may limit the scope of that preemption through various types of savings clauses. For example, some federal laws explicitly exclude certain categories of state law from preemption.[32] Others seek to create a "federal floor" on which state laws can build.[33] Such floor-preemption provisions often state that the relevant statute "does not annul, alter, or affect" state laws "except to the extent that those laws are inconsistent" with the federal statute."[34] Some statutes using this "inconsistency" language further provide that state laws are not "inconsistent" with the relevant federal statute if they provide greater protection to consumers than federal law.[35] As discussed later in the report, several federal privacy statutes employ this language to create a federal floor, on which states have built with their own privacy laws.[36]

Implied Preemption

Even when a federal law does not expressly preempt state law, it may do so implicitly. Implied preemption takes two forms: *field* preemption and *conflict* preemption. Field preemption occurs when federal law occupies the field "so comprehensively that it has left no room for supplementary state legislation."[37] The Supreme Court has held that federal law preempts regulatory fields such as alien registration,[38] nuclear safety,[39] and wholesales of natural gas in interstate commerce,[40] among other areas.[41]

Conflict preemption occurs when either (1) "compliance with both federal and state regulations is a physical impossibility" (impossibility preemption)[42] or (2) the "challenged state law 'stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress'" (obstacle preemption).[43] The Supreme Court has said that litigants making conflict

[32] *See, e.g.*, 7 U.S.C. § 2910(a) ("Nothing in this chapter may be construed to preempt or supersede any other program relating to beef promotion organized and operated under the laws of the United States or any State."); *id.* § 6812(c) ("Nothing in this chapter may be construed to preempt or supersede any other program relating to cut flowers or cut greens promotion and consumer information organized and operated under the laws of the United States or a State."); *id.* § 7811(c) ("Nothing in this chapter may be construed to preempt or supersede any other program relating to Hass avocado promotion, research, industry information, and consumer information organized and operated under the laws of the United States or of a State.").

[33] *See, e.g.*, United States v. Pac. Gas & Elec. Co., 153 F. Supp. 3d 1128, 1131 (N.D. Cal. 2015) ("In other words, the Pipeline Safety Act creates a federal floor . . . upon which certified states are free to expand.").

[34] *See, e.g.*, 12 U.S.C. § 2616; 15 U.S.C. § 1693q; *id.* § 5722(a).

[35] *See, e.g.*, 12 U.S.C. § 2616; 15 U.S.C. § 1693q; *id.* § 5722(a).

[36] *See infra* "Preemption in Federal Privacy Statutes" for a discussion of preemption provisions in current federal law and *infra* "State Privacy Laws" for a discussion of how states have supplemented federal privacy law with their own requirements.

[37] Murphy v. Nat'l Collegiate Athletic Ass'n, 584 U.S. 453, 479 (2018) (quoting R. J. Reynolds Tobacco Co. v. Durham County, 479 U. S. 130, 140 (1986)).

[38] *See* Arizona v. United States, 567 U.S. 387, 401–03 (2012).

[39] *See, e.g.*, English v. Gen. Elec. Co., 496 U.S. 72, 82–85 (1990).

[40] *See* Schneidewind v. ANR Pipeline Co., 485 U.S. 293, 300, 305 (1988); Exxon Corp. v. Eagerton, 462 U.S. 176, 184 (1983).

[41] *See* "Field Preemption" in CRS Report R45825, *Federal Preemption: A Legal Primer*, by Bryan L. Adkins, Alexander H. Pepper, and Jay B. Sykes (2023) for examples of field preemption.

[42] Fla. Lime & Avocado Growers v. Paul, 373 U.S. 132, 142–43 (1963).

[43] *Arizona*, 567 U.S. at 399 (quoting Hines v. Davidowitz, 312 U.S. 52, 67 (1941)).

preemption arguments must meet a "high threshold."[44] Any conflict must be actual and irreconcilable, rather than "hypothetical or potential."[45]

Conflict preemption may occur even when a federal law's express preemption clause does not preempt the state law in question. In *Geier v. American Honda Motor Co.*, the Supreme Court held that the National Traffic and Motor Vehicle Safety Act's (NTMVSA's) express preemption provision did not preempt a state tort action against a motor vehicle manufacturer for negligently designing a car without a driver's side airbag.[46] The Court reasoned that the statute's savings clause, which preserved "liability under common law," removed state tort suits "from the scope of the express pre-emption clause."[47] Nevertheless, the Court held that NTMVSA and its implementing regulations impliedly preempted the state tort claim.[48] The Court reasoned that the tort action conflicted with the federal objective of giving car manufacturers the option of installing a "variety and mix" of passive restraints.[49] The Court also rejected the argument that NTMVSA's savings clause barred the Court's application of conflict preemption. The Court explained that nothing in the savings clause "suggest[ed] an intent to save state-law tort actions that conflict with federal regulations."[50]

Preemption in Federal Privacy Statutes

There is no single comprehensive federal law governing companies' data privacy practices. Rather, Congress has enacted various privacy laws that are primarily directed at certain industries and subcategories of data. These laws—which are often described as sector-specific or "sectoral" privacy laws[51]—are discussed more fully in another CRS report.[52] The list below, however, provides an introduction to some of the key sectoral privacy statutes.

- **The Children's Online Privacy Protection Act (COPPA)** and the Federal Trade Commission's (FTC's) implementing regulations require online operators who direct their services at children,[53] or who knowingly collect children's information, to comply with data privacy and data security requirements.[54] Covered operators must, among other things, obtain parental consent before collecting or using children's information, unless an exception applies.[55]
- **The Communications Act of 1934 (the Communications Act)**, as amended, requires telecommunications carriers, cable operators, and satellite carriers to

[44] U.S. Chamber of Com. v. Whiting, 563 U.S. 582, 608 (2011) (quoting Gade v. Nat'l Solid Wastes Mgm't Ass'n, 505 U.S. 88, 110 (1992) (Kennedy, J., concurring in part and concurring in judgment)).

[45] Rice v. Norman Williams Co., 458 U.S. 654, 659 (1982) ("As in the typical pre-emption case, the inquiry is whether there exists an irreconcilable conflict between the federal and state regulatory schemes. The existence of a hypothetical or potential conflict is insufficient to warrant the preemption of the state statute.").

[46] Geier v. Am. Honda Motor Co., Inc., 529 U.S. 861, 867–68 (2000).

[47] *Id.* at 868–69.

[48] *Id.* at 869–74.

[49] *Id.* at 881.

[50] *Id.* at 869.

[51] *See, e.g.*, Solove & Hartzog, *supra* note **Error! Bookmark not defined.**, at 587; Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L. J. 902, 908–12 (2009) (discussing the U.S. "sectoral" approach to privacy law).

[52] CRS Report R45631, *Data Protection Law: An Overview*, by Steve P. Mulligan and Chris D. Linebaugh (2019).

[53] COPPA defines a "child" as "an individual under the age of 13." 15 U.S.C. §6501(1).

[54] *Id.* §§ 6501–6506; 16 C.F.R. pt. 312 (2025).

[55] 15 U.S.C. § 6502(b); 16 C.F.R. § 312.5.

comply with data privacy and data security requirements.[56] These entities must, absent an exception, obtain customer consent before disclosing certain customer information to third parties and take steps to protect against unauthorized access to customer information.[57]

- **The Fair Credit Reporting Act** governs the collection and use of data contained in consumer reports.[58] Among other things, consumer reporting agencies (CRAs) must maintain reasonable procedures to ensure that the information used in consumer reports is accurate, and they may only give consumer reports to someone if they have reason to believe that the recipient will use it for certain permissible purposes.[59]
- **The Gramm-Leach-Bliley Act (GLBA)** requires financial institutions to comply with data privacy and data security requirements.[60] Financial institutions must notify consumers and give them an opportunity to "opt-out" before sharing their nonpublic personal information with third parties, unless an exception applies, and they must maintain safeguards to protect against unauthorized access to customer information.[61]
- **The Health Insurance Portability and Accountability Act (HIPAA)**[62] and the Department of Health and Human Services (HHS) implementing regulations require covered health care entities[63] and their business associates to comply with various data privacy and data security requirements.[64] Covered entities are, for instance, prohibited from disclosing a patient's protected health information (PHI) to third parties without the patient's consent, unless an exception applies.[65] They must also maintain safeguards to protect the security of PHI and notify affected individuals following a breach of unsecured PHI.[66]

These privacy laws, for the most part, contain express preemption provisions that set a federal floor rather than a federal ceiling. COPPA,[67] GLBA,[68] the Communications Act's cable and satellite privacy provisions,[69] and HIPAA[70] only preempt to the extent that a state law is

[56] 47 U.S.C. §§ 222, 338(i), 551.

[57] *Id.*

[58] 15 U.S.C. §§ 1681–1681x.

[59] *Id.* §§ 1681b(a)(3), 1681e(b).

[60] *Id.* §§ 6801–6809.

[61] *Id.* §§ 6801(a), 6802.

[62] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in relevant parts at 42 U.S.C. §§ 1320d–1320d-9).

[63] Covered entities under HIPAA include health care providers, health plans, and health care clearinghouses.45 C.F.R. § 164.104 (2025).

[64] *See* 45 C.F.R. §§ 164.302–318 (data security requirements), 164.400–414 (data breach notification requirements), 164.500–534 (data privacy requirements).

[65] *Id.* § 164.502. *See* CRS Legal Sidebar LSB11347, *Congressional Access to Personal Health Information*, by Todd Garvey (2025), for a discussion of whether HIPAA would restrict physicians from disclosing patient information in the context of congressional investigations.

[66] *Id.* §§164.302–318, 164.400–414.

[67] 15 U.S.C. §§ 6502(d).

[68] *Id.* § 6807(a).

[69] 47 U.S.C. §§ 338(i)(8), 551(g)

[70] 42 U.S.C. §§ 1320d-2 note, 1320d-7(a)(2)(b); *see also* 45 C.F.R. § 160.203 (HHS rules implementing HIPPA's preemption provisions).

inconsistent with, or contrary to, those federal laws.[71] GLBA and HIPAA further contain savings provisions preserving state laws with stricter privacy standards than those laws. Under GLBA, a state law will not be considered "inconsistent" if the Consumer Financial Protection Bureau determines that it affords a protection that is "greater than the protection" provided by GLBA.[72] Under HIPAA, a state health privacy law will not be preempted if it is "more stringent" than HIPAA's privacy provisions.[73]

FCRA, in contrast, preempts a broader set of state laws. In 1996, Congress amended FCRA to add a "strong preemption provision" that was designed to avoid a "patchwork system of conflicting regulations."[74] Section 1681t(b) of FCRA preempts any state law that imposes a "requirement or prohibition" "with respect to any subject matter" regulated under FCRA provisions "relating to" certain topics.[75] For instance, it preempts state laws "with respect to . . . [S]ection 1681s-2 [of FCRA], relating to the responsibilities of persons who furnish information to consumer reporting agencies."[76]

Because FCRA's § 1681t(b) uses the qualifier "with respect to," federal appellate courts have relied on the Supreme Court's *Dan's City* decision to construe it more narrowly than a typical "related to" preemption provision.[77] These courts have held that § 1681t(b) only preempts state laws if those laws "concern" the specific obligations contained in the enumerated FCRA provisions.[78] For example, in *Aargon Agency, Inc. v. O'Laughlin*, the U.S. Court of Appeals for the Ninth Circuit (Ninth Circuit) held that a Nevada law, which required debt collectors to notify debtors and wait sixty days before reporting medical debt to a CRA, was not preempted by FCRA because it did not "concern" FCRA's furnisher obligations.[79] The Ninth Circuit, citing *Dan's City*, concluded that § 1681t(b)'s use of the phrase "'with respect to' 'massively limits the scope of preemption' to only those state laws that 'concern' the phrase's referents."[80] The Ninth Circuit explained that FCRA requires furnishers to, among other things, provide accurate information to CRAs and to inform CRAs when a consumer disputes the information that they furnished.[81] It

[71] *See* 15 U.S.C. §§ 6502(d), 6807(a); 47 U.S.C. §§ 338(i)(8), 551(g); 45 C.F.R. § 160.203.

[72] 15 U.S.C. § 6807(b).

[73] 42 U.S.C. § 1320d-2, note; 45 C.F.R. § 160.203.

[74] Consumer Credit Reporting Reform Act of 1996, Pub. L. No. 104-208, § 2419, 110 Stat. 3009, 3009–52; Ross v. Fed. Deposit Insur. Corp., 625 F.3d 808, 813 (4th Cir. 2010) (quoting Michael Epshteyn, *The Fair and Accurate Credit Transactions Act of 2003: Will Preemption of State Credit Reporting Laws Harm Consumers?*, 93 GEO. L.J. 1143, 1154 (2005)).

[75] 15 U.S.C. § 1681t(b).

[76] *Id.* § 1681t(b)(F); *see also id*. § 1681s-2 (containing obligations for furnishers of information to CRAs).

[77] *See* Aargon Agency, Inc. v. O'Laughlin, 70 F.4th 1224 (9th Cir. 2023); Consumer Data Industry Ass'n v. Frey, 26 F.4th 1 (1st Cir. 2022); Galper v. JP Morgan Chase Bank, 802 F.3d 437 (2d Cir. 2015).

[78] *See Galper*, 802 F.3d at 446 ("[W]e hold that § 1681t(b)(1)(F) preempts only those claims that *concern* a furnisher's responsibilities."); *see also Aargon*, 70 F.4th at 1235 (explaining that § 1681t(b)(1)(F)'s preemption is limited "to only those state laws that 'concern' the phrases referents") (quoting Dan's City Used Cars, Inc. v. Pelkey, 569 U.S. 251, 261 (2013)); *Frey*, 26 F.4th at 7 ("Section 1681t(b)(1)(E)'s mandate expresses Congress' intent only to preempt those claims that concern subject matter regulated under Section 1681c. . . . So construed, the preemption clause necessarily reaches a subset of laws narrower than those that merely relate to information contained in consumer reports.").

[79] *Aargon*, 70 F.4th at 1236.

[80] *Id.* at 1235 (quoting *Dan's City*, 569 U.S. at 261).

[81] *Id.* at 1236.

does not, however, address when a furnisher must report a debt to a CRA.[82] The court accordingly concluded that the Nevada law "in no way interferes" with furnishers' obligations under FCRA.[83]

FCRA is not the only federal privacy law to generate preemption litigation. Even when federal laws only preempt inconsistent state laws, there can be disagreements over what constitutes inconsistency. For example, courts have disagreed on whether COPPA—which has no private right of action and is enforced only by the FTC and state attorneys general[84]—preempts individuals from bringing state lawsuits based on conduct that also violates COPPA.[85] COPPA prohibits state and local governments from imposing "any liability" on online operators in a manner that is "inconsistent with the treatment of those activities or actions" under COPPA. The Ninth Circuit has concluded this preemption language does not create an "exclusive remedial scheme for enforcement of COPPA requirements" and has allowed parallel state causes of action to proceed.[86] The Ninth Circuit reasoned that, "[s]ince [COPPA's] bar on 'inconsistent' state laws implicitly preserves 'consistent' state substantive laws, it would be nonsensical to assume Congress intended to simultaneously preclude all state remedies for violations of those laws."[87] On the other hand, some district courts in other circuits have held that such suits are inconsistent with Congress's decision to make COPPA enforceable only by the FTC and state attorneys general rather than individuals.[88]

State Privacy Laws

As shown in the preceding section, the current suite of federal data privacy laws leaves room for states to adopt their own privacy standards. States have used this freedom to enact an array of privacy laws. Many of these laws follow the sectoral approach and either build on the federal sectoral privacy laws or apply to new industries or types of data not covered by federal laws. Increasingly, however, states have adopted comprehensive commercial privacy laws that apply to a broad swath of entities handling consumer data.

This section begins by surveying state sectoral privacy laws before taking a closer look at the comprehensive state privacy laws. Rather than an exhaustive survey of all 50 states' privacy laws, this section instead provides a sketch of the main contours and trends in state privacy law, with the goal of informing Congress's future preemption decisions.

[82] *Id.*

[83] *Id.*

[84] *See* 15 U.S.C. §§ 6502(c) (providing for FTC enforcement), 6504 (providing for state attorney general enforcement).

[85] *Compare* Jones v. Google LLC, 73 F.4th 636 (9th Cir. 2023) *with* H.K. through Farwell v. Google, 595 F.Supp.3d 702 (C.D. Ill. 2022) *and* Manigault-Johnson v. Google, LLC, No. 2:18-cv-1032, 2019 WL 3006646 (D.S.C. Mar. 31, 2019).

[86] *Jones*, 73 F.4th at 642–43.

[87] *Id.* at 643.

[88] *See H.K. through Farwell*, 595 F. Supp. 3d at 710 ("[T]o allow Plaintiffs to assert H.K.'s claim against Defendant would be 'inconsistent with [COPPA's] treatment' of online data collection from children under 13 because COPPA provides for no private right of action, . . . whereas [the state law] does so explicitly."); *Manigault-Johnson*, No. 2:18-cv-1032, 2019 WL 3006646, at *6 ("Thus, it appears to the Court that Plaintiffs seek to use the vehicle of state law to privately enforce the provisions of COPPA, which Congress clearly intended to preclude when it included an express preemption clause in COPPA and assigned exclusive enforcement of COPPA to the Federal Trade Commission and state attorneys general.").

Sectoral State Privacy Laws

Many states have adopted laws that supplement the federal sectoral privacy laws. For example, in the years following Congress's enactment of GLBA, states like California and Vermont passed financial privacy laws that require financial institutions to give state residents an opportunity to *opt in* (in contrast to GLBA's *opt-out* standard) before sharing their nonpublic personal information with third parties.[89]

States likewise have adopted their own health privacy laws, some of which apply to more entities than HIPAA.[90] For instance, California's Confidentiality of Medical Information Act (CMIA)[91] applies to providers of health apps, mental health digital services, and reproductive or sexual health digital services.[92] The CMIA further requires employers to comply with specific privacy restrictions regarding their employees' medical information.[93] The Texas Medical Records Privacy Act[94] also surpasses HIPAA's scope of covered entities, applying to anyone who engages in "assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information," "comes into possession of protected health information," or "obtains or stores protected health information."[95]

Some states have sought to protect bodily-related data not covered by HIPAA. In 2008, for example, Illinois enacted the Biometric Information Privacy Act (BIPA), which restricts the way private entities may use biometric data.[96] A number of states have also adopted genetic information privacy acts, which generally require direct-to-consumer genetic testing companies to comply with privacy protections for consumer's genetic data.[97] In addition, some states, like California and Washington, have adopted health privacy protections that expressly apply to reproductive and gender-affirming care.[98]

Some states have supplemented COPPA by adopting their own online privacy protections for children. For example, under California's Age-Appropriate Design Codes Act—which is

[89] California Financial Information Privacy Act (SB1), CAL. FIN. CODE §§ 4050–4060 (West 2003); Vt. Stat. Ann. tit. 8, § 10,204 (2009).

[90] *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462, 82463–64 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164) (explaining that most states have "enacted one or more laws to safeguard privacy" but that the laws "vary significantly," with many protecting specific medical conditions rather than providing "comprehensive protections to people's medical records").

[91] California Confidentiality of Medical Information Act, 1981 CAL. STAT. ch. 782 (codified at CAL CIV. CODE §§ 56 – 56.37) (West 1981).

[92] CAL. CIV. CODE § 56.06.

[93] *Id.* §§ 56.06, 56.20–56.24.

[94] Texas Medical Records Privacy Act, TEX. HEALTH & SAFETY CODE ANN. §§ 181.001–181.207 (West 2001).

[95] *Id.* § 181.001(b)(2).

[96] 740 ILL. COMP. STAT. 14/1–14/25 (2008).

[97] *See, e.g.*, Utah Genetic Information Privacy Act, UTAH CODE ANN. §§ 13-60-101–13-60-106 (2021); CALIFORNIA GENETIC PRIVACY ACT, CAL. CIV. CODE §§ 56.18–56.186 (West 2022); TEX. BUS. & COMMERCE CODE ANN. §§ 503A.001– 503A.008 (West 2023).

[98] In 2023 California amended the CMIA to include specific protections for information related to abortions and gender-affirming care. *See* Confidentiality of Medical Information Act, 2023 CAL. STAT. 94 (codified at CAL. CIV. CODE §§ 56.05–06 (West 2023)). Also in 2023, Washington passed the My Health My Data Act, which broadly protects personal information that is "linked or reasonably linkable to a consumer" and that identifies their "past, present, or future physical or mental health status," including their "reproductive or sexual health information" and "gender-affirming care information." WASH. REV. CODE §§ 19.373.005–19.373.900 (2023).

preliminarily enjoined by a court[99]—online platforms that are likely to be used by minors must complete data impact assessments and configure minors' default privacy settings to a high level of privacy.[100] The Utah Minor Protection in Social Media Act—which has also been preliminarily enjoined by a court[101]—requires, among other things, social media platforms to verify users' ages, and impose privacy restrictions on minors' accounts.[102]

Some states have adopted privacy laws aimed at the data broker industry. Data brokers are entities who collect, compile, and sell information on consumers with whom they do not have a direct relationship.[103] Except for data brokers who qualify as CRAs and are subject to FCRA,[104] data brokers are not subject to a federal sectoral privacy statute.[105] Between 2017 and 2023, Vermont,[106] California,[107] Texas,[108] and Oregon[109] adopted laws regulating data brokers. All four states require data brokers to register with state authorities on an annual basis and to disclose certain aspects of their data collection and privacy practices.[110] Vermont and Texas's laws further require data brokers to comply with information security requirements.[111] In 2023, California supplemented its data broker law by passing SB 362, known as the Delete Act.[112] The Delete Act

[99] In 2023, the U.S. District Court for the Northern District of California issued a preliminary injunction blocking the law from going into effect, holding that the party challenging the law was likely to succeed on the argument that the law on its face violates the First Amendment. NetChoice, LLC v. Bonta, 692 F.Supp.3d 924 (N.D. Cal. 2023). The U.S. Court of Appeals for the Ninth Circuit vacated some aspects of the district court's preliminary injunction and remanded the case to the district court for further proceedings. NetChoice, LLC v. Bonta, 113 F.4th 1101 (9th Cir. 2024). Following the Ninth Circuit's remand, the district court granted the plaintiff's second motion for a preliminary injunction and enjoined the law in its entirety. NetChoice, LLC v. Bonta, 770 F. Supp. 3d 1164 (N.D. Cal. 2025).

[100] California Age-Appropriate Design Code Act, CAL. CIV. CODE §§ 1798.99.28 –1798.99.40 (West 2023).

[101] NetChoice, LLC v. Reyes, 748 F. Supp. 3d 1105, 1119–20 (D. Utah 2024) (holding that NetChoice is substantially likely to succeed on its claim that the law violates the First Amendment and granting its motion for a preliminary injunction).

[102] UTAH CODE ANN. §§ 13-71-101–13-71-401 (2024).

[103] For further discussion of the data broker industry, see CRS Report R47298, *Online Consumer Data Collection and Data Privacy*, by Clare Y. Cho and Ling Zhu (2022).

[104] Data brokers may be considered CRAs if they sell information about a consumer that is used or expected to be used in evaluating the consumer for credit, insurance, or employment. *See* 15 U.S.C. § 1681a(d), (f). In 2024, the Consumer Financial Protection Bureau issued a proposed rule addressing when data brokers qualify as CRAs subject to FCRA. *See* Protecting Americans From Harmful Data Broker Practices, 89 Fed. Reg. 101402 (Dec. 13, 2024) (proposed rule). The CFPB withdrew this proposed rule, however, in May 2025. *See* Protecting Americans From Harmful Data Broker Practices, 90 Fed. Reg. 20568 (May 15, 2025) (withdrawal of proposed rule).

[105] Data brokers are, however, subject to the Federal Trade Commission Act's broad prohibition on "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a). They must also comply with certain cross-border data flow requirements. Namely, under the Protecting Americans' Data from Foreign Adversaries Act of 2024, data brokers are prohibited from selling or transferring U.S. individual's "sensitive data"— which includes biometric, genetic, and geolocation information, among other things—to foreign adversaries. 15 U.S.C. § 9901. In addition, under Department of Justice regulations implementing Executive Order 14,117, data brokers are restricted from making bulk transfers of Americans' sensitive data to certain countries of concern. *See* Exec. Order No. 14,117, 89 Fed. Reg. 15421 (Feb. 28, 2024); Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636 (Jan. 8, 2025) (to be codified at 28 C.F.R. pt. 202).

[106] VT. STAT. ANN. tit. 9, §§ 2430, 2446, 2447 (2019).

[107] CAL. CIV. CODE §§ 1798.99.80–1798.99.89 (2024).

[108] TEX. BUS. & COMMERCE CODE ANN. §§ 509.001–509.010 (West 2024).

[109] OR. REV. STAT. § 646A.593 (2023).

[110] VT. STAT. ANN. tit. 9, § 2446; CAL. CIV. CODE § 1798.99.82; TEX. BUS. & COM. CODE ANN. § 509.005; OR. REV. STAT. §§ 646A.593(2)–646A.593(3).

[111] VT. STAT. ANN. tit. 9, § 2447; TEX. BUS. & COM. CODE ANN. § 509.007.

[112] 2023 Cal. Stat. ch. 709 (codified as amended at CAL. CIV. CODE §§ 1798.99.80–1798.99.82, 1798.99.84 – 1798.99.87, 1798.99.89 (2023)).

directs the California Privacy Protection Agency to establish a universal delete mechanism, whereby consumers will be able to request that all data brokers registered in the state delete their data.[113]

States have also adopted data breach response requirements, which, other than for some specific industries, do not exist at the federal level.[114] While the precise contours of these laws differ, all fifty states generally require companies who have experienced a data breach to notify affected individuals within a certain time frame.[115]

Comprehensive State Privacy Laws

In recent years, states have adopted comprehensive privacy laws in quick succession. Rather than focusing on specific industries or types of data, these laws govern how a broad range of businesses handle most individually identifiable consumer information. In 2018, California was the first mover when it enacted the California Consumer Privacy Act (CCPA).[116] Since then, from March 2021 onward, at least eighteen[117] other states have passed their own comprehensive privacy laws. In order of enactment, these states include Virginia,[118] Colorado,[119] Utah,[120]

[113] CAL. CIV. CODE § 1798.99.86.

[114] See CRS Legal Sidebar LSB10210, *What Legal Obligations do Internet Companies Have to Prevent and Respond to a Data Breach?*, by Chris D. Linebaugh (2018) for a discussion of federal data breach reporting requirements and an overview of state data breach requirements.

[115] *See*, *e.g.*, FLA. STAT. § 501.171(4) (2024) (requiring notice to affected individuals within thirty days); DEL. CODE ANN. tit. 6, § 12B-102 (2017) (requiring notice to affected individuals within sixty days).

[116] CAL. CIV. CODE §§ 1798.100–1798.199.100 (2024).

[117] The Florida Digital Bill of Rights (FDBR), signed into law in 2023, contains consumer rights and entity obligations similar to most comprehensive state privacy laws. *See* Florida Digital Bill of Rights, 2023 Fla. Sess. Law Serv. ch. 2023–201 (West) (codified at FLA. STAT. §§ 501.701–501.722 (2023)). The FDBR, however, primarily applies to entities who have a global gross annual revenue of at least $1 billion and who (a) derive fifty percent or more of their revenue from online adverting, (b) operate a smart speaker and voice command service, or (c) operate an "app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install." FLA. STAT. § 501.702(9). Because of the limited scope of covered entities, the FDBR is not included in the following list of comprehensive state privacy laws.

[118] Virginia Consumer Data Protection Act, 2021 Va. Acts. ch. 36 (codified as amended at VA. CODE ANN. §§ 59.1-575–59.1-584 (West 2025)).

[119] Colorado Privacy Act, 2021 Colo. Legis. Serv. ch. 483 (West) (codified as amended at COLO. REV. STAT. §§ 6-1-1301–6-1-1314) (2025)).

[120] Utah Consumer Privacy Act, 2022 Utah Laws ch. 462 (codified at UTAH CODE ANN. §§ 13-61-101–13-61-404 (2024)).

Connecticut,[121] Iowa,[122] Indiana,[123] Tennessee,[124] Montana,[125] Texas,[126] Oregon,[127] Delaware,[128] New Jersey,[129] New Hampshire,[130] Maryland,[131] Kentucky,[132] Nebraska,[133] Minnesota,[134] and Rhode Island.[135]

Protected Data

All nineteen state comprehensive privacy laws protect consumers' "personal information" or "personal data."[136] Most state comprehensive privacy laws contain similar definitions of personal information, typically encompassing any information that is "linked or reasonably linkable" to an individual but excluding publicly available or deidentified information.[137]

Covered Entities

Under most state comprehensive privacy laws, a business operating in the state will be subject to the law if, during a calendar year, it either (1) collects the personal information of a certain number of consumers (typically 100,000) or (2) collects the personal information of a lesser

[121] An Act Concerning Personal Data Privacy and Online Monitoring, 2022 Conn. Acts 22-15 ((Reg. Sess.) (codified as amended at CONN. GEN. STAT. §§ 42-515–42-527 (2025)).

[122] An Act Relating to Consumer Data Protection, 2023 Iowa Legis. Serv. ch. 17 (West) (codified at IOWA CODE §§ 715D.1–715D.9 (2025)).

[123] An Act to amend the Indiana Code concerning trade regulation, 2023 Ind. Acts. 1050 (to be codified at IND. CODE §§ 24-15-1-1–24-15-11-2).

[124] Tennessee Information Protection Act, 2023 Tenn. Pub. Acts ch. 408 (codified at TENN. CODE ANN. §§ 47-18-3301–47-18-3315 (2025)).

[125] Montana Consumer Data Privacy Act, 2023 Mont. Laws ch. 681 (codified as amended at MONT. CODE ANN. §§ 30-14-2801–30-14-2817 (2024)).

[126] Texas Data Privacy and Security Act, 2023 Tex. Sess. Law Serv. ch. 995 (West) (codified at TEX. BUS. & COM. CODE §§ 541.001–541.205 (2024)).

[127] Oregon Consumer Privacy Act, 2023 Or. Laws ch. 369 (codified as amended at OR. REV. STAT. §§ 646A.570 – 646A.589 (2025)).

[128] Delaware Personal Data Privacy Act, 2023 Del. Legis. Serv. ch. 197 (West) (codified at DEL. CODE ANN. TIT. 6, §§ 12D-101–12D-111 (West 2023)).

[129] New Jersey Data Privacy Act, 2023 N.J. Sess. Law Serv. ch. 266 (West) (codified at N.J. STAT. ANN. §§ 56:8-166.4 –56:8-166.19 (2025)).

[130] An Act relative to the expectation of privacy, 2024 N.H. Laws ch. 5 (codified at N.H. REV. STAT. ANN. §§ 507-H:1–507-H:12 (2025)).

[131] Maryland Online Data Privacy Act, 2024 Md. Laws ch. 455 (to be codified at MD. CODE ANN., COM. LAW §§ 13–301(14), 14-4601–14-4614).

[132] An Act relating to consumer privacy and making an appropriation therefor, 2024 Ky. Acts ch. 72 (to be codified at KY. REV. STAT. ANN. §§ 367.3611–367.3629).

[133] Nebraska Data Privacy Act, 2024 Neb. Laws L.B. 1074, §§ 1–30.

[134] Minnesota Consumer Data Privacy Act, 2024 Minn. Sess. Law Serv. ch. 121, art. 5 (codified at MINN. STAT. ANN. §§ 325M.10–325M.21 (West 2025)).

[135] Rhode Island Data Transparency and Privacy Protection Act, 2024 R.I. Pub. Laws ch. 430 (to be codified at 6 R.I. GEN. LAWS §§ 6-48.1-1–6-48.1-10).

[136] *See, e.g.*, CAL. CIV. CODE § 1798.100 (2024) (providing general duties and obligations of businesses that collect personal information); TEX. BUS. & COM. CODE §§ 541.051, 54.101 (West 2024) (providing consumer rights and covered entity duties with respect to personal data).

[137] *See, e.g.*, VA. CODE. ANN. § 59.1-575 (West 2023); COLO. REV. STAT. § 6-1-1303(17) (2024); CONN. GEN. STAT. § 42-515(26) (2023). *See also* CAL. CIV. CODE § 1798.140(v)(1) (defining personal information as information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household").

number of consumers (typically 25,000) and derives a certain amount of its revenue from the sale of personal information (typically 25% or 50%).[138] Some state privacy laws, however, exempt small businesses entirely from their scope.[139] For example, Utah and Tennessee require that businesses have $25 million in annual gross revenue to be subject to their privacy laws.[140]

Consumer Rights and Entity Obligations

These state comprehensive privacy laws provide a similar set of consumer rights, including the right to

- confirm whether a business collects their personal data;[141]
- obtain a copy of their personal data in a portable and readily usable format;[142]
- correct inaccuracies in their personal data;[143] and
- request that a business delete their personal data.[144]

All nineteen laws also have consumer opt-out and consumer consent requirements, although there are some differences. In terms of opt-out rights, most state privacy laws require businesses to let consumers opt out of the sale of their personal data.[145] Further, most state laws require businesses to let consumers opt out of the use of their personal data for targeted advertising or for automated decisionmaking (often referred to in state laws as "profiling") that produces legal or similarly significant effects.[146]

---

[138] *See, e.g.*, VA. CODE. ANN. § 59.1-576; COLO. REV. STAT. § 6-1-1304(1); CONN. GEN. STAT. § 42-516. The CCPA adds a third threshold that brings large businesses within the law's scope irrespective of the personal information they collect or sell. CAL. CIV. CODE § 1798.140(d). Under the CCPA, a business will be subject to the law if it (1) has more than $25 million in annual gross revenues; (2) alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households; or (3) derives 50% or more of its annual revenues from selling or sharing consumers' personal information. *Id.*

[139] *See, e.g.*, TEX. BUS. & COM. CODE § 541.002(a) (exempting small businesses as defined by the Small Business Administration).

[140] UTAH CODE ANN. § 13-61-102(1) (2024); TENN. CODE ANN. § 47-18-3303(1) (2025).

[141] *See, e.g.*, CAL. CIV. CODE § 1798.110; VA. CODE. ANN. § 59.1-577(A)(1); COLO. REV. STAT. § 6-1-1306(1)(b) (2024); TEX. BUS. & COM. CODE ANN. § 541.051(b)(1).

[142] *See, e.g.*, CAL. CIV. CODE § 1798.130(a)(3)(B)(iii); VA. CODE. ANN. § 59.1-577(A)(4); COLO. REV. STAT. § 6-1-1306(1)(e); TEX. BUS. & COM. CODE ANN. § 541.051(b)(4).

[143] *See, e.g.*, CAL. CIV. CODE § 1798.106; VA. CODE. ANN. § 59.1-577(A)(2); COLO. REV. STAT. § 6-1-1306(1)(c); TEX. BUS. & COM. CODE ANN. § 541.051(b)(2).

[144] *See, e.g.*, CAL. CIV. CODE § 1798.105; VA. CODE. ANN. § 59.1-577(A)(3); COLO. REV. STAT. § 6-1-1306(1)(d); TEX. BUS. & COM. CODE ANN. § 541.051(b)(3).

[145] *See, e.g.*, CAL. CIV. CODE § 1798.120; VA. CODE. ANN. § 59.1-577(A)(5); COLO. REV. STAT. § 6-1-1306(1)(a)(B); TEX. BUS. & COM. CODE ANN. § 541.051(b)(5)(B).

[146] *See, e.g.*, CAL. CIV. CODE §§ 1798.120, 1798.140(ah); VA. CODE. ANN. § 59.1-577(A)(5); COLO. REV. STAT. § 6-1-1306(1)(a)(C); TEX. BUS. & COM. CODE ANN. § 541.051(b)(5)(C). Rather than including requirements for automated-decision-making in the law itself, the CCPA directs the California Privacy Protection Agency (CPPA) to adopt regulations addressing this topic. CAL. CIV. CODE § 1798.185(a)(15). The CPPA has released draft automated decision-making regulations, which it voted to adopt on July 24, 2025. *See Modified Text of Proposed Regulations*, CAL. PRIV. PROT. AGENCY (May 9, 2025), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf [https://perma.cc/QNF3-LBS6]; *July 24, 2025 Board Meeting*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/meetings/materials/20250724.html [https://perma.cc/2SDP-H2H7] (last visited Aug. 13, 2025).

In terms of consent requirements, most state comprehensive privacy laws require that businesses obtain a consumer's affirmative consent before collecting or using their "sensitive"[147] personal data.[148] The CCPA, however, only requires that businesses give consumers the opportunity to opt out of the use of sensitive data, except for certain limited purposes.[149] Another distinction is that the CCPA mandates that businesses obtain consent before selling the personal data of teenagers ages thirteen to fifteen years old.[150] While several other state laws contain similar consent requirements for teenagers' personal data, many do not.[151]

The state comprehensive privacy laws contain a number of other similar entity obligations. For instance, nearly[152] every law requires companies to abide by a data minimization requirement, whereby they limit their use of personal information to what is reasonably necessary to achieve the purpose for which it was collected, as disclosed to the consumer.[153] Most laws also require companies to conduct data impact assessments, in which they must weigh the risks and benefits of certain activities (such as targeted advertising or automated decisionmaking).[154]

Enforcement and Rulemaking

Most state comprehensive privacy laws give exclusive enforcement authority to the state's attorney general.[155] These laws typically authorize the state attorney general to seek up to $7,500 in penalties per violation.[156] Others provide that violations constitute violations of state consumer protection statutes, thus incorporating the penalties from those statutes.[157]

Many of these state laws require the attorney general to give violators an opportunity to cure the violation before bringing an enforcement action,[158] although some state laws give the attorney

[147] Sensitive personal data is typically defined to include categories of data such as health data, geolocation data, and biometric data. *See, e.g.*, CAL. CIV. CODE § 1798.140(ae); VA. CODE. ANN. § 59.1-575.

[148] *See, e.g.*, VA. CODE. ANN. § 59.1-578(A)(5); COLO. REV. STAT. § 6-1-1308(7); TEX. BUS. & COM. CODE ANN. § 541.101(b)(4).

[149] CAL. CIV. CODE §§ 1798.121(a), 1798.135.

[150] *Id.* § 1798.120(c).

[151] *Compare* CONN. GEN. STAT. § 42-520 (requiring consent to process data of teenagers ages thirteen–fifteen years old) *with* VA. CODE. ANN. § 59.1-578 (silent on any covered entity obligations related to teenagers).

[152] Utah and Iowa's privacy laws do not have data minimization provisions. *See* IOWA CODE §§ 715D.1–715D.9 (2025); UTAH CODE ANN. §§ 13-61-101–13-61-404 (2024).

[153] *See, e.g.*, CAL. CIV. CODE § 1798.100(c); VA. CODE. ANN. § 59.1-578(A)(1)-(2); COLO. REV. STAT. § 6-1-1308(3)-(4); TEX. BUS. & COM. CODE ANN. § 541.101(a)(1), (b)(1). The CCPA likewise requires data impact assessments, although it directs the CPPA to adopt regulations specifying the requirements for these assessments rather than including those requirements in the law itself. *See* CAL. CIV. CODE § 1798.185(a)(14)(B).

[154] *See, e.g.*, VA. CODE. ANN. § 59.1-580; COLO. REV. STAT. § 6-1-1309; TEX. BUS. & COM. CODE ANN. § 541.105.

[155] *See, e.g.*, CONN. GEN. STAT. § 42-525; UTAH CODE ANN. § 13-61-402.

[156] *See, e.g.*, VA. CODE. ANN. § 59.1-584; UTAH CODE ANN. § 13-61-402; IOWA CODE § 715D.8; TEX. BUS. & COM. CODE ANN. § 541.155; IND. CODE § 24-15-10-2; TENN. CODE ANN. § 47-18-3312 (West 2025); OR. REV. STAT. § 646A.589 (2025).

[157] *See, e.g.*, CONN. GEN. STAT. § 42-525; 2024 Md. Laws ch. 455, § 1.

[158] *See, e.g.*, VA. CODE. ANN. § 59.1-584 (requiring attorney general to provide the violator with a thirty-day period to cure the violation); IOWA CODE § 715D.8 (requiring attorney general to provide the violator with a ninety-day period to cure the violation).

general discretion over whether to provide an opportunity to cure,[159] and some provide that the right-to-cure provision will sunset after a certain date.[160]

The CCPA's enforcement framework is distinct in that enforcement authority is shared between the state attorney general and the California Privacy Protection Agency (California PPA).[161] The CCPA authorizes the attorney general to bring civil suits, and it empowers the California PPA to pursue administrative enforcement.[162] Both civil and administrative enforcement actions may result in penalties up to $2,500 per violation or $7,500 for each intentional violation involving the personal information of minors.[163] The CCPA also provides a limited private right of action, whereby an individual may sue a company in certain circumstances where a security breach compromised the consumer's personal information.[164]

Most state privacy laws do not give any state agency authority to issue regulations implementing or expounding upon the laws' requirements. The CCPA, however, gives the California PPA broad rulemaking authority over its provisions and requires the agency to issue regulations on certain topics, such as risk assessments and businesses' use of automated decisionmaking technology.[165]

Colorado's law also gives the state attorney general authority to "promulgate rules for the purpose of carrying out [the law]" and requires it to adopt rules that create a "universal opt-out mechanism" allowing consumers to opt out of the sale of their data or the processing of their personal data for targeted advertising.[166]

Considerations for Congress

If Congress seeks to adopt new federal privacy laws, preemption of state law will be a key consideration. As described in the previous section, there is a complex array of state sectoral and comprehensive privacy laws. Any future federal privacy law will either displace or preserve these state laws, depending on Congress's intent.

In crafting a preemption regime, a salient decision for Congress is whether to include an express preemption provision or to rely on implied preemption. Federal laws, as discussed earlier in the report, may preempt state laws even without an express preemption provision. Under principles of implied preemption, a federal law will preempt state law when the state law conflicts with the federal law, or when the federal law regulates a topic so pervasively that it occupies the "field" and leaves no room for state law.[167] Congress could forego an express preemption provision if it wants reviewing courts to determine the scope of a law's preemption on a case-by-case basis through the application of these implied preemption principles.

[159] *See, e.g.*, N.J. STAT. ANN. § 56:8-166.17 (West 2025) (providing an opportunity to cure if "a cure is deemed possible" by the attorney general).

[160] MONT. CODE ANN. § 30-14-2817 (2024) (providing that right-to-cure provision terminates on April 1, 2026).

[161] CAL. CIV. CODE §§ 1798.155, 1798.199.90 (2025).

[162] *Id.*

[163] *Id.*

[164] *Id.* § 1798.150.

[165] *Id.* § 1798.185.

[166] COLO. REV. STAT. § 6-1-1313 (2023).

[167] *See supra* "Implied Preemption" for further discussion of implied preemption principles. *See also* "Implied Preemption," CRS Report R45825, *Federal Preemption: A Legal Primer*, by Bryan L. Adkins, Alexander H. Pepper, and Jay B. Sykes (2023).

On the other hand, an express preemption provision could define more specifically the scope of state laws that are preempted and could preempt state privacy laws that might not be impliedly preempted. In crafting an express preemption provision, Congress might use common phrases with meanings established by courts.[168] For instance, Congress could preempt any state laws on a subject matter "covered" by the federal law (i.e., the subject matter of the state law is "substantially subsumed" by the federal law). Alternatively, if Congress wants to preempt a broader swath of state law, it could preempt any state laws "related to" the federal law.

Congress could cabin the scope of an express preemption provision by including a savings clause. Savings clauses expressly preserve certain types of state laws or state remedies.[169] For instance, a savings clause could preserve state common law claims, to the extent they are not inconsistent with the federal law, or it could preserve certain sectoral state privacy laws. A savings clause could even preserve state law remedies by allowing states to provide additional liability or different remedies for a violation of a federal standard.[170] Some savings clauses, such as those in GLBA and HIPAA, aim to preserve states' ability to build on the federal law by only preempting inconsistent state laws and stating that a state law does not conflict with the federal law if it provides greater protections than the federal law.[171]

Congress could also delegate preemption decisions to a federal agency. As mentioned, some sector-specific federal privacy statutes, like GLBA, allow federal regulators to approve or preempt certain state regulations.[172] Congress can also give agencies the power to preempt state laws by giving them the power to issue regulations implementing the federal statute, as validly enacted regulations enjoy the same preemptive power under the Supremacy Clause as statutes.[173]

Preemption and Comprehensive Privacy Bills

In recent Congresses, there have been legislative efforts to adopt a comprehensive federal privacy law. Stakeholders have disagreed over how such a law should handle preemption. Some states with their own comprehensive privacy laws have been critical of any federal attempts to preempt their laws. For example, California's privacy agency, the California PPA, has argued against preemption by stressing the importance of states as "laboratories" of democracy, adopting innovative protections in response to new technologies and privacy challenges.[174] Industry groups, in contrast, have highlighted the challenges of navigating a complex landscape of divergent state privacy laws and have pushed for sweeping preemption. The U.S. Chamber of

[168] *See supra* "Express Preemption" for further discussion on how courts have interpreted common phrases in express preemption provisions, such has "covered" and "related to. *See also* "Express Preemption Clauses," CRS Report R45825, *Federal Preemption: A Legal Primer*, by Bryan L. Adkins, Alexander H. Pepper, and Jay B. Sykes (2023).

[169] *See supra* "Express Preemption" for a further discussion of savings clauses. *See also* "Savings Clauses," CRS Report R45825, *Federal Preemption: A Legal Primer*, by Bryan L. Adkins, Alexander H. Pepper, and Jay B. Sykes, Federal Preemption: A Legal Primer, by Bryan L. Adkins, Alexander H. Pepper, and Jay B. Sykes (2023).

[170] *See, e.g.*, Bates v. Dow Agrosciences LLC 544 U.S. 431, 448–50 (2005) (holding that Congress did not intend to deprive injured parties of state law remedies for the violation of federal standards when it prohibited state requirements "in addition to or different from" the federal requirements).

[171] 15 U.S.C. § 6807(b); 42 U.S.C. § 1320d-2, note; 45 C.F.R. § 160.203.

[172] 15 U.S.C. § 6807(b).

[173] *See* Fid. Fed. Sav. & Loan Ass'n v. De la Cuesta, 458 U.S. 141, 153 (1982) (explaining that validly enacted regulations have "no less pre-emptive effect" than statutes).

[174] Letter from Ashkan Soltani, Exec. Dir., Cal. Priv. Prot. Agency, to Representatives McMorris Rodgers and Gus Bilirakis, (Apr. 16, 2024), https://cppa.ca.gov/pdf/apra_discussion_draft.pdf [https://perma.cc/YS67-SGAT].

Commerce, for instance, has argued that perpetuating a "state patchwork of laws" would be "confusing to consumers" and "potentially impossible" for small businesses to comply with.[175]

Comprehensive privacy bills introduced in past Congresses have taken different approaches to preemption. Some, like the Online Privacy Act of 2023, would not have preempted state laws unless there was a direct conflict with the bill and specified that greater protections under state law did not constitute a conflict.[176]

Other bills would have broadly preempted most state data privacy laws. For example, a draft bill circulated in the 116th Congress would have preempted all state laws "related to the data privacy or security and associated activities of covered entities," except for state data breach notification laws.[177]

Finally, some bills would have combined general express preemption provisions with detailed savings clauses. For instance, the American Privacy Rights Act (APRA), introduced in the 117th Congress, and the American Data Privacy and Protection Act (ADPPA), introduced in the 118th Congress, would have preempted state laws that are "covered by" the provisions of those bills or the regulations promulgated under them.[178] In both bills, the express preemption provision was cabined by savings clauses preserving specific categories of state law, including consumer protection laws of general applicability, data breach notification laws, laws addressing the privacy rights of employees or employee information, and health privacy laws, among others.[179] ADPPA would have further preserved several particular state privacy laws, such as Illinois's Biometric Privacy Act and California's private right of action for victims of data breach.[180] In contrast, under APRA, these laws would not have been expressly preserved, although individuals would have been able to obtain the remedies provided by these laws in certain circumstances.[181]

Author Information

Chris D. Linebaugh
Legislative Attorney

[175] Letter from Jordan Crenshaw, Senior Vice President, U.S. Chamber of Com., to Representatives Gus Bilirakis and Janice Schakowsky (Apr. 17, 2024), https://www.uschamber.com/assets/documents/USChamber-APRA-Letter.pdf [https://perma.cc/G5D5-QLEC].

[176] H.R. 2701, 118th Cong. § 601(2023).

[177] United States Consumer Data Privacy Act of 2019, Staff Discussion Draft, § 404, 116th Cong. (2019), https://www.crs.gov/products/Documents/USCDPA_Draft/pdf [https://perma.cc/678N-N75U].

[178] APRA, H.R. 8818, 118th Cong. § 118(a)(2) (2024); ADPPA, H.R. 8152, 117th Cong. § 404(b)(1) (2022). *See also* CRS Legal Sidebar LSB11161, *The American Privacy Rights Act*, by Chris D. Linebaugh et al. (2024); CRS Legal Sidebar LSB10776, *Overview of the American Data Privacy and Protection Act, H.R. 8152*, by Jonathan M. Gaffney, Eric N. Holmes, and Chris D. Linebaugh (2022).

[179] H.R. 8818 § 118(a)(3); H.R. 8152 § 404(b)(2).

[180] H.R. 8152 § 404(b)(2)(M), (R).

[181] H.R. 8818 §§ 117(a)(2)(B)–(C), 118(a)(3).

Disclaimer