

Preemption in U.S. Federal Privacy Laws

Summary: In this table, we compile twelve (12) leading federal sectoral privacy laws in the United States that apply to commercial entities (with the exception of DPPA, which primarily applies to state government entities) and provide summarized legal analysis of their preemptive effect on similar or supplementary state laws. As a discussion draft, this document is intended to: 1) assist policymakers considering the extent to which a federal comprehensive privacy law ought to preempt similar state efforts; and 2) demonstrate the wide range of paths Congress has taken with respect to preemption in previous privacy laws.

Please send feedback to sgray@fpf.org

Contributors: Stacey Gray (FPF), Polly Sanderson (FPF), and Felicity Slater (FPF)

Table of Contents: *(in approximate order of original passage)*

1. The Wiretap Act (1968)	2
2. Fair Credit Reporting Act (FCRA) (1970)	2
3. Family Educational Rights and Privacy Act (FERPA) (1974)	4
4. Cable Communications Policy Act (CCPA) (1984)	4
5. Employee Polygraph Protection Act (EPPA) (1988)	5
6. Video Privacy Protection Act (VPPA) (1988)	6
7. The Telephone Consumer Protection Act (TCPA) (1991)	6
8. Driver's Privacy Protection Act (DPPA) (1994)	8
9. Children's Online Privacy Protection Act (COPPA) (1998)	9
10. Gramm-Leach-Bliley Act (GLBA) (1999)	10
11. The Health Insurance Portability and Accountability Act (HIPAA) (1999)	11
12. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act (2003)	13

Statute	Overview and Statutory Language	Summary of Preemptive Effect
<p>1. The Wiretap Act (1968)¹</p>	<p><i>Title I of ECPA, usually referred to as “The Wiretap Act,” governs U.S. Government agents and employees, as well as non-governmental individuals and groups, for intentional, unauthorized wiretapping of wire, oral, or electronic communications. The Act grants individuals who are subject to unlawful interception of communications the right to equitable and declaratory relief, damages, attorney’s fees, and court costs.</i></p> <p><i>[No general preemption provisions.]</i></p>	<p>The Wiretap Act does not preempt state regulatory efforts imposing additional requirements so long as they adhere to the federal minimum standards.² Eleven states require two-party (or “all-party”) consent prior to recording an oral communication.³ Hawai’i is generally a one-party consent state, but, when the recording device is put in a private location, requires two-party consent.⁴</p>
<p>2. Fair Credit Reporting Act (FCRA) (1970)⁵</p>	<p><i>The Fair Credit Reporting Act (FCRA) regulates the collection and use of consumer data by credit reporting agencies (CRAs) for the purpose of providing credit reports, including, e.g., in lending and employment decisions. FCRA also gives consumers rights to access, verify, and dispute the accuracy of information in credit reports.</i></p> <p>“Except as provided in subsections (b) and (c), this title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to the collection, distribution, or use of any information on consumers, or for the prevention or mitigation of identity theft, except to the extent that those laws are inconsistent with any provision of this title, and then only to the extent of the inconsistency.” 15 USC § 1681(t)(a)</p>	<p>FCRA currently preempts state laws broadly in two categories: (1) any state laws that govern particular subject matters as applied to a consumer reporting agency (CRA) (subject matter preemption); and (2) common law claims based on disclosures not involving malice or willful intent.</p> <p>As a result, courts often dismiss state statutory, tort, or contract claims as preempted when claims involve activities listed in 15 USC 1581(t)(b) or arise out of disclosures in consumer reports (e.g. defamation). See, e.g., <i>Shah v. Wells Fargo Bank</i></p>

¹ 18 U.S. Code § 2510-2523.

² See *Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, UNITED STATES DEPARTMENT OF JUSTICE, <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1284>; see also [Senate Report on the Omnibus Crime Control and Safe Streets Act of 1968 \(Judiciary Committee\)](#), Sen. Rep. No. 1097, 90th Cong., 2d Sess., U. S. Code Cong. & Adm. News 1968, at 69 (commenting that “[18 USC § 2516(2)] envisions that States would be free to adopt more restrictive legislation, or no legislation at all, but not less restrictive legislation.”).

³ California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania, and Washington. See Recording Phone Calls and Conversations, Digital Media Law Project, <https://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations>.

⁴ HAW. REV. STAT. §711-1111 (2021).

⁵ 15 U.S.C. §§ 1681 *et seq* (as amended over the years (originally passed in 1970). See the Federal Trade Commission’s most recent complete text of the Fair Credit Reporting Act (last revised 2018), *available at* https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf.

	<p>“No requirement or prohibition may be imposed under the laws of any State—with respect to any subject matter regulated under—” [sections regulating:</p> <ul style="list-style-type: none"> ● <i>prescreening of consumer reports;</i> ● <i>time periods in which a CRA must take actions (e.g. notification, disputed accuracy);</i> ● <i>information in consumer reports;</i> ● <i>responsibilities of persons who furnish information to CRAs;</i> ● <i>exchanges of information regarding solicitation for marketing purposes;</i> ● <i>duties of users of consumer reports to provide certain notice;</i> ● <i>security freezes;</i> ● <i>duties of users of consumer reports to provide notice with respect to terms in certain credit transactions;</i> ● <i>duties of a person who takes an adverse action with respect to a consumer;</i> ● <i>requirements relating to the “disclosure of credit scores for credit granting purpose,” subject to exceptions for certain specified existing laws in CA and CO;</i> ● <i>frequency of annual disclosures (with exceptions for specific state laws in effect on December 4, 2003, (e.g. CO, GA, ME, MD, MA, NJ, and VT).]</i> 15 USC § 1681(t)(b) <p>“Notwithstanding any definition of the term “firm offer of credit or insurance” (or any equivalent term) under the laws of any State, the definition [in FCRA] shall be construed to apply in the enforcement and interpretation of the laws of any State governing consumer reports.” 15 USC § 1681(t)(c)</p> <p>“Except as provided in sections 1681n and 1681o [willful or negligent noncompliance], no consumer may bring any action or proceeding in the nature of defamation, invasion of privacy, or negligence . . . based on information disclosed pursuant to section 1681g, 1681h, or 1681m of this title, or based on information disclosed by a user of a consumer report to or for a consumer against whom the user has taken adverse action, based in whole or in part on the report except as to false information furnished with malice or willful intent to injure such consumer.” 15 USC s1681h(e)</p>	<p>(Ind. App. Sept. 25, 2018) (preempting a claim that a bank provided inaccurate billing statements to credit agencies). State laws may occasionally go beyond FCRA, for example if they create requirements that do not fall into any 1681(t)(b) categories. See, e.g., <i>Walters v. Certegy Check Servs. Inc.</i>, No. A-17-CV-1100-SS, 2018 WL 4762141 (W.D. Tex. Oct 2, 2018) (allowing a claim to proceed under the Texas Business and Commercial Code that would require additional disclosures on a reinvestigation report).</p> <p>FCRA also has two notable features that are unique (to this list) and may be helpful:</p> <ul style="list-style-type: none"> ● a preemptive definition (“firm offer of credit or insurance”) that must be followed, even in the interpretation of state credit reporting laws; and ● a “preemption sunset clause,” implemented in 1996, indicating that state credit reporting laws would be permitted after January 1, 2004 if they “explicitly [stated] that the provision is intended to supplement [FCRA]”; and “[gave] greater protection to consumers than is provided under this title.”⁶ In 2003, the preemption provisions in FCRA were extended indefinitely.⁷
--	--	---

⁶ Making omnibus consolidated appropriations for the fiscal year ending September 30, 1997, and for other purposes, Pub. L. No. 104-208, 110 Stat. 3009 (<https://www.govinfo.gov/content/pkg/PLAW-104publ208/pdf/PLAW-104publ208.pdf>).

⁷ Margaret Mikung Lee, *Fair Credit Reporting Act: Preemption of State Law*, Congressional Research Service (Dec. 8, 2003), https://digital.library.unt.edu/ark:/67531/metadc817121/m2/1/high_res_d/RS21449_2003Dec08.pdf.

<p>3. Family Educational Rights and Privacy Act (FERPA) (1974)⁸</p>	<p><i>The Family Educational Rights and Privacy Act (FERPA) conditions federal funding of educational institutions on requirements to not disclose student information except in specified circumstances, including with parental consent. It also affords parents the right to access and control their children’s educational records.</i></p> <p>“Nothing in subparagraph (E) [disclosure to child welfare agencies, caseworkers, or tribal associations] shall prevent a State from further limiting the number or type of State or local officials who will continue to have access thereunder.” 20 U.S.C. § 1232g(b)(1)(L)</p> <p>“Nothing in paragraph (1) [disclosure in cases of drug and alcohol violations] shall be construed to supersede any provision of State law that prohibits an institution of higher education from making the disclosure . . .” 20 U.S.C. § 1232g(i)</p>	<p>In general, FERPA does not preempt state laws, even laws that prohibit disclosures that FERPA would otherwise allow. 20 U.S.C. § 1232g. As a result, state laws that establish stricter privacy requirements for student records have proliferated.⁹</p> <p>In some cases, conflicts arise between FERPA and state “right to know” or “freedom of information” (FOI) laws. In such cases, FERPA is likely to prevail.¹⁰</p>
<p>4. Cable Communications Policy Act (CCPA) (1984)¹¹</p>	<p><i>The Cable Communications Policy Act (CCPA or “Cable Act”), which amended the Communications Act of 1934, applies to cable operators and service providers. The Cable Act’s privacy provisions require cable operators to provide written privacy policies, provide subscribers access to their personal information, and limit the collection and disclosure of subscriber personal information without prior written or electronic consent.¹²</i></p> <p>“Nothing in this subchapter shall be construed to prohibit any State or any franchising authority from enacting or enforcing laws consistent with this section for the protection of subscriber privacy.” 47 USC § 551(g).</p>	<p>Despite the text of the Cable Act, the Federal Communications Commission (FCC) has prevailed in establishing preemptive national standards, and “federal law dominates the shape of cable television regulation.”¹³ See, e.g., <i>Capital Cities v. Crisp</i>, 467 U.S. 691 (1984) (affirming the FCC’s power to preempt state cable laws, noting that the agency has “for the past 20 years unambiguously expressed its intent to preempt state or local regulation of any type of signal carried by cable television systems.”).</p> <p>Some current state laws that do govern cable operators may simply incorporate the Cable Act</p>

⁸ Family Education Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232(g), amended by 12 Stat. 2480 (2013).

⁹ See, e.g., *State Student Privacy Laws*, Student Privacy Compass, <https://studentprivacycompass.org/state-laws/> (last visited: Jun. 2, 2021).

¹⁰ See, e.g., *DTH Publishing Corp. v. University of North Carolina at Chapel Hill*, 496 S.E.2d 8, 10-11 (N.C. Ct. App. 1998) (holding that FERPA “make[s] student education records ‘privileged or confidential’” for North Carolina open records law purposes); *U.S. v. Miami Univ.*, 294 F.3d 797, 811 (finding that “Ohio Public Records Act does not require disclosure of records the release of which is prohibited by federal law.”).

¹¹ Pub. L. No. 98-549, codified at 47 U.S.C. § 521-573.

¹² An Act To Amend the Communications Act of 1934 to Provide a National Policy Governing Cable Television, [Pub. L. No. 98-549](#) 98 Stat. 2779 (1984) (codified at 47 U.S.C. § 521-573).

¹³ Cameron F. Kerry and John B. Morris, Jr., Preemption: A balanced national approach to protecting all Americans’ privacy, BROOKINGS (Jun. 29, 2020), <https://www.brookings.edu/blog/techtank/2020/06/29/preemption-a-balanced-national-approach-to-protecting-all-americans-privacy/>.

		<p>by reference into state law. See, e.g., Illinois, 220 ILL. Comp. Stat. 5/22-501 (West 2021), and Missouri (MO Ann. Stat. §67.2694 (West 2021).</p>
<p>5. Employee Polygraph Protection Act (EPPA) (1988)¹⁴</p>	<p><i>The Employee Polygraph Protection Act (EPPA) prohibits most private employers from using lie detector tests, either for pre-employment screening or during the course of employment. Where polygraph examinations are allowed, they are subject to strict standards for the conduct of the test, including the pretest, testing and post-testing phases. An examiner must be licensed and bonded or have professional liability coverage. The Act strictly limits the disclosure of information obtained during a polygraph test.</i>¹⁵</p> <p>“Except as provided in subsections (a), (b), and (c) of section 2006 of this title,* this chapter shall not preempt any provision of any State or local law or of any negotiated collective bargaining agreement that prohibits lie detector tests or is more restrictive with respect to lie detector tests than any provision of this chapter.” 29 U.S. Code § 2009. [<i>* Subsections (a), (b), and (c) of section 2006 establish exemptions for federal government employees, national defense, and security.</i>]</p> <p>“§ 801.5 Effect on other laws or agreements. (a) Section 10 of EPPA provides that the Act, except for subsections (a), (b), and (c) of section 7, does not preempt any provision of a State or local law, or any provision of a collective bargaining agreement, that prohibits lie detector tests or is more restrictive with respect to the use of lie detector tests. (b) (1) This provision applies to all aspects of the use of lie detector tests, including procedural safeguards, the use of test results, the rights and remedies provided examinees, and the rights, remedies, and responsibilities of examiners and employers. . . . (3) On the other hand, industry exemptions and applicable restrictions thereon, provided in EPPA, would preempt less restrictive exemptions established by State law for the same industry, e.g., random testing of current employees in the drug industry</p>	<p>The EPPA provides a clear example of “floor” preemption. It establishes minimum requirements for a range of permissible uses of polygraph tests by private employers, but permits states and local governments to create more restrictive rules, including prohibiting their use.</p> <p>At least 30 states and the District of Columbia have prohibited or passed more restrictive laws regarding polygraph tests,¹⁶ including:</p> <ul style="list-style-type: none"> ● Prohibiting their use on state employees and employees subject to investigations, and even by employers who run security services or work with controlled controlled substances (which federal law would otherwise permit); ● Requiring that an employee receive advance, written notice before being subject to a polygraph exam; ● Establishing higher penalties for violation of the state polygraph law (including criminal penalties; or ● Establishing licensing requirements for polygraph operators.

¹⁴ 29 U.S. Code § 2009 et seq

¹⁵ See generally, *Employee Polygraph Protection Act*, U.S. Department of Labor, [dol.gov/agencies/whd/polygraph](https://www.dol.gov/agencies/whd/polygraph) (last visited: Jun. 2, 2021); Fact Sheet #36: Employee Polygraph Protection Act of 1988, U.S. Department of Labor, <https://www.dol.gov/agencies/whd/fact-sheets/36-eppa> (last visited: Jun. 2, 2021), Fact Sheet #44: Visits to Employers, U.S. Department of Labor, <https://www.dol.gov/agencies/whd/fact-sheets/44-flsa-visits-to-employers> (last visited: Jun. 2, 2021).

¹⁶ See, e.g., Alaska Stat. § 23.10.037 (2021); N.M. STAT. ANN. § 29-14-5 (2021); Wis. Stat. Ann. § 111.37 (2021) (full list on file with authors).

	<p>not prohibited by State law but limited by this Act to tests administered in connection with ongoing investigations.” 29 CFR §801.5</p>	
<p>6. Video Privacy Protection Act (VPPA) (1988)¹⁷</p>	<p><i>The Video Privacy Protection Act of 1988 (VPPA) prohibits video tape rental services from releasing consumer’s video tape rental records without that consumer’s specific, informed, and written prior consent. VPPA allows law enforcement agents to collect such information only with a warrant or court order.</i></p> <p>“The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.” 18 USC § 2710 (f)</p>	<p>The VPPA does not preempt state laws that would impose additional requirements on covered entities (video tape service providers).</p> <p>As a result, there are many state laws that establish protections for video rental records beyond those in VPPA. For example¹⁸:</p> <ul style="list-style-type: none"> • Connecticut¹⁹ bans the sharing or sale of video rental records and creates a cause of action for consumers whose records have been circulated to sue. • Michigan²⁰ also forbids the disclosure of rental records to anyone but the consumer, and includes books, written materials, and sound recordings.
<p>7. The Telephone Consumer Protection Act (TCPA) (1991)²¹</p>	<p><i>The Telephone Consumer Protection Act (TCPA) regulates the use of automatic telephone dialing systems and artificial or prerecorded voice messages in telemarketing calls. Covered entities, including telemarketers, must obtain prior written consent from consumers prior to robocalling them, and provide opt-out mechanisms.</i></p> <p><i>The Federal Communications Commission (FCC) has broad rulemaking authority under the Act, and in 2003 established, in coordination with the Federal Trade Commission (FTC), a national Do-Not-Call Registry. Telemarketers and other covered entities are prohibited from making telemarketing calls to numbers on the registry without express, written agreement or in the context of an established business relationship.</i></p>	<p>In general, the TCPA does not preempt state laws that create more restrictive requirements for telemarketers, or prohibit certain activities (e.g. the use of fax machines to send unsolicited advertisements). However, the law does require (and preempts state laws that differ from) certain “technical and procedural standards,” to be promulgated by the FCC.</p> <p>Between 2003-2005, the FCC received at least</p>

¹⁷ 18 U.S.C. §§ 2710 et seq

¹⁸ For a helpful review of VPPA, its 2011 amendments, state video rental laws, and relevant case law, see *Video Privacy Protection Act*, ELECTRONIC INFORMATION PRIVACY CENTER, <https://epic.org/privacy/vppa/> (last visited: 5/25/21).

¹⁹ CT. Gen. Stat. § 53-450 (2021).

²⁰ Mich. Comp. Laws § 445.1711 (2021).

²¹ 47 U.S. Code § 227 (b)(2).

	<p>“Except for the standards prescribed under subsection (d) [technical and procedural standards] and subject to paragraph (2) of this subsection, nothing in this section or in the regulations prescribed under this section shall preempt any State law that imposes more restrictive intrastate requirements or regulations on, or which prohibits—</p> <p>(A) the use of telephone facsimile machines or other electronic devices to send unsolicited advertisements;</p> <p>(B) the use of automatic telephone dialing systems;</p> <p>(C) the use of artificial or prerecorded voice messages; or</p> <p>(D) the making of telephone solicitations.” 47 USC § 227(f)(1)</p> <p>“If . . . the Commission requires the establishment of a single national database of telephone numbers of subscribers who object to receiving telephone solicitations, a State or local authority may not, in its regulation of telephone solicitations, require the use of any database, list, or listing system that does not include the part of such single national database that relates to such State.” 47 USC § 227(f)(2).</p>	<p>ten petitioners for a declaratory ruling on preemption of state telemarketing laws (dismissed in 2020).²² Despite this, courts have often upheld state telemarketing laws against preemption claims. See, e.g., <i>State ex rel. Stenehjem v. FreeEats.com, Inc.</i>, 712 N.W.2d 828, 841 (Del. 2006) (upholding a North Dakota law prohibiting interstate political calls to state residents, which would otherwise be permitted under TCPA regulations).</p> <p>Today, many states have laws governing telemarketers,²³ including laws that: require state registration to engage in telemarketing; do not recognize the TCPA “established business relationship exception” in all circumstances;²⁴ prohibit the sending of “pre-recorded voice” messages;²⁵ explicitly forbid sending of unsolicited commercial text messages;²⁶ forbid blocking caller ID;²⁷ require telemarketers to provide their “own true names” within the first 30 seconds of a call.²⁸</p> <p>Additionally, many states still maintain state</p>
--	--	---

²² See, ex. [Consumer & Governmental Affairs Bureau Seeks Comment on Express Consolidation, Inc. Petition for Declaratory Ruling on Preemption of Florida Telemarketing Rules](#), 69 Fed. Reg. 61381 (Oct. 18, 2004); [Consumer & Governmental Affairs Bureau Seeks Comment on CCA Advertising Petition for Declaratory Ruling on Preemption of North Dakota Telemarketing Rules](#), 69 Fed. Reg. 61380 (Nov. 17, 2004); See CGB dismisses nine preemption petitions, FEDERAL COMMUNICATIONS COMMISSION (Dec. 17, 2020), <https://www.fcc.gov/document/cgb-dismisses-nine-preemption-petitions>.

²³ LexisNexis State Telemarketing Laws 50 State Survey (on file with authors). See also, *Telemarketing and the Telephone Consumer Protection Act (TCPA)*, ELECTRONIC INFORMATION PRIVACY CENTER, <https://epic.org/privacy/telemarketing/%0D> (last visited: Jun. 3, 2021)

²⁴ N.J. STAT. ANN. § 56:8-128 (2021); IND. CODE § 24-4.7-4-1 (2021); WIS. STAT. § 100.52 (2021).

²⁵ N.D. CENT. CODE § 51-28-02 (2021).

²⁶ CONN. GEN. STAT. § 42-288(a)(7) (2021).

²⁷ CONN. GEN. STAT. § 42-288(a)(12) (2021).

²⁸ ALA. CODE § 8-19A-12 (2021).

		<p>do-not-call registries, although many have adopted the national Do-Not-Call list (with state penalties attached).²⁹ A few states maintain more expansive lists. For example, Texas maintains two do not call registries, with one allowing businesses to register their telephone numbers to avoid solicitation calls from retail electric providers (Tex. Utilities Code § 39.1025).</p>
<p>8. Driver’s Privacy Protection Act (DPPA) (1994)³⁰</p>	<p><i>The Driver’s Privacy Protection Act (DPPA) prohibits State Departments of Motor Vehicles (DMVs) and their employees from disclosing, selling, or using certain personal information associated with motor vehicle records without drivers’ express consent. The law requires driver’s express consent for certain disclosures. It was passed in the aftermath of a series of crimes, including stalking, murders, and robberies, which were committed by perpetrators who used information about their victims obtained from motor vehicle records, using the victim’s license plate numbers.</i>³¹</p> <p>“No State may condition or burden in any way the issuance of an individual’s motor vehicle record as defined in 18 U.S.C. 2725(1) to obtain express consent. Nothing in this paragraph shall be construed to prohibit a State from charging an administrative fee for issuance of a motor vehicle record.” 18 USC § 2721(e).</p>	<p>The DPPA, with a few narrow exceptions, provides a baseline but does not preempt state laws that provide greater protections for motor vehicle records. Many states have laws that are stricter than DPPA.³²</p> <p>After it was passed, DPPA was challenged on 10th Amendment grounds. In <i>Reno v. Condon</i>, 528 U.S. 141 (2000), the Supreme Court upheld the constitutionality of DPPA, finding that the law was generally applicable and was a valid exercise of Congress’ power to regulate interstate commerce.</p>

²⁹ See Kathleen Ann Ruane, *Telemarketing Regulation: National and State*

Do Not Call Registries, CONGRESSIONAL RESEARCH SERVICE (Apr. 1, 2016), <https://fas.org/sgp/crs/misc/R43684.pdf>

³⁰ 18 U.S. Code § 2721, amended by Pub. L. 106–346, § 101(a) [title III, § 309(c)–(e)], Oct. 23, 2000, 114 Stat. 1356, 1356A–24.

³¹ See generally, *The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record*, Electronic Information Privacy Center, <https://epic.org/privacy/drivers/> (last visited: Jun. 3, 2021).

³² For example, Alaska law restricts the release of driver’s license information to the license holder, their legal guardian, or government officials (fewer entities than are permitted under DPPA). ALASKA STAT. § 28.15.151 (2021). California law allows certain individuals, including judges, public defenders, and social workers, to make their addresses confidential on their DMV records. CAL. VEHICLE CODE § 1808.4(a) (2021).

<p>9. Children’s Online Privacy Protection Act (COPPA) (1998)³³</p>	<p><i>The Children’s Online Privacy Protection Act (COPPA) imposes requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.</i></p> <p>“No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.” 15 USC 6502(d).</p>	<p>COPPA strongly preempts state laws that create liability for commercial activities involving the collection of PII from children under 13 through online services, in a manner that is inconsistent with the liability imposed by COPPA.</p> <p>As a result, state common law remedies for claims involving data collection from children are sometimes, but not always, preempted. As COPPA-related lawsuits have proliferated in recent years, there has been some variability in judicial interpretations.</p> <p>The following recent four cases are illustrative:</p> <ul style="list-style-type: none"> • <i>In Re Nickelodeon Consumer Privacy Litigation</i>, 827 F.3d 262 (3d Cir. 2016) (finding that a state common law claim of “intrusion upon seclusion” was not inconsistent with COPPA, and thus not preempted, in a case alleging that Viacom promised not to collect any PI about children on its websites and then did so). • <i>Manigault-Johnson v. Google, LLC</i>, Civ. Act. No. 2:18-cv-1032 BHH, slip. op. at *17-20 (D. S.C. Mar. 31, 2019) (dismissing an “intrusion upon seclusion” claim based on collection of PI from children under 13 from websites and apps; distinguishing from <i>In Re Nickelodeon</i> insofar as the latter involved deceptive statements beyond COPPA). • <i>New Mexico ex rel. Balderas v. Tiny Lab Prods.</i>, 457 F. Supp. 3d. 1103 (D. N.M. 2020)
---	--	--

³³ The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.

		<p>(dismissing state law claims against third party SDK networks that would impose liability without actual knowledge, due to being inconsistent with - and thus preempted by - COPPA, but not finding preemption of state claims against Google that were consistent with COPPA).</p> <ul style="list-style-type: none"> • <i>Hubbard v. Google LLC</i>, No. 19-cv-07016-BLF, slip. op at. *19-20 (N.D. Cal. 2020) (dismissing state tort claims against Google as inconsistent with, and thus preempted by, COPPA); <p>State legal protections for teens (13 and older) are likely not preempted. See the FTC’s amicus brief in <i>Batman v. Facebook</i> (9th Cir. 2014) (making a compelling argument against implied or field preemption of protections for teens).</p>
<p>10. Gramm-Leach-Bliley Act (GLBA) (1999)³⁴</p>	<p><i>The Gramm-Leach-Bliley Act (GLBA) re-structured the financial services industries in 1999 (previously regulated under the Glass-Steagall Act of 1933). GLBA authorizes widespread sharing of non-public personal information by financial institutions with affiliated companies, and with non-affiliated companies subject to the right of individuals to “opt out.” 6802(b). The law also requires privacy notices and limits disclosure of certain sensitive information (such as account numbers). The FTC Safeguards Rule (finalized in 2002) establishes further requirements, including that financial institutions implement a comprehensive information security program.</i></p>	<p>GLBA expressly does not preempt state laws that are more protective of consumers with respect to data privacy, although other features of the law (such as the ability of financial institutions to freely affiliate) are preemptive.</p> <p>Many states have financial privacy laws that exceed the requirements in GLBA,³⁵ including a</p>

³⁴ Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (codified primarily at 15 U.S.C. §§ 6801-6809, §§ 6821-6827).

³⁵ For helpful reviews of state financial privacy laws, we recommend CALPIRG Education Fund, *Financial Privacy In The States* (Feb 2004), available at <https://frontiergroup.org/sites/default/files/reports/CA-Financial-Privacy-in-the-States-text-cover.pdf>, and Goodwin-Proctor, *Gramm-Leach-Bliley: Tip of the Privacy Iceberg* (2001), available at https://www.goodwinlaw.com/~media/Files/Publications/Attorney%20Articles/2001/Gramm_Leach_Bliley_Tip_of_the_Privacy_Iceberg.ashx. See also, generally, Solove & Schwarz *Information Privacy Law*, Sixth Edition, 773-76.

	<p>“(a) In general. This subchapter and the amendments made by this subchapter shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency.</p> <p>(b) Greater protection under State law. For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter, as determined by the Bureau of Consumer Financial Protection, after consultation with the agency or authority with jurisdiction under section 6805(a) of this title of either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party.” 15 USC § 6807.</p> <p><i>Note: GLBA contains additional specific preemption provisions (not discussed here) that prevent states from restricting the ability of banks and other depository institutions and their affiliates from freely affiliating, with some exceptions, and preserves certain state laws related to insurance activities. 15 USC 6701(c)-(d).</i></p>	<p>number of states - California,³⁶ Vermont,³⁷ North Dakota, and others - that require an “opt in” for sharing of personal information by financial institutions with non-affiliated companies (in contrast to GLBA’s “opt-out”).</p> <p>At least one such law, California’s SB-1, was challenged on preemption grounds and the opt-in provision survived. <i>American Bankers Ass’n v. Lockyer</i>, 541 F.3d 1214 (9th Cir. 2008) (preempting other aspects of SB-1 that were governed by FCRA).</p>
<p>11. The Health Insurance Portability and Accountability Act (HIPAA) (1999)³⁸</p>	<p><i>The Health Insurance Portability and Accountability Act (HIPAA) governs health plans, health care clearinghouses, and health care providers and their business associates. HIPAA’s Privacy Rule regulates the way in which entities subject to HIPAA may use and disclose sensitive health information, setting limits for how this information can be used, requiring patient consent for certain users, and establishing patient rights over their personal information.</i>³⁹</p> <p>“A standard, requirement, or implementation specification adopted under this</p>	<p>HIPAA establishes minimum legal protections and preempts contrary state legislation, while allowing states to pass additional requirements, including those that provide greater privacy protections.</p> <p>In addition, however, HIPAA explicitly reserves state powers to conduct certain data collection activities related to public health surveillance,</p>

³⁶ California Financial Information Privacy Act (“SB-1”), Cal. Fin. Code §§ 4050-4060 (2021).

³⁷ State of Vermont, Department, Insurance, Securities & Health Care Administration, Banking Division, Regulation B-2001-01, Privacy of Consumer Financial and Health Information Regulation.

³⁸ The Health Insurance Portability and Accountability Act of 1996 Title II, 42 U.S.C. §§ 1320d-1320d-9.

³⁹ *To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, https://privacyruleandresearch.nih.gov/pr_06.asp#:~:text=Covered%20entities%20are%20defined%20in,which%20HHS%20has%20adopted%20standards (last visited: May 27, 2021); *The HIPAA Privacy Rule*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> (last visited: May 27, 2021).

	<p>subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:</p> <p>(a) A determination is made by the Secretary under § 160.204 that the provision of State law: (1) Is necessary: (i) To prevent fraud and abuse related to the provision of or payment for health care; (ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation; (iii) For State reporting on health care delivery or costs; or (iv) For purposes of serving a compelling need related to public health, safety, or welfare . . . ; or (2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances . . .</p> <p>(b) The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.</p> <p>(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.</p> <p>(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.” 45 CFR § 160.203.</p>	<p>reporting of disease or injury, child abuse, birth, or death; or require certain health plan reporting, such as for management or financial audits. 45 CFR § 160.203(A)(i-iv).</p> <p>Notably, HIPAA also allows HHS, “upon specific request from a State or other entity or person” to preserve a provision of State law that would otherwise be preempted, on a case-by-case basis. 45 CFR § 160.204(a)(1-6).</p> <p>At least one scholar has argued that the statutory text of HIPAA is more preemptive of state law than is HHS’s Privacy Rule, preempting state laws that would interfere with any important public health law, state or federal.⁴⁰</p> <p>Many states have health privacy laws, including comprehensive laws pertaining to medical information, that supplement HIPAA, including:</p> <ul style="list-style-type: none"> ● limiting disclosures made by additional entities (such as state agencies,⁴¹ or nursing homes and long-term care facilities⁴²); ● establishing greater protections for certain types of records (such as mammograms⁴³ or mental health⁴⁴); or
--	---	---

⁴⁰ Barbara J. Evans, *Institutional Competence to Balance Privacy and Competing Values: The Forgotten Third Prong of HIPAA Preemption Analysis*, 46 U.C. DAVIS L. REV. 1175, 1200 (2013) (“The basic directive of [U.S.C.] §1320d-7(b) is that privacy laws -- not just the Privacy Rule, but any state privacy laws that the Privacy Rule fails to preempt -- must give way if they interfere with important public health laws.”)

⁴¹ See, e.g., CAL. CIV. CODE § 1798.24 (2021) (prohibiting state agencies from disclosing personal health information without the subject’s written consent, with exceptions).

⁴² See, e.g., ALA. ADMIN. CODE tit. 7, § 12.890 (2021) (requiring that nursing homes inform patients of their right to confidentiality in writing); FLA. STAT. ANN. § 400.022 (2021) (exempting nursing home records from public access under the Public Records Act).

⁴³ See, e.g., MASS. CODE REGS. § 127.020(D)(2) (2021) (classifying mammogram records as confidential information that cannot be disclosed without a patient's consent).

⁴⁴ See, e.g., HAW. REV. STAT. § 334-5 (2021) (classifying information about mental health care, alcoholism, and addiction as confidential and limiting the circumstances under which it may be disclosed).

	<p>“A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the [HHS] Secretary . . . by a State . . . through its chief elected official, or his or her designee <i>[subject to administrative requirements]</i>.” 45 CFR § 160.204(a)(1-6).</p>	<ul style="list-style-type: none"> • limiting, or in some cases mandating, disclosure of information related to particular health conditions (such as HIV/AIDs,⁴⁵ cancer,⁴⁶ or birth defects⁴⁷); or • establishing more stringent penalties, including private rights of action, to violations of medical confidentiality.⁴⁸
<p>12. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act (2003)⁴⁹</p>	<p><i>The CAN-SPAM Act (“Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003”) establishes requirements for transparency and control in the sending of commercial e-mail, including requiring businesses to respect consumer requests to opt-out or unsubscribe.</i></p> <p>“This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages...” 15 USC § 7707 (b)(1)</p> <p>“...except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.” 15 USC § 7707 (b)(1). “This chapter shall not be construed to preempt the applicability of— (A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or (B) other State laws to the extent that those laws relate to acts of fraud or computer crime.” 15 USC § 7707 (b)(2)</p>	<p>CAN-SPAM strongly preempts any state law that regulates the sending of electronic mail for commercial purposes. 15 USC § 7707 (b)(1). When it came into effect in 2004, this preempted a wide variety of existing state anti-spam laws that had established labeling, opt-in, or opt-out requirements for unsolicited commercial email.⁵⁰</p> <p>CAN-SPAM does not preempt (through a Savings Clause) generally applicable state laws, for example against deceptive trade practices, deceptive communications, or banning the sale of spam software.</p>

⁴⁵ See, e.g., ARK. CODE. ANN. § 20-15-904 (2021) (requiring that physicians report a patient's positive HIV/AIDs test results to the Department of Health).

⁴⁶ See, e.g., KAN. STAT. ANN. § 65-1, 171-172 (2021) (classifying information in Kansas’s cancer registry as confidential, may not be disclosed without patient’s consent).

⁴⁷ See, e.g., OHIO REV. CODE. ANN. § 3705.32 (2021) (classifying information in Ohio’s birth defect registry as confidential, may not be disclosed without parent or guardian’s consent).

⁴⁸ See, e.g., California’s Confidentiality of Medical Information Act (CMIA), CAL. CIV. CODE §§ 56-56.37 (2021).

⁴⁹ Controlling the Assault of Non-Solicited Pornography and Marketing (“CAN-SPAM”) Act of 2003, 15 U.S.C § 7701-7713.

⁵⁰ See generally, Roger Allan Ford, *Preemption of State Spam Laws by the Federal CAN-SPAM Act*, Comment, 72 U. Chi. L. Rev. 355 (2005).