STATEMENT OF:

NEEMA SINGH GULIANI
SENIOR LEGISLATIVE COUNSEL, WASHINGTON LEGISLATIVE OFFICE
AMERICAN CIVIL LIBERTIES UNION

For a Hearing on:

"Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework"

Before

United States Senate
Committee on Commerce, Science, and Transportation

May 1, 2019

For further information, please contact Neema Singh Guliani, Senior Legislative Counsel, at nguliani@aclu.org.

Chairman Thune, Ranking Member Cantwell, and Members of the Committee,

Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU)[1] and for holding this hearing on, "Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework."

Privacy impacts virtually every facet of modern life. Personal information can be exploited to unfairly discriminate, exacerbate economic inequality, or undermine security. Unfortunately, our existing laws have not kept pace with technology, leaving consumers with little ability to control their own personal information or recourse in cases where their rights are violated. And, as numerous examples illustrate, consumers are paying the price. Studies have documented how several retailers charged consumers different prices by exploiting information related to their digital habits inferred from people's web-browsing history. [2] Some online mortgage lenders have charged Latino and Black borrowers more for loans, potentially by determining loan rates based on machine learning and patterns in big data. [3] And, sensitive data about the location and staffing of U.S. military bases abroad was reportedly revealed inadvertently by a fitness app that posted the location information of users online.[4]

The current privacy landscape is untenable for consumers. The ACLU supports strong baseline federal legislation to protect consumer privacy. I would like to emphasize several issues that are of particular concern to the ACLU and our members. **The ACLU strongly urges Congress to ensure that any federal privacy legislation, at a minimum, (1) sets a floor, not a ceiling, for state level protections; (2) contains robust enforcement mechanisms, including a private right of action; (3) prevents data from being used to improperly discriminate on the basis of race, sexual orientation, or other protected characteristics; and (4) creates clear and strong ground rules for the use, collection, and retention of consumers' personal data, which does not rest solely on the flawed notice and consent model.**

I. Federal legislation should not prevent states from putting in place stronger consumer protections or taking enforcement action

Any federal privacy standards should be a floor — not a ceiling — for consumer protections. The ACLU strongly opposes legislation that would, as some industry groups have urged,

---

[1] For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country. With more than three million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico and Washington, D.C., to preserve American democracy and an open government.

[2] Aniko Hannak, et al., *Measuring Price Discrimination and Steering on E-commerce Web Sites*, PROCEEDINGS OF THE 2014 CONFERENCE ON INTERNET MEASUREMENT CONFERENCE, 2014, at 305-318, http://doi.acm.org/10.1145/2663716.2663744.

[3] ROBERT BARTLETT, ADAIR MORSE, RICHARD STANTON & NANCY WALLACE, CONSUMER-LENDING DISCRIMINATION IN THE ERA OF FINTECH 4 (2018), http://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf?_ga=2.121311752.1273672289.1556324969-25127549.1556324969.

[4] Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret US Army Bases*, THE GUARDIAN (Jan. 28, 2018), https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

preempt stronger state laws.[5] Such an approach would put existing consumer protections, many of which are state-led, on the chopping block and prevent additional consumer privacy protections from ever seeing the light of day. We also oppose efforts to limit the ability of state Attorneys General or other regulators from suing, fining, or taking other actions against companies that violate their laws.

There are multiple examples of states leading the charge to pass laws to protect consumer privacy from new and emerging threats. For example, California was the first state in the nation to require that companies notify consumers[6] of a data breach (all states have since followed suit),[7] the first to mandate that companies disclose through a conspicuous privacy policy the types of information they collect and share with third parties,[8] and among the first to recognize data privacy rights for children.[9] The state's recently passed California Consumer Privacy Act of 2018, which goes into effect next year, is also the first in the nation to apply consumer protections to a broad range of businesses, including provisions that limit the sale of personal information, give consumers the right to delete and obtain information about how their data is being used, and provide a narrow private right of action for some instances of data breach.

Similarly, Illinois has set important limits on the commercial collection and storage of biometric information, such as fingerprints and face prints.[10] Idaho, West Virginia, Oklahoma, and other states have passed laws to protect student privacy.[11] Nevada and Minnesota require internet service providers to keep certain information about their customers private and to prevent disclosure of personally identifying information.[12] Arkansas and Vermont have enacted legislation to prevent employers from requesting passwords to personal Internet accounts to get or keep a job. At least 34 states also require private or governmental entities to conduct data minimization and/or disposal of personal information,[13] and 22 have laws implementing data security measures.[14]

Historically, states have also served a critical enforcement role in the consumer space, as illustrated by the recent Equifax breach. As a result of that breach, the data of over 140 million consumers

---

[5] *See* U.S. Chamber of Commerce, *U.S. Chamber Privacy Principles*, (Sept. 6, 2018), available at https://www.uschamber.com/issue-brief/us-chamber-privacy-principles; Internet Association, *Privacy Principles*, available at https://internetassociation.org/positions/privacy/.

[6] *See* California Civil Code s.1798.25-1798.29.

[7] *See* National Conference of State Legislatures, *Security Breach Notification Laws*, (Sept. 29, 2018), available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[8] *See* California Code, Business and Professions Code - BPC § 22575.

[9] See California Code, Business and Professions Code - BPC§ 22582.

[10] *See* Biometric Information Privacy Act, 740 ILCS 14/, http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[11] *See* Center for Democracy and Technology, *State Student Privacy Law Compendium* (Oct. 2016), available at https://cdt.org/files/2016/10/CDT-Stu-Priv-Compendium-FNL.pdf.

[12] *See* National Conference of State Legislatures, *Privacy Legislation Related to Internet Service Providers-2018* (Oct. 15, 2018), available at http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx.

[13] *See* National Conference of State Legislatures, *Data Disposal Law*s, available at http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

[14] *See* National Conference of State Legislatures, *Data Security Laws* (Oct. 15, 2018), available at http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

were exposed due to what some members of Congress referred to as "malfeasance" on the part of the company.[15] Despite this, the company posted record profits the following year, and consumers have still have not been fully compensated for the cost of credit freezes the breach made necessary. While the FTC has an ongoing investigation, it has yet to take action. In the meantime, the Massachusetts attorney general is currently suing Equifax seeking damages in an attempt to obtain compensation for individuals impacted by the breach. In addition, several state regulators have entered into a consent decree with the company that puts in place new requirements.[16]

States have been and will continue to be well-positioned to respond to emerging privacy challenges in our digital ecosystem. New technology will likely require additional protections and experimenting with different solutions, and states can serve as laboratories for testing these solutions. Thus, we should avoid preemption that could lock in place federal standards that may soon be obsolete or prevent states from fully utilizing their enforcement capabilities.

Preemption would not only be bad for consumers, it would represent a shift in the approach taken by many of our existing laws. For example, the Telecommunications Act explicitly allows states to enforce additional oversight and regulatory systems for telephone equipment, provided they do not interfere federal law; it also permits states to regulate additional terms and conditions for mobile phone services. Title I of the Affordable Care Act permits states to put in place additional consumer protections related to coverage of health insurance plans, and HIPPA similarly allows states to enact more stringent protections for health information.

In addition, all 50 states in some way regulate unfair or deceptive trade practices, an area also governed by section 5 of the FTC Act.[17] While the strength of these state laws vary, they are harmonious with the FTC's mandate and are integral to manageable privacy regulation enforcement. Such coordination has historically allowed states to fill gaps that federal regulators simply do not have the resources or expertise to address. (An Appendix of additional state privacy laws is attached to this testimony.)

We recognize that any federal legislation must account for conflicts in cases where it would be impossible for an entity to comply with both federal and state laws. However, this can be accomplished through a clear, narrow conflict-preemption provision, which explicitly preserves stronger state laws that do not undermine federal standards, maintains state enforcement capabilities, and retains state consumer remedies.

II. Federal legislation must contain strong enforcement mechanisms, including a private right of action

Federal privacy legislation will mean little without robust enforcement. Thus, any legislation should grant greater resources and enforcement capabilities to the FTC and permit state and

---

[15] Kevin Liles, *Hack Will Lead to Little, if Any, Punishment for Equifax*, N.Y. TIMES (Sept. 20, 2017), available at https://www.nytimes.com/2017/09/20/business/equifax-hack-penalties.html.

[16] Kate Fazzini, *Equifax Gets New To-do List, But No Fines or Penalties*, CNBC (Jun. 27, 2018), https://www.cnbc.com/2018/06/27/equifax-breach-consent-order-issued.html.

[17] Carolyn Carter, *Consumer Protection in the States: A 0-State Report on Unfair and Deceptive Acts and Practices Statutes*, National Consumer Law Center, (Feb. 2019), available at https://www.nclc.org/images/pdf/udap/report_50_states.pdf.

local authorities to fully enforce federal law. To fill the inevitable government enforcement gaps, however, the ACLU urges Congress to ensure that federal legislation also grants consumers the right to sue companies for privacy violations.

The FTC has a long history of protecting consumer privacy in the United States. But, alone and with current resources and authorities, it cannot effectively police privacy alone. In the last 20 years, the number of employees at the FTC has grown only slightly.[18] And the number of employees in the Division of Privacy and Identity Protection (DPIP) and the Division of Enforcement, which are responsible for the agency's privacy and data security work, stands at approximately 50 and 44 people, respectively.[19] To put this in perspective, this is smaller than the Washington, D.C. offices of many large technology companies alone. Both the FTC as a whole and DPIP require additional resources and employees to address the outsize risks to privacy facing consumers.

And for the agency's investigations and enforcement actions to have meaningful deterrent effect, the FTC should be given authority to levy significant civil penalties in consumer protection actions for the first violation, rather than only in cases where a company is already under a consent decree.[20] It was recently announced that Facebook has set aside 3 to 5 billion dollars to pay a potential fine to the FTC for its mishandling of personal information, including conduct related to Cambridge Analytica.[21] Following this announcement, Facebook's stock value surged nonetheless, suggesting that the FTC's current enforcement powers are woefully lacking when measured against the earning potential of the largest online businesses.

To augment the limited federal enforcement resources, state and local enforcement entities should also be given the power to investigate and enforce federal privacy law. This aligns with the approach taken by other laws, including the Fair Debt Collection Practices Act, which is enforceable by state Attorneys General as well as through a private right of action.[22]

Even with these reforms, however, the scale and scope of potential harm associated with poor privacy practices are too extensive to be left to regulators.[23] Government enforcement will inevitably have gaps. Thus, providing consumers a private right of action is also critical from an

---

[18] FTC Fiscal Year 2019 Budget, p. 4, https://www.ftc.gov/system/files/documents/reports/fy-2019-congressional-budget-justification/ftc_congressional_budget_justification_fy_2019.pdf

[19] *Id.* at 18.

[20] *See* Testimony of FTC Chairman Joseph Simons Before the House Committee on Energy and Commerce, 6 ("Section 5 does not provide for civil penalties, reducing the Commission's deterrent capability"), available at https://www.ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_07182018.pdf.

[21] Elizabeth Dwoskin and Tony Romm, *Facebook Sets Aside Billions of Dollars for Potential FTC Fine*, WASHINGTON POST (April 24, 2019), https://www.washingtonpost.com/technology/2019/04/24/facebook-sets-aside-billions-dollars-potential-ftc-fine/?utm_term=.b09f3d5a6bbd

[22] Letter from Attorneys General of Twenty-One States to House and Senate Leadership, April 19, 2018, https://ag.ny.gov/sites/default/files/hr_5082_multistate_letter.pdf.

[23] *See* Letter from California Attorney General Xavier Becerra to California Assemblymember Ed Chau and Senator Robert Hertzberg, August 22, 2018 ("The lack of a private right of action, which would provide a critical adjunct to governmental enforcement, will substantially increase the [Attorney General's Office's] need for new enforcement resources. I urge you to provide consumers with a private right of action under the [California Consumer Privacy Act]."), available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2801&context=historical.

enforcement standpoint – a concept reflected in several state approaches. For example, the Illinois Biometric Information Privacy Act permits aggrieved individuals whose rights are violated to file suit to seek damages.[24] The Illinois Supreme Court has interpreted the law as providing a private right of action to individuals who allege a statutory violation of the law.[25] Similarly, recently, the California Attorney General supported legislation that would provide a private right of action to consumers in the privacy context, noting "We need to have some help. And that's why giving [consumers] their own private right to defend themselves in court if the Department of Justice decides it's not acting—for whatever number of good reasons—that's important to be able to truly say … you have rights."[26]

In order to be effective, a private right of action should have two key protections for consumers. First, it should specify statutory damages for all violations of privacy rights, not just instances where a consumer has offered conclusive proof of tangible damages. When conduct is potentially harmful, statutory damages offer a compelling solution. In copyright infringement, for example, statutory damages can range from $750 to $30,000 per work infringed.[27] Similarly, the Fair Debt Collection Practices Act provides for statutory damages of up to $1,000 per violation.[28] These statutory-damage provisions encourage rigorous compliance by establishing that violations carry a significant penalty. Privacy law should do the same.

Second, consumers should be protected against mandatory arbitration clauses buried in terms of service that restrict their rights to have a court hear their claims and undermine the ability of class actions to collectively redress privacy violations.[29] One federal judge called these arbitration clauses "a totally coerced waiver of both the right to a jury and the right of access to the courts" that are "based on nothing but factual and legal fictions."[30] Similarly, in a dissent in this term's *Lamps Plus* case, Justice Ginsburg noted, "mandatory individual arbitration continues to thwart 'effective access to justice' for those encountering diverse violations of their legal rights."[31] Privacy law should neither tolerate such waivers nor indulge the legal and factual fictions that underlie them.

III. Federal legislation should guard against discrimination in the digital ecosystem

Existing federal laws prohibit discrimination in the credit, employment, and housing context. Any federal privacy legislation should ensure such prohibitions apply fully in the digital ecosystem and are robustly enforced. In addition, we urge Congress to strengthen existing laws to guard against unfair discrimination, including in cases where it may stem from algorithmic bias.

---

[24] Biometric Information Privacy Act, *supra* note 10, 740 ILCS 14/, Section 20.
[25] *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 (2019).
[26] Cheryl Miller, *Becerra Backs Bill Giving Consumers Power to Sue for Data Privacy Violations*, LAW.COM: THE RECORDER (Feb. 25, 2019), https://www.law.com/therecorder/2019/02/25/becerra-backs-bill-giving-consumers-power-to-sue-for-data-privacy-violations/.
[27] 17 U.S.C. § 504(c)(2).
[28] 15 USC 1692k.
[29] Jessica Silver-Greenberg & Robert Gebeloff, *Arbitration Everywhere, Stacking the Deck of Justice*, N.Y. TIMES, October 31, 2015, https://www.nytimes.com/2015/11/01/business/dealbook/arbitration-everywhere-stacking-the-deck-of-justice.html.
[30] *Meyer v. Kalanick*, 291 F. Supp. 3d 526, 529 (S.D.N.Y. 2018).
[31] *Lamps Plus v. Varela*, 587 U.S. __(2019)(Ginsburg, R., dissenting).

Many online providers have been slow to fully comply with federal antidiscrimination laws. The rise of big data and personalized marketing has enabled new forms of discrimination that run afoul of existing federal laws, including Title VII of the Civil Rights Act, the Age Discrimination in Employment Act, the Fair Housing Act, and the Equal Credit Opportunity Act. For example, Facebook recently settled a lawsuit brought by ACLU and other civil rights organizations amid allegations that it discriminated on the basis of gender and age in targeting ads for housing and employment.[32] The lawsuit followed repeated failures by the company to fully respond to studies demonstrating that the platform improperly permitted ad targeting based on prohibited characteristics, like race, or proxies for such characteristics. The company is also now the subject of charges brought by the Department of Housing and Urban Development (HUD), which includes similar allegations.[33]

Outside the credit, employment, and housing contexts, discriminatory targeting and marketing may also raise civil rights concerns. For example, commercial advertisers should not be permitted to offer different prices, services, or opportunities to individuals, or to exclude them from receiving ads offering certain commercial benefits, based on characteristics like their gender or race. And regulators and consumers should be given information and tools to address algorithms or machine learning models that disparately impact individuals on the basis of protected characteristics.

Federal law must be strengthened to address these challenges. First, federal privacy law should make clear that existing antidiscrimination laws apply fully in the online ecosystem, including in online marketing and advertising. Federal agencies that enforce these laws, like HUD, the EEOC, and the Consumer Financial Protection Bureau, should be fully resourced and given the technical capabilities to vigorously enforce the law in the context of these new forms of digital discrimination. In addition, companies should be required to audit their data processing practices for bias and privacy risks, and such audits should be made available to regulators and disclosed publicly, with redactions if necessary to protect proprietary information. Finally, researchers should be permitted to independently audit platforms for bias, and Congress should not permit enforcement of terms of service that interfere with such testing.

IV. Federal privacy legislation must place limits on how personal information can be collected, used, and retained

Legislation must include real protections that consider the modern reality of how people's personal information is collected, retained, and used. The law should limit the purposes for which consumer data can be used, require purging of data after permissible uses have completed, prevent coercive conditioning of services on waiving privacy rights, and limit so-called "pay for privacy" schemes. Otherwise, we risk ending up in the same place we began — with consumers simply checking boxes to consent with no real understanding of or control over how their data will be used.

[32] ACLU, *Facebook Agrees to Sweeping Reforms to Curb Discriminatory Ad Targeting Practices* (Mar. 19, 2019), https://www.aclu.org/news/facebook-agrees-sweeping-reforms-curb-discriminatory-ad-targeting-practices.
[33] Complaint of Discrimination Against Facebook, FHEO No. 01-18-032308, https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

This current broken privacy regime has largely been built around the concept of "notice and consent": as long as a company includes a description of what it is doing somewhere in a lengthy fine-print click-through "agreement," and the consumer "agrees" (which they must do to utilize a service), then the company is broadly regarded as having met its privacy obligations. And legally, a company is most vulnerable if it violates specific promises in those click-through agreements or other advertisements.[34] An ecosystem of widespread privacy invasions has grown out of the impossible legal fiction that consumers read and understand such agreements.[35] The truth is that consumers do not have real transparency into how their data is being used and abused, and they do not have meaningful control over how their data is used once it leaves their hands.

Worse, technologists and academics have found that advertising companies "innovate" in online tracking technologies to resist consumers' attempts to defeat that tracking. This is done by, for example, using multiple identifiers that replicate each other, virus-like, when users attempt to delete them. Technical circumvention of privacy protections is sufficiently commonplace that data brokers are even offering what is effectively re-identification as a service, promising the ability to "reach customers, not cookies."[36] Advertisers, the experts conclude, "use new, relatively unknown technologies to track people, specifically because consumers have not heard of these techniques. Furthermore, these technologies obviate choice mechanisms that consumers exercise."[37]

In short, not only have consumers lost control over how and when they are monitored online, companies are actively working to defeat efforts to resist that monitoring. Currently, individuals who want privacy must attempt to win a technological arms race with the multi-billion dollar Internet-advertising industry. American consumers are not content with this state of affairs. Numerous polls show that the current online ecosystem makes people profoundly uncomfortable.[38] Similarly, recent polling released by the ACLU of California showed overwhelming support for measures adding strong privacy protections to the law, including requiring that companies get permission before sharing people's personal information.[39]

---

[34] Dave Perrerra, FTC privacy enforcement focuses on deception, not unfairness, Mlex Market Insight, February 22, 2019, available at https://mlexmarketinsight.com/insights-center/editors-picks/Data-Protection-Privacy-and-Security/north-america/ftc-privacy-enforcement-focuses-on-deception,-not-unfairness.

[35] *See* Alex Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar 1. 2012), available at https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[36] Reach Customers, Not Just Cookies, LiveRamp Blog, September 10, 2015 (available at https://liveramp.com/blog/reach-customers-not-just-cookies/) ("Cookies are like an anonymous ID that cannot identify you as a person.").

[37] Chris Jay Hoofnagle, et al, *Behavioral Advertising: The Offer You Cannot Refuse*, 6 Harvard Law & Policy Review (Aug. 2010), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2137601.

[38] *See, e.g.* Marc Fisher & Craig Timberg, *American Uneasy About Surveillance but Often Use Snooping Tools, Post Poll Finds*, WASH. POST (Dec. 21, 2013), https://www.washingtonpost.com/world/national-security/americans-uneasy-about-surveillance-but-often-use-snooping-tools-post-poll-finds/2013/12/21/ca15e990-67f9-11e3-ae56-22de072140a2_story.html; Edward Baig, *Internet Users Say, Don't Track Me*, U.S.A. TODAY (Dec. 14, 2010), http://usatoday30.usatoday.com/money/advertising/2010-12-14-donottrackpoll14_ST_N.htm; JOSEPH TUROW ET. AL., CONTRARY TO WHAT MARKETERS SAY, AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT (2009), https://www.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

[39] California Voters Overwhelmingly Support Stronger Consumer Privacy Protections, New Data Shows, ACLU of Northern California, available at https://www.aclunc.org/news/california-voters-overwhelmingly-support-stronger-consumer-privacy-protections-new-data-shows.

To address these deficiencies, privacy legislation should include a meaningful "opt-in" baseline rule for the collection and sharing of personal information. To be meaningful, protections must not allow businesses to force consumers, in order to participate fully in society, to "agree" to arcane lengthy, agreements that they cannot understand. Legislation should also support technological opt-in mechanisms such as "do not track" flags in web browsers by requiring that companies honor those flags. In addition to this, federal legislation should approach the collection (and especially use) of personal information that is not necessary for the provision of a service with skepticism.

Moreover, the law should reject so-called "pay-for-privacy" schemes, which allow companies to offer a more expensive or lower quality product to people who exercise privacy rights. These kinds of schemes discourage everyone from exercising their privacy rights, and risk causing disastrous follow-on consequences for people who are already financially struggling.[40] Privacy is a right that everyone should have, not just people with the ability to pay for it.

V. Conclusion

The current federal privacy framework is failing consumers. But, in enacting federal privacy legislation, Congress must ensure that it does not do more harm than good by preempting existing and future state laws that protect consumers. Moreover, it must ensure that its reforms amount to more than just a fig leaf. Consumers do not need another box to check; they need limits on how companies can treat their data, the ability to enforce their privacy rights in court, and protection against digital discrimination. These reforms and others are necessary to prevent exploitation of data from being used to exacerbate inequality, unfairly discriminate, and undermine security.

[40] Mary Madden, The Devastating Consequences of Being Poor in the Digital Age, The New York Times, April 25, 2019 ("When those who influence policy and technology design have a lower perception of privacy risk themselves, it contributes to a lack of investment in the kind of safeguards and protections that vulnerable communities both want and urgently need.") (available at https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html).

Appendix. State Privacy Laws

The chart below provides a list of some existing state privacy laws. This is not an exhaustive list of all state consumer privacy laws, nor does it include all general laws that may be relevant in the consumer privacy context.

State	Summary and/or Relevant Provisions	Source
Alabama	Data security. Requires business entities and government to provide notice to certain persons upon a breach of security that results in the unauthorized acquisition of sensitive personally identifying information. Provides standards of reasonable security measures and investigations into breaches.	Ala. Code 1975 § 8-38-1 to -12 ("Alabama Data Breach Notification Act of 2018")
	Deceptive Trade Practices Act. Broadly prohibits unfair, deceptive, or unconscionable acts. Creates a private right of action and gives Attorney General and district attorneys power to enforce statute.	Ala. Code §§ 8-19-1 to -15

Alaska	Breach notification law that provides for: (1) notice requirement when a breach of security concerning personal information has occurred; (2) ability to place a security freeze on a consumer credit report; (3) various restrictions on the use of personal information and credit information; (4) disposal of records containing personal information; (5) allowing a victim of identity theft to petition the court for a determination of factual innocence; and (6) truncation of credit card information. The SSN section also states that no one can require disclosure of a SSN to access a product or service.	Alaska Stat. Ann. § 45.48.010 ("Alaska Personal Information Act")
	State constitution: "The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section."	Alaska Const. art. I, § 22
	Unfair Trade Practices and Consumer Protection Act. Broadly prohibits unfair, deceptive, or unconscionable acts. Creates a private right of action and gives Attorney General and district attorneys power to enforce statute.	Alaska Stat. §§ 45.50.471 to .561
	When disposing of records that contain personal information, a business and a governmental agency shall take all reasonable measures necessary to protect against unauthorized access to or use of the records.	Alaska Stat. § 45.48.500

Arizona	Provides that public library or library systems shall not allow disclosure of records or other information which identifies a user of library services as requesting or obtaining specific materials or services or as otherwise using the library.	Ariz. Rev. Stat. § 41-151.22
	State constitution: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law."	Ariz. Const. art. II § 8
	Consumer Fraud Act. Broadly prohibits unfair, deceptive, or unconscionable acts. Gives Attorney General power to enforce statute.	Ariz. Rev. Stat. Ann. §§ 44-1521 through 44-1534
	Entity must discard and dispose of records containing personal identifying information. Enforceable by attorney general or a county attorney.	Ariz. Rev. Stat. § 44-7601
Arkansas	Requires government websites or state portals to establish privacy policies and procedures and incorporate machine-readable privacy policies into their web sites	Ark. Code Ann. § 25-1-114
	Data security law that applies to a person or business that acquires, owns, or licenses personal information. Requires implementation and maintenance of reasonable security procedures and practices appropriate to the nature of the information. Amended to include biometric data.	Ark. Code § 4-110-101 to -10 (Personal Information Protection Act) *amended in 2019 Arkansas Law Act 1030 (H.B. 1943)*
	Prevents employers from requesting passwords to personal internet accounts to get or keep a job.	Ark. Code Ann. § 11-2-124

	Prohibits use of Automated License Plate Readers (ALPRs) by individuals, partnerships, companies, associations or state agencies. Provides exceptions for limited use by law enforcement, by parking enforcement entities, or for controlling access to secure areas. Prohibits data from being preserved for more than 150 days.	Ark. Code §§ 12-12-1801 to 12-12-1808 ("Automatic License Plate Reader System Act")
	Deceptive Trade Practices Act. Broadly prohibits deceptive and unconscionable trade practices. Makes it a misdemeanor to knowingly and willfully commit unlawful practice under the law and gives attorney general power of civil enforcement and to create a Consumer Advisory Board.	Ark. Code Ann. §§ 4-88-101 through 4-88-207
California	Gives consumers right to request a business to disclose the categories and specific pieces of personal information that the business has collected about the consumers and the source of that information and business purpose for collecting the information. Consumers may request that a business delete personal information that the business collected from the consumers. Consumers have the right to opt out of a business's sale of their personal information, and a business may not discriminate against consumers who opt out. Applies to California residents. Effective Jan. 1, 2020.	Cal. Civ. Code § 1798.100 to .198 ("The California Consumer Privacy Act of 2018")

State constitution: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." "Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law."	Cal. Const. art. I §§ 1, 23
Require government websites or state portals to establish and publish privacy policies and procedures	Cal. Govt. Code § 11019.9
Permits minors to remove, or to request and obtain removal of, content or information posted on website, online service, online application, or mobile application. Prohibits operator of a website or online service directed to minors from marketing or advertising specified products or services that minors are legally prohibited from buying. Prohibits marketing or advertising products based on personal information specific to a minor or knowingly using, disclosing, compiling, or allowing a third party to do so.	Cal. Bus. & Prof. Code §§ 22580-22582 ("California's Privacy Rights for California Minors in the Digital World Act")

Protects a library patron's use records, such as written records or electronic transaction that identifies a patron's borrowing information or use of library information resources, including, but not limited to, database search records, borrowing records, class records, and any other personally identifiable uses of library resources information requests, or inquiries	Cal. Govt. Code § 6267
Protects information about the books Californians browse, read or purchase from electronic services and online booksellers who may have access to detailed information about readers, such as specific pages browsed. Requires a search warrant, court order, or the user's affirmative consent before such a business can disclose the personal information of its users related to their use of a book, with specified exceptions, including an imminent danger of death or serious injury.	Cal. Civil Code § 1798.90 ("Reader Privacy Act")
Operator of a commercial web site or online service must disclose in its privacy policy how it responds to a web browser 'do not track' signal or similar mechanisms providing consumers with the ability to exercise choice about online tracking of their personal information across sites or services and over time. Operator must disclose whether third parties are or may be conducting such tracking on the operator's site or service.	Cal. Bus. & Prof. Code § 22575

Operator, defined as a person or entity that collects personally identifiable information from California residents through an Internet website or online service for commercial purposes, must post a conspicuous privacy policy on its website or online service (which may include mobile apps) and to comply with that policy. The privacy policy must identify the categories of personally identifiable information that the operator collects about individual consumers who use or visit its website or online service and third parties with whom the operator may share the information.	Calif. Bus. & Prof. Code § 22575-22578 (CalOPPA)
Prohibits a person or entity from providing the operation of a voice recognition feature in California without prominently informing, during the initial setup or installation of a connected television, either the user or the person designated by the user to perform the initial setup or installation of the connected television. Prohibits manufacturers or third-party contractors from collecting any actual recordings of spoken word for the purpose of improving the voice recognition feature. Prohibits a person or entity from compelling a manufacturer or other entity providing the operation of voice recognition to build specific features to allow an investigative or law enforcement officer to monitor communications through that feature.	Cal. Bus. & Prof. Code § 22948.20
Requires private nonprofit or for-profit postsecondary educational institutions to post a social media privacy policy on the institution's website	Cal. Educ. Code § 99122

Requires all nonfinancial businesses to disclose to customers the types of personal information the business shares with or sells to a third party for direct marketing purposes or for compensation. Businesses may post a privacy statement that gives customers the opportunity to choose not to share information at no cost.	Cal. Civ. Code §§ 1798.83 to .84
Breach notification requirements when unencrypted personal information, or encrypted personal information and the security credentials, was or reasonably believed to have been acquired by an unauthorized person. Applies to agencies and businesses.	Cal. Civ. Code §§ 1798.29, 1798.82
Data security. Applies to a business that owns, licenses, or maintains personal information & third-party contractors. Must implement and maintain reasonable security procedures and practices appropriate to the nature of the information.	Cal Civ. Code § 1798.81.5
Provides that the California Highway Patrol (CHP) may retain data from a license plate reader for no more than 60 days, unless the data is being used as evidence in felony cases. Prohibits selling or making available ALPR data to non-law enforcement officers or agencies. Requires CHP to report to the legislature how ALPR data is being used.	Cal. Vehicle Code § 2413

	Establishes regulations on the privacy and usage of automatic license plate recognition (ALPR) data and expands the meaning of "personal information" to include information or data collected through the use or operation of an ALPR system. Imposes privacy protection requirements on entities that use ALPR information, as defined; prohibit public agencies from selling or sharing ALPR information, except to another public agency, as specified; and require operators of ALPR systems to use that information only for authorized purposes. Establishes private right of action.	Cal. Civ. Code §§ 1798.90.50 to .55
	Prohibits unfair competition, which includes any unlawful, unfair, or fraudulent business act or practice.	Cal. Bus. & Prof. Code §§ 17200 through 17594
	Prohibits unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or that results in the sale or lease of goods or services to a consumer. Provides a private right of action.	Cal. Civ. Code §§ 1750 through 1785 ("Consumer Legal Remedies Act")
Colorado	Requires the state or any agency, institution, or political subdivision that operates or maintains an electronic mail communications system to adopt a written policy on any monitoring of electronic mail communications and the circumstances under which it will be conducted. The policy shall include a statement that correspondence of the employee in the form of electronic mail may be a public record under the public records law and may be subject to public inspection under this part.	Colo. Rev. Stat. § 24-72-204.5

Requires government websites or state portals to establish and publish privacy policies and procedures	Colo. Rev. Stat. § 24-72-501 to -502
Data security. Applies to any private entity that maintains, owns, or licenses personal identifying information in the course of the person's business or occupation. Must develop written policies for proper disposal of personal information once such information is no longer needed. Implement and maintain reasonable security practices and procedures to protect personal identifying information from unauthorized access.	Colo. Rev. Stat. § 6-1-713, § 6-1-716
Requires that video or still images obtained by "passive surveillance" by governmental entities, such as images from monitoring cameras, must be destroyed within three years after the recording of the images. Specifies that the custodian of a passive surveillance record may only access the record beyond the first anniversary after the date of creation of the record if there has been a notice of claim filed, or an accident or other specific incident that may cause the passive surveillance record to become evidence in any civil, labor, administrative, or felony criminal proceeding. Creates exceptions allowing retention of passive surveillance records of any correctional facility, local jail, or private contract prison and passive surveillance records made or maintained as required under federal law	Colo. Rev. Stat. § 24-72-113
Prohibits deceptive trade practices. Attorney generals and district attorneys enforce statute.	Colo. Rev. Stat. §§ 6-1-101 through 6-1-115

Connecticut	Requires any person who collects Social Security numbers in the course of business to create a privacy protection policy. The policy must be "publicly displayed" by posting on a web page and the policy must (1) protect the confidentiality, (2) prohibit unlawful disclosure, and (3) limit access to Social Security numbers.	Conn. Gen. Stat. § 42-471
	Employers who engage in any type of electronic monitoring must give prior written notice to all employees, informing them of the types of monitoring which may occur. If employer has reasonable grounds to believe that employees are engaged in illegal conduct and electronic monitoring may produce evidence of this misconduct, the employer may conduct monitoring without giving prior written notice. Labor Commissioner may levy civil penalties against a violator who fails to give notice of monitoring.	Conn. Gen. Stat. § 31-48d
	Health data security law that applies to any health insurer, health care center or other entity licensed to do health insurance business in the state. Requires them to implement and maintain a comprehensive information security program to safeguard the personal information of insureds and enrollees that is compiled or maintained by such company.	Conn. Gen. Stat. § 38a-999b

	Data security law that applies to contractors, defined as an individual, business or other entity that is receiving confidential information from a state contracting agency or agent of the state pursuant to a written agreement to provide goods or services to the state. Must implement and maintain a comprehensive data-security program, including encryption of all sensitive personal data transmitted wirelessly or via a public Internet connection, or contained on portable electronic devices.	Conn. Gen. Stat. § 4e-70
	Prohibits unfair or deceptive acts or practices in the conduct of any trade or commerce. Commissioner enforces. Creates private right of action.	Conn. Gen. Stat. §§ 42-110a through 42-110q
Delaware	Prohibits operators of websites, online or cloud computing services, online applications, or mobile applications directed at children from marketing or advertising on its Internet service specified products or services. When the marketing is provided by an advertising service, the operator of Prohibits disclosing a child's personally identifiable information if it is known that the child's personally identifiable information will be used to market those products or services to the child.	Del. Code Ann. tit. 6, § 1204C

Requires an operator of a commercial internet website, online or cloud computing service, online application, or mobile application that collects personally identifiable information through the Internet about individual users residing in Delaware to make its privacy policy conspicuously available. An operator shall be in violation of this subsection only if the operator fails to make its privacy policy conspicuously available within 30 days after being notified of noncompliance.	Del. Code Ann. tit. 6, § 1205C
Prohibits a commercial entity which provides a book service from disclosing users' personal information to law enforcement entities, governmental entities, or other persons, except under specified circumstances. Allows immediate disclosure of a user's book service information to law enforcement entities when there is an imminent danger of death or serious physical. Requires a book service provider to prepare and post online an annual report on its disclosures of personal information, unless exempted from doing so. The Consumer Protection Unit of the Department of Justice has the authority to investigate and prosecute violations of the acts.	Del. Code Ann. tit. 6, § 1206C

	Prohibits employers from monitoring or intercepting electronic mail or Internet access or usage of an employee unless the employer has first given a one-time notice to the employee. Provides exceptions for processes that are performed solely for the purpose of computer system maintenance and/or protection, and for court ordered actions. Provides for a civil penalty of $100 for each violation.	Del. Code Ann. tit. 19, § 705
	Require government websites or state portals to establish and publish privacy policies and procedures	Del. Code tit. 29 § 9018C
	Prohibits deceptive acts in connection with the sale, lease, or advertisement of any merchandise. Gives investigative power to attorney general and creates a private right of action.	Del. Code Ann. tit. 6, §§ 2511 through 2527, 2580 through 2584 ("Consumer Fraud Act")
	Any person who conducts business in the state and owns, licenses, or maintains personal information must implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.	Del. Code § 12B-100
District of Columbia	Prohibits unfair or deceptive trade practices involving any and all parts of economic output of society.	D.C. Code §§ 28-3901 through 28-3913

Florida	State constitution: The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated	Fla. Const. art. I § 12
	Data security law that applies to commercial entities and third-party agents (entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity). Requires reasonable measures to protect and secure data in electronic form containing personal information.	Fla. Stat. Ann. § 501.171
	Creates a public records exemption for certain images and data obtained through the use of an automated license plate recognition system and personal identifying information of an individual in data generated from such images. Provides that images and data containing personal information obtained from automated license plate recognition systems are confidential. Allows for disclosure to criminal justice agencies and to individuals to whom the license plate is registered in certain circumstances.	Fla. Stat. Ann. § 316.0777
	Prohibits unfair or deceptive acts or practices in the conduct of any trade of commerce, defined as advertising, soliciting, providing, offering, or distributing commodity or thing of value. Creates private right of action.	Fla. Stat. §§ 501.201 through 501.213 (" Deceptive and Unfair Trade Practices Act")

Georgia	License plate data may be collected and accessed only for a law enforcement purpose. The data must be destroyed no later than 30 months after it was originally collected unless the data are the subject matter of a toll violation or for law enforcement. Allows sharing of captured license plate data among law enforcement agencies. Law enforcement agencies deploying an automated license plate recognition system must maintain policies for the use and operation of the system, including but not limited to policies for the training of law enforcement officers in the use of captured license plate data	Ga. Code Ann. § 35-1-22
	Broadly prohibits unfair and deceptive practices in the conduct of consumer transactions, defined as the sale, purchase, lease, or rental of goods, services, or property. Creates private right of action.	Ga. Code Ann. §§ 10-1-390 through 10-1-407 ("Fair Business Practices Act")
Hawaii	Any business or government agency that collects personal information shall provide notice upon discovery of a security breach. Establishes a council that will identify best privacy practices.	Haw. Stat. § 487N-1 to N-7

	State constitution: "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right." "The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and invasions of privacy shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized or the communications sought to be intercepted."	Haw. Const. art. I §§ 6, 7
	Prohibits unfair competition against any person and unfair or deceptive acts or practices, enforceable by any consumer. Applies to the conduct of any trade or commerce.	Haw. Rev. Stat. § 480-2
Idaho	Prohibits use of drones to capture images of people or gather information about individuals in the absence of a warrant or written consent.	Idaho Code § 21-213
	Imposes regulations on individual student data, restricts secondary uses of such data, and provides for data destruction	Idaho Code § 33-133
	Broadly prohibits unfair or deceptive acts and practices in the conduct of any trade or commerce. An unconscionable act is a violation whether it occurs before, during, or after the transaction.	Idaho Code Ann. §§ 48-601 through 48-619 ("Consumer Protection Act")

Illinois	Prohibits state agency websites to use cookies or other invasive tracking programs to monitor viewing habits	Ill. Rev. Stat. ch. 5 § 177/10
	Limits on collection and storage of biometric data. Prohibits private entity from capturing or obtaining biometric information without notice and consent. Creates private right of action	740 Ill. Comp. Stat. 14/1 (Biometric Information Privacy Act)
	State constitution: "The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized.	Ill. Const. art. I, § 6
	Makes it unlawful for an employer or prospective employer to request or require an employee or applicant to authenticate or access a personal online account in the presence of the employer, to request or require that an employee or applicant invite the employer to join a certain group, or join an online account established by the employer; prohibits retaliation against an employee or applicant.	820 Ill. Comp. Stat. 55/10 (Right to Privacy in the Workplace Act)
	Broadly prohibits unfair methods of competition and unfair or deceptive acts or practice in the conduct of any trade or commerce.	815 Ill. Comp. Stat. 505/1 through 505/12

Indiana	Data Security. Applies to database owner, defined as a person that owns or licenses computerized data that includes personal information. Must implement and maintain reasonable procedures, including taking any appropriate corrective action for breaches.	Ind. Code § 24-4.9-3-3.5
	Prohibits unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Creates private right of action for a person relying upon an uncured or incurable deceptive act.	Ind. Code §§ 24-5-0.5-1 to -12 ("Deceptive Consumer Sales Act")
Iowa	Require government Web sites or state portals to establish and publish privacy policies and procedures.	Iowa Code § 22.11
	Prohibits unfair and deceptive acts in connection with the lease, sale, or advertisement of any merchandise. Enforceable only by the Attorney General, unless there was intent to cause reliance upon the act in which case consumers can enforce the prohibition.	Iowa Code §§ 714.16 through 714.16A
Kansas	Defines breach of privacy such as intercepting phone calls and private messages, use of recording devices inside or outside of a place without prior consent, use of video recording without prior consent. Does not apply to utility companies where recording communications is necessary in order to provide the service/utility requested.	K.S. Stat § 21-6101

	Data security. Applies to a holder of personal information (a person who, in the ordinary course of business, collects, maintains or possesses, or causes to be collected, maintained or possessed, the personal information of any other person.) Must implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure.	K.S. § 50-6,139b
	Prohibits deceptive and unconscionable acts in connection with a consumer transaction, regardless of whether the act occurs before, during, or after the transaction. Creates private right of action.	Kan. Stat. Ann. §§ 50-623 through 50-640 and 50-675a through 50-679a
Kentucky	Notification to affected persons of computer security breach involving their unencrypted personally identifiable information.	Ky. Rev. Stat. Ann. 365.732
	Personal information security and breach investigation procedures and practices for certain public agencies and nonaffiliated third parties.	Ky. Rev. Stat. Ann. 61.932
	Prohibited uses of personally identifiable student information by cloud computing service provider	Ky. Rev. Stat. Ann. 365.734
	Department procedures and regulations, including appropriate procedures to protect against unauthorized access to or use of personal information	Ky. Rev. Stat. Ann. 171.450

	Prohibits unfair, deceptive, and unconscionable acts relating to trade or commerce. Private cause of action only to person who purchases or leases goods or services.	Ky. Rev. Stat. Ann. §§ 367.110 through 367.990 (“Consumer Protection Act”)
Louisiana	Data security law applies to any person that conducts business in the state or that owns or licenses computerized data that includes personal information. Must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Personal information includes name, SSN, driver's license or state ID number, account numbers, passport numbers, or biometric data, but excludes information lawfully made public from federal, state, or local government records.	La. Rev. Stat. 51:3071 to :3077 ("Database Security Breach Notification Law")
	State constitution: “Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy. No warrant shall issue without probable cause supported by oath or affirmation, and particularly describing the place to be searched, the persons or things to be seized, and the lawful purpose or reason for the search. Any person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court.”	La. Const. art. I § 5

	Prohibits unfair or deceptive acts and practices in the conduct of any trade or commerce, including advertising. Creates private right of action.	La. Rev. Stat. Ann. §§ 51:1401 to :1420
Maine	Require government websites or state portals to establish and publish privacy policies and procedures	1 M.R.S.A. § 542
	Prohibits the use of automatic license plate recognition systems except for certain public safety purposes. Provides that data collected is confidential and may be used only for law enforcement purposes. Data collected may not be stored more than 21 days.	29-A M.R.S.A. § 2117-A
	Prohibits unfair or deceptive practice in the conduct of any trade or commerce, including advertising. Creates private right of action for any person who purchases or leases goods, services, or property as a result of an unlawful practice or act under the law.	Me. Rev. Stat. Ann. tit. 5, §§ 205A to 214 ("Unfair Trade Practices Act")
Maryland	Data security provisions apply to businesses and nonaffiliated third party/service provider. Must implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations. Personal information includes name, SSN, driver's license or state ID number, account numbers, TIN, passport number, health information, biometric data, user name or email address in combination with password or security question.	Md. Code Com Law §§ 14-3501 to -3503

	Specifies the procedures and protocols that a law enforcement agency must follow in connection with the operation of an "automatic license plate reader system" and "captured plate data." Requires the State Police to adopt procedures to address who has access to the data, training, and create an audit process. Data gathered by an automatic license plate reader system are not subject to disclosure under the Public Information Act.	Md. Public Safety Code § 3-509
	Prohibits unfair, abusive, or deceptive trade practices, regardless of whether the consumer was in fact misled, deceived, or damage as a result of the practice. Consumer can file a complaint, which the agency will investigate and potentially refer to the FTC	Md. Code Ann., Com. Law §§ 13-101 to -501 ("Consumer Protection Act")
Massachusetts	A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.	Mass. Gen. Laws Ch. 214 § 1B
	Data security law applies to any person that owns or licenses personal information. Authorizes regulations to ensure security and confidentiality of customer information in a manner fully consistent with industry standards. The regulations shall take into account the person's size, scope and type of business, resources available, amount of stored data, and the need for security and confidentiality of both consumer and employee information.	Mass. Gen. Laws Ch. 93H § 2(a)

	Broadly prohibits unfair and deceptive acts and practice sin the conduct of any trade or commerce. Creates private right of action.	Mass. Gen. Laws Ann. ch. 93A, §§ 1 to 11
Michigan	Preserve personal privacy with respect to the purchase, rental, or borrowing of certain materials. Provides penalties and remedies	Mich. Comp. Laws Ann. § 445.1712
	Prohibits unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce. Creates private right of action.	Mich. Comp. Laws §§ 445.901 to .922
Minnesota	Requires Internet Service Providers to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Prohibit disclosure of personally identifying information, and requires ISPs to get permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited.	Minn. Stat. §§ 325M.01 to .09
	Require government websites or state portals to establish and publish privacy policies and procedures.	Minn. Stat. § 13.15
	Makes a misdemeanor to publish or disseminate of advertisements which contain any material assertion, representation, or statement of fact which is untrue, deceptive, or misleading	Minn. Stat. Ann. § 325F.67

	Prohibits act, use, or employment by any person of any fraud, false pretense, misleading statement, or deceptive practice, with the intent that others rely on it in the sale of any merchandise	Minn. Stat. §§ 325F.68
Mississippi	Data security law that applies to any person who conducts business in the state and in the ordinary course of business. Personal information includes name, SSN, driver's license or state ID number, or financial account numbers	Miss. Code Ann. § 75-24-29
	Broadly prohibits unfair and deceptive practices as long as they are in or affecting commerce. Only attorney general can enforce the prohibitions.	Miss. Code Ann. §§ 75-24-1 to -27
Missouri	Defines "E-book" and "digital resource or material" and adds them to the items specified in the definition of "library material" that a library patron may use, borrow, or request. Provides that any third party contracted by a library that receives, transmits, maintains, or stores a library record may not release or disclose all or a portion of a library record to anyone except the person identified in the record or by a court order.	Mo. Rev. Stat. § 182.815, 182.817

	Prohibits unfair or deceptive trade practices or omissions in connection with the sale or advertisement of merchandise in trade or commerce, whether the act was committed before, during, or after the sale, advertisement, or solicitation. Any person who purchases or leases merchandise and suffers loss as a result of the unlawful act may bring a civil action	Mo. Rev. Stat. §§ 407.010 to -.307 ("Merchandising Practices Act")
Montana	Require government website or state portals to establish and publish privacy policies and procedures. Allows sale and disclosure to third parties, provided notice and consent.	Mont. Code Ann. § 2-17-550 to -553
	State constitution: The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.	Mont. Const. art. II § 10
	Prohibits methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.	Mont. Code Ann. §§ 30-14-101 to -142
Nebraska	Data security law applies to any individual or commercial entity that conducts business in Nebraska and maintains personal information about Nebraska residents. Must establish and maintain reasonable security processes and practices appropriate to the nature of the personal information maintained. Ensure that all third parties to whom the entity provides sensitive personal information establish and maintain reasonable security processes and practices appropriate to the nature of the personal information maintained.	Neb. Rev. Stat. §§ 87-801 to -807

	Prohibits employers from accessing an applicant or an employee's personal Internet accounts and taking adverse action against an employee or applicant for failure to provide any information related to the account; prohibits retaliation against an employee who files a complaint under the Act; prohibits an employee from downloading or transferring any private proprietary information or financial data to a personal Internet account without authorization.	Neb. Rev. Stat. §§ 48-3501 to 48-3511 (Workplace Privacy Act)
	Requires any governmental entity that uses an automatic license plate reader (ALPR) system to adopt a policy governing use of the system. Governmental entities also must adopt a privacy policy to ensure that captured plate data is not shared in violation of this act or any other law. The policies must be posted on the Internet or at the entity's main office. Requires annual reports to the Nebraska Commission on Law Enforcement and Criminal Justice on ALPR practices and usage. Provides that captured plate data is not considered a public record.	Neb. Rev. Stat. § 60-3201 to 3209
	Broadly prohibits unfair or deceptive trade practices in the conduct of any trade or commerce. Creates private right of action.	Neb. Rev. Stat. §§ 59-1601 to -1623
Nevada	Requires operators of Internet websites or online services that collect personally identifiable information from residents of the state to notify consumers about how that information is used.	Nev. Rev. Stat. § 603A.340

	Require Internet Service Providers to keep private certain information concerning their customers, unless the customer gives permission to disclose the information.	Nev. Rev. Stat. §205.498
	Data security. Applies to data collector that maintains records which contain personal information and third parties to whom they disclose. Must implement and maintain reasonable security measures	Nev. Rev. Stat. §§ 603A.210, 603A.215
	Prohibits deceptive trade practices, including knowingly making any other false representation in the course of a business or occupation. Also prohibits failing to disclose material fact in connection with sale or lease of goods or services. Private right of action created under Nev. Rev. Stat. § 41.600.	Nev. Rev. Stat. §§ 598.0903 to .0999
New Hampshire	Prohibits government officials from obtaining access to customer financial or credit records, or the information they contain, held by financial institutions or creditors without the customer's authorization, an administrative subpoena, a search warrant, or a judicial subpoena	N.H. Rev. Stat. § 359-C:4
	Makes a crime to willfully intercept any telecommunication or oral communication without the consent of all parties to the communication. It is unlawful to willfully use an electronic, mechanical, or other device to intercept an oral communication or to disclose the contents of an intercepted communication. Law enforcement needs warrant, exception to warrant, or consent to use cell site simulators.	N.H. Rev. Stat. § 570-A:2 to A:2-a

	State constitution: An individual's right to live free from governmental intrusion in private or personal information is natural, essential, and inherent.	N.H. Const. Pt. 1, art. II
	Broadly prohibits unfair method of competition or any unfair or deceptive practice in the conduct of any trade or commerce within the state. Creates private right of action.	N.H. Rev. Stat. §§ 358-A:1 to -A:13
New Jersey	Prohibits act, use, or employment by any person of any unconscionable commercial practice, deception, fraud, misrepresentation, or the knowing concealment, suppression, or omission of any material fact with the intent that others rely upon it in connection with the sale or advertisement of any merchandise or real estate. Creates private right of action.	N.J. Stat. Ann. §§ 56:8-1 to -91
New Mexico	Data security law applies to a person that owns or licenses personal identifying information of a New Mexico resident. Must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure.	N.M. Stat. § 57-12C-4, to 12C-5
	Prohibits unfair, unconscionable, and deceptive practices involving goods, services, credit, or debt collection, made in the course of the person's trade or commerce. Private right of action.	N.M. Stat. §§ 57-12-1 to -22 ("Unfair Practices Act")

New York	Require government Web sites or state portals to establish and publish privacy policies and procedures	N.Y. State Tech. Law § 201 to 207
	Prohibits deceptive acts in the conduct of any business, trade, or commerce or service. Only attorney general can enforce prohibitions on repeated fraudulent acts or unconscionable contract provisions	N.Y. Exec. Law § 63(12); N.Y. Gen. Bus. Law §§ 349 and 350
North Carolina	Requires state or local law enforcement agencies to adopt a written policy governing the use of an ALPR system that addresses databases used to compare data obtained by the system, data retention and sharing of data with other law enforcement agencies, system operator training, supervision of system use, and data security and access. Requires audits and reports of system use and effectiveness. Limits retention of ALPR data to no more than 90 days, except in specified circumstances. Provides that data obtained by the system is confidential and not a public record.	N.C. Gen. Stat. §§ 20-183.30 to .32
	Prohibits unfair methods of competition, and unfair or deceptive acts or practices in or affecting business activities. Creates private right of action	N.C. Gen. Stat. §§ 75-1.1 to -35

North Dakota	Prohibits an act, use, or employment of any deceptive act or practice, fraud, or misrepresentation, with the intent that others rely thereon in connection with the sale or advertisement of any merchandise. Acts or advertisements which causes or is likely to cause substantial injury to a person and not reasonably avoidable by the injured person and not outweighed by countervailing benefits to consumers or to competition, is declared to be an unlawful practice. Creates private right of action.	N.D. Cent. Code §§ 51-15-01 to -11
Ohio	Data security law that applies to Business or nonprofit entity that accesses, maintains, communicates, or handles personal information or restricted information. To qualify for an affirmative defense to a cause of action alleging a failure to implement reasonable information security controls resulting in a data breach, an entity must create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information	Ohio Rev. Code Ann. § 1354.01 to 1354.05
	Prohibits unfair, unconscionable, or deceptive trade practices in connection with a consumer transaction, regardless of whether the act occurs before, during, or after the transaction.	Ohio Rev. Code Ann. §§ 1345.01 to .13

Oklahoma	Requires public reporting of which student data are collected by the state, mandates creation of a statewide student data security plan, and limits the data that can be collected on individual students and how that data can be shared. It establishes new limits on the transfer of student data to federal, state, or local agencies and organizations outside Oklahoma	70 Okl. Stat. Ann. § 3-168 (Student Data Accessibility, Transparency and Accountability Act)
Oregon	Data security law that applies to any person that owns, maintains, or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities. Must develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the personal information, including disposal of the data	Or. Rev. Stat § 646A.622
	Prohibits unconscionable tactics and other unfair or deceptive conduct in trade commerce. Consumer can challenge unfair or deceptive conduct only after the Attorney General has first established a rule declaring that conduct to be unfair or deceptive.	Or. Rev. Stat. §§ 646.605 through 646.656
Pennsylvania	Prohibits unfair or deceptive practices in the conduct of any trade or commerce. Creates private right of action.	73 Pa. Stat. Ann. §§ 201-1 through 201-9.3

Rhode Island	Data security measure applies to a business that owns or licenses computerized unencrypted personal information & a nonaffiliated third-party contractor. Must implement and maintain a risk-based information security program with reasonable security procedures and practices appropriate to the nature of the information.	R.I. Gen. Laws § 11-49.3-2
	Prohibits unfair or deceptive practices in the conduct of any trade or commerce. Creates private right of action.	R.I. Gen. Laws §§ 6-13.1-1 through 6-13.1-27
South Carolina	Requires government Web sites or state portals to establish and publish privacy policies and procedures	S.C. Code Ann. § 30-2-40
	Data security law that applies to a person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of the state. Requires a licensee to develop, implement and maintain a comprehensive information security program based on the licensee's risk assessment. Establishes requirements for the security program, such as implementing an incident response plan and other details	S.C. Code § 38-99-10 to -100.

	State constitution: The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained.	S.C. Const. art. I, § 10
	Prohibits unfair or deceptive practices in the conduct of any trade or commerce. Creates private right of action.	S.C. Code Ann. §§ 39-5-10 through 39-5-160
South Dakota	Prohibits knowing and intentional deceptive acts in connection with the sale or advertisement of merchandise	S.D. Codified Laws §§ 37-24-1 through 37-24-35, *amended by 2019 South Dakota Laws Ch. 177 (SB 20)*
Tennessee	Requires the state or any agency, institution, or political subdivision thereof that operates or maintains an electronic mail communications system to adopt a written policy on any monitoring of electronic mail communications and the circumstances under which it will be conducted. The policy shall include a statement that correspondence may be a public record under the public records law and may be subject to public inspection under this part.	Tenn. Code § 10-7-512

	Provides that any captured automatic license plate data collected by a government entity may not be stored for more than 90 days unless they are part of an ongoing investigation, and in that case provides for data to be destroyed after the conclusion of the investigation.	Tenn. Code § 55-10-302
	Prohibits specific unfair or deceptive acts or practices limited to those enumerated which affect the conduct of any trade or commerce. Only attorney general can bring an enforcement action.	Tenn. Code Ann. §§ 47-18-101 through 47-18-125
Texas	Data security measure that applies to a business or association that collects or maintains sensitive personal information. (Does not apply to financial institutions). Requires implementation of reasonable procedures, including taking any appropriate corrective action.	Tex. Bus. & Com. Code § 521.052
	Prohibits false, unconscionable and deceptive acts in the conduct of any trade or commerce. Consumer protection division can enforce	Tex. Bus. & Com. Code Ann. §§ 17.41 through 17.63
Utah	Require all nonfinancial businesses to disclose to customers, in writing or by electronic mail, the types of personal information the business shares with or sells to a third party for direct marketing purposes or for compensation. Provides a private right of action	Utah Code Ann. §§ 13-37-201 to -203
	Requires government websites or state portals to establish privacy policies and procedures	Utah Code Ann. § 63D-2-101, to -104

	Data security. Applies to any person who conducts business in the state and maintains personal information. Must implement and maintain reasonable procedures. Amended in 2019 to define is subject to a civil penalty	Utah Code Ann. §§ 13-44-101, -201, 301
	Captured license plate data are a protected record if the captured plate data are maintained by a governmental entity. Provides that captured plate data may only be shared for specified purposes, may only be preserved for a certain time, and may only be disclosed pursuant to specific circumstances such as a disclosure order or a warrant. Government entities may not use privately held captured plate data without a warrant or court order, unless the private provider retains captured plate data for 30 days or fewer.	Utah Code Ann. §§ 41-6a-2001 to -2005
	Prohibits deceptive and unconscionable acts or practices by suppliers in connection with a consumer transaction, regardless of whether it occurs before, during, or after the transaction. Private right of action.	Utah Code Ann. §§ 13-11-1 through 13-11-23
Vermont	Prevents employers from requesting passwords to personal Internet accounts to get or keep a job.	21 V.S.A. § 495

	Data security. Applies to Data brokers--businesses that knowingly collect and license the personal information of consumers with whom such businesses do not have a direct relationship. Must implement and maintain a written information security program containing administrative, technical, and physical safeguards to protect personally identifiable information.	9 V.S.A § 2446-2447
	Broadly prohibits unfair or deceptive acts or practices in commerce	9 V.S.A. §§ 2451 to 2480g
Virginia	Require government websites or state portals to establish and publish privacy policies and procedures	Va. Code § 2.2-3800
	Prohibits specified fraudulent and deceptive acts and practices committed by a supplier in connection with a consumer transaction.	Va. Code Ann. §§ 59.1-196 through 59.1-207
Washington	State constitution: No person shall be disturbed in his private affairs, or his home invaded, without authority of law	Wash. Const. art. I, § 7
	Prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. Private right of action.	Wash. Rev. Code §§ 19.86.010 through 19.86.920
West Virginia	Student data law governing use sharing of student privacy rights, and notification of transfer of confidential information.	W. Va. Code, § 18-2-5h

Prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. Private right of action.	W. Va. Code §§ 46A-6-101 through 46A-6-110