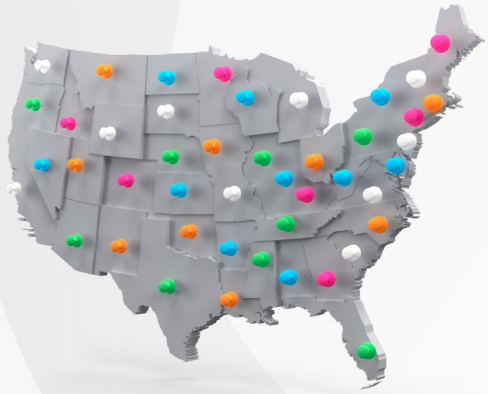
Private Internet Access:

US Privacy Rankings 2023 by State



There are currently no all-encompassing online privacy laws in the US, and each state has its own rules. While some have comprehensive protections in place, others allow sites to collect data, share it, and use it to track what individuals are doing online. This is the second annual privacy report from Private Internet Access, VPN provider and online privacy advocate, which outlines the current imbalance of digital privacy protection across the US.

The report explores which states currently have the best and worst protection and what the US is doing at the federal and state levels to protect online privacy.

Private Internet ACCESS®

Our Ranking Criteria

Our research team examined various criteria to determine which states have the best and worst consumer protections in place at the moment, and are making the best progress toward improving consumer privacy.

To create our rankings, we asked the following questions and tallied the results for each state:

General Strength of Privacy Laws

- Does the consumer have a right to access, delete, or modify personal data?
- Can consumers opt out of data collection and use?
- Are companies required to disclose data collection, source, and use information?
- Are ISPs required to protect online privacy under current legislation?

General Strength of Data Security Laws

- What methods are used to create and enforce privacy policies?
- How do companies in each state safeguard consumer data?

Private Internet ACCESS®

Presence of Data Broker Laws

- Do laws exist that prevent the sale of certain forms of information?
- Do laws exist to monitor/regulate what type of information is collected?
- What, if any, rights do consumers have in regard to data brokers?

Laws in Place to Protect Children's Privacy

- Are laws in place to protect children aged 0–9 while using the internet?
- Do parents/minors have the ability to remove data on request?

Strength of Companies' Data Collection Policies

- Do employees have the right to delete personal data on request?
- Do employees have the right to opt out of third-party sharing?
- Are companies required to disclose what employee data they collect/store?

Laws that Infringe on Digital Privacy

- Has the state implemented any laws that infringe on digital privacy?
- Have state legislators been vocal in their support of further legislation that would harm citizens' rights to online privacy?

Private Internet ACCESS®

PIA's Ranking of the Best & Worst States for Digital Privacy

1st	California
2nd	Connecticut
3rd	Colorado, Virginia
4th	Illinois, Michigan, New York, Oregon
5th	Washington, New Jersey, New Mexico, Maryland, Massachusetts, Hawaii, Florida
6th	Utah*, Texas**, Arizona, Delaware
7th	Pennsylvania, New Hampshire
8th	Missouri, Maine, Indiana, Iowa, Tennessee, Vermont, Wisconsin
9th	Alabama, Alaska, Georgia, Idaho, Kansas, Kentucky, Minnesota, Montana, Nebraska, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Rhode Island, South Carolina, South Dakota, West Virginia, Wyoming
10th	Arkansas, Louisiana, Mississippi

*Utah's ranking is expected to improve once the Consumer Privacy Act (UCPA) takes effect from December 31 2023.
**The Texas Data Privacy and Security Act will take effect in July 2024. This is expected to improve Texas's position in the rankings.

US States with Notable Improvements to Digital Privacy

California

California was the first state to implement a comprehensive data privacy law, the California Consumer Privacy Act, which came into effect in 2020. The CCPA introduced obligations for businesses and consumer rights like access, deletion, and opting out of personal information sales. It was later amended by the CPRA, which added requirements for data sharing, sensitive data, and contractors, while expanding consumer rights with correction and enhanced access. California also has laws mandating sending breach notification to affected individuals and the Attorney General (AG) for breaches impacting more than 500 residents. Other notable privacy laws in California include the California Online Privacy Protection Act, Shine the Light Law, California Invasion of Privacy Act, and the upcoming California Age-Appropriate Design Code Act (effective from July 1, 2024). The California Privacy Protection Agency (CPPA) has continued to focus on improving legal provisions for online privacy, and has published revised CCPA regulations effective from March 29, 2023.

Connecticut

The Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA), signed in May 2022, became effective on July 1, 2023. The CTDPA introduces new consumer rights, including access, rectification, deletion, portability, and the right to opt out of targeted advertising, the sale of personal data, and profiling. It also outlines responsibilities for controllers and processors, with enforcement powers granted to the AG. Additionally, Connecticut has the Data Breach Law, regulating data breach notification requirements. The Personal Information Safeguarding Law protects both paper and electronic information, mandating reasonable security measures for personal information holders.

Colorado

Colorado became the third state to enact its own privacy law with the Colorado Privacy Act (CPA), effective from July 1, 2023. The CPA grants various privacy rights, including the right to opt out of personal data processing and the right to access, correct, delete, or obtain a portable copy of personal data. It also places obligations on data controllers, such as specifying purposes, minimizing data, and handling sensitive data appropriately. Additionally, the CPA requires controllers to conduct assessments for processing activities with higher risks to consumers. These rules are enforced by the AG and district attorneys.

Virginia

Virginia's Consumer Data Protection Act (CDPA) became effective at the start of 2023. It grants consumers various rights, including access, correction, deletion, portability, and the ability to opt out of certain types of data processing. It also imposes obligations on controllers and processors, such as conducting data protection impact assessments and handling de-identified data. Virginia also has the Personal Information Privacy Act, which restricts the sale of personal information by merchants and regulates the use of social security numbers. Virginia also has a personal information breach notification law requiring that affected consumers, the Attorney General, and nationwide consumer reporting agencies are notified in certain breach scenarios. Specific protections are in place for health, employment, and financial information. The Virginia Telephone Privacy Protection Act prohibits solicitation calls to individuals who have previously expressed their desire not to receive such calls. However, Virginia lost points due to following other states that implemented an online age verification law in 2023, mandating that those wishing to access adult content online would have to share their ID in order to have their age digitally verified.

Illinois

Illinois does not have a comprehensive privacy law that covers all aspects of data privacy. However, it does have stronger privacy protections than many other states. The Biometric Information Privacy Act of 2008 (BIPA) is its most significant privacy statute. BIPA prohibits the collection of biometric identifiers or information without meeting specific conditions. It also allows for private individuals to take legal action, resulting in numerous cases and class actions against private entities. The Personal Information Protection Act of 2004 requires that the Attorney General and affected Illinois residents are notified about personal data breaches. Other notable privacy laws in Illinois include the Right to Privacy in the Workplace Act, the Electronic Mail Act, and the Illinois Banking Act.

Michigan

Currently, Michigan does not have a comprehensive privacy act that covers all aspects of data privacy. However, the state does have its own regulations for data breach incidents known as the Data Breach Requirements, which are outlined in the Identity Theft Protection Act (Act 452 of 2004) within the Michigan Compiled Laws. These requirements state that if Michigan residents' data is accessed and acquired by an unauthorized individual, or if someone gains access to the encryption key of encrypted data, the affected individuals must be notified. It's important to note that the Data Breach Requirements can be enforced by the AG or a private attorney, even though there is no specific obligation to inform the AG about a data breach. Apart from the Data Breach Requirements, Michigan has additional privacy laws that apply to specific sectors.

Oregon

In Oregon, there is currently no comprehensive legislation specifically addressing data privacy. However, privacy protections are established through a combination of common law torts, such as invasion of privacy, and laws that focus on specific sectors. In 2019, Oregon updated its data breach notification law, the Oregon Consumer Information Protection Act (OCIPA), which was originally called the Oregon Consumer Identity Theft Protection Act. The OCIPA led to significant changes, including an expanded definition of security breaches and new obligations for vendors. Vendors are now required to notify the relevant organization within ten days of discovering a breach. In addition to this general data breach law, Oregon has sector-specific regulations. These regulations cover the use, disclosure, and processing of student data, as well as disclosures of private financial information.

New York

New York does not yet have a comprehensive privacy law in place, but it is hoped that the New York Privacy Act (NYPA) will provide individuals with extensive control over their data if enacted. The NYPA includes rights such as access, correction, deletion, and the ability to opt out of data processing for targeted advertising. New York has implemented the Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which imposes data breach notification requirements and mandates reasonable data security measures for businesses handling personal information. New York has other sector-specific privacy laws, such as the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation, which focuses on data protection in the financial sector, and the Biometric Privacy Act, which regulates the collection and use of biometric information.

Utah

Utah's Consumer Privacy Act (UCPA), enacted on March 24, 2022, will become effective as of December 31, 2023, making it the fourth state with comprehensive privacy legislation. The UCPA grants consumer rights regarding access, deletion, portability, and opting out of targeted advertising and data sales. It imposes obligations on controllers and processors, mandates privacy notices, and gives the AG exclusive enforcement authority. Utah also has the Electronic Information or Data Privacy Act, protecting third-party electronic data with breach notification requirements and potential penalties enforced by the AG. However, Utah lost points for recently introducing mandatory ID verification for people trying to access adult content online as a huge amount of personal, sensitive data will now be collected.

Texas

Texas passed the Texas Data Privacy and Security Act in May 2023, marking significant progress towards improving data privacy. However, the law will not take effect until July 2024. The Texas Identity Theft Enforcement and Protection Act encompasses general privacy provisions aimed at safeguarding personal identifying information and sensitive personal information. Furthermore, Texas has specific privacy regulations applicable to various sectors, including health data, financial data, biometric data, and unsolicited commercial communications. Texas has some sector-specific privacy laws related to data breach notifications, requiring businesses to notify individuals in the event of a breach of their personal information.

States Most in Need of Privacy Law Improvements

Arkansas

Arkansas dropped in the ranking to become the lowest-ranked state for digital privacy. This is due to a lack of progress in introducing new laws to protect consumer data and privacy, coupled with the introduction of the Social Media Safety Act which mandates digital age verification for access to adult content online. Arkansas has severely limited privacy laws in place compared to other states, but does have some laws related to data breach notifications. Businesses are required to notify individuals if there's breach of their personal information.

Mississippi

Mississippi dropped in the ranking to become the joint lowest-ranked state for digital privacy. Like Arkansas, there was a lack of progress to introduce new pro-privacy laws, as well as the introduction of its own age verification law which made digital age verification compulsory when trying to access adult content. Mississippi does not have comprehensive online privacy legislation to protect individuals, and privacy laws are limited compared to other states.

Louisiana

Instead of making progress towards improving online privacy for its citizens, Louisiana became the first state to implement mandatory digital age verification for access to adult content online. These laws created unnecessary data privacy risks by collecting large amounts of sensitive personal data.

Online Privacy Laws in Specific States

While most states are becoming more diligent about protecting people's privacy, there isn't a single set of regulations in place for the US as a whole. A one-size-fits-all solution may not work for online privacy. Separate cohesive legislation is needed for businesses, consumers, children, and federal and state entities, so everyone knows where they stand.

Online Privacy Laws Across the US

Protection	Applies To	Adopted In
Access, delete, or change personal data already collected by businesses	Consumer	UT, CA, VA, NV
Opt out of the collection/use of personal data	Consumer	CO, UT, VA, CA
Request that businesses disclose what personal information they collect, the source, and how it's used	Consumer	CA, UT, NV
Opt out of having personal data sold to third parties	Consumer	CO, NV, UT, VA

Protection	Applies To	Adopted In
Require ISPs to keep certain information about subscribers private, unless the subscriber requests otherwise	Consumer	NV, MN
Require ISPs to get permission from subscribers before disclosing a subscriber's browsing habits or sites visited	Consumer	NV, MN
Prohibit ISPs from using, disclosing, selling, or permitting access to subscriber personal information except on request of the subscriber	Consumer	ME
Prohibit site/online service operators from advertising certain products to minors based on information specific to the minor, or knowingly using, disclosing, or compiling a minor's information or allowing third parties to do so	Children	DE, CA
Permit minors to remove, or request removal, of personal content or information from sites, services, and mobile apps	Children	CA
Require privacy policies to be publicly and noticeably displayed on websites	Consumer	CO, CA, CT, UT, VA
Require operators to disclose whether third parties are/may conduct tracking on the operator's site/service	Consumer	DE, CA

Protection	Applies To	Adopted In
Require operators to disclose how a site/service responds to “Do Not Track” signals/similar transmissions	Consumer	CA
Prohibit knowingly making false or misleading statements in privacy policies	Consumer	NE, PA
Require government sites and state portals to establish privacy policies or procedures or incorporate machine-readable privacy policies	Consumer	AZ, AR, CA, CO, DE, IA, IL, ME, MD, MN, MT, NY, SC, TX, UT, VA
Require employers to notify employees prior to monitoring electronic communications or internet access	Employees	CT, DE, NY
Require states and public entities to adopt policies in regard to monitoring public employee emails	Employees	CO, TN
(A) Prohibit employers from requiring employees to download a mobile app to their personal devices that allows their location to be tracked or personal information to be revealed. (B) Prohibit any form of retribution for refusing or opposing any practice forbidden as stated in part (A).	Employees	HI

Protection	Applies To	Adopted In
Require private sector employers to provide written notice immediately on hiring any employee that makes them aware if they are subject to electronic, internet, or phone monitoring	Employees	NY
Require the state and any subdivision thereof that operates or maintains electronic mail communications systems to adopt a written policy on monitoring and when/why they conduct monitoring	Employees	CO, TN
Require employers to make a statement available that any form of electronic mail may be public record under the Public Record Law, and that makes it subject to public inspection	Employees	CO, TN
Protect the personal information of students in grades K–12	Children	NJ

Other Notable Online Privacy Laws

Summation	Adopted In
Have biometric data protection legislation in place	NY, IL, CA, TX, WA
Apply data disposal laws to government and business entities	AL, AK, HI, IL, MA, AZ, AR, KS, MD, MA, MI, NJ, OR, SC, WA
Apply data disposal laws to government entities only	VA, MN, TX
Apply data disposal laws to business entities only	CA, CO, CT, DE, FL, GA, IN, KY, LA, MT, NE, TN, VT, NV, NM, NY, NC, RI, UT, WI
Require consent from both parties when recording calls of any kind	CA, CT, FL, IL, MD, MA, MT, NH PA, WA
Have laws/legislation surrounding the use of artificial intelligence (AI)	AL, CO, IL, MS, NYC

States with Cybersecurity Task Forces

As a response to the increase in cybercrime, some states have developed special task forces to deal with cyber threats. Currently, 30 states have a task force or similar enforcement group in place. Only 8 states took the initiative to create legislation and develop their task forces on their own; the rest were issued by executive order.

Arizona	**Florida**	**Kansas**	**Missouri**	**Oregon**
Arkansas	**Georgia**	**Louisiana**	**Montana**	**Rhode Island**
California	**Idaho**	**Maine**	**New Hampshire**	**Texas**
Colorado	**Illinois**	**Maryland**	**New York**	**Utah**
Connecticut	**Indiana**	**Minnesota**	**North Carolina**	**Vermont**
Delaware	**Iowa**	**Mississippi**	**North Dakota**	**Virginia**

Federal Digital Privacy and Security Laws

Currently, federal (nationwide) laws on digital privacy and security are well meaning but ambiguous. Each tends to isolate one sector, issue, age group, or industry instead of providing a stable solution for all consumers and companies. I'll show you what I mean – here are a few of the major federal online privacy laws

HIPAA's Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) created a national standard for the security of electronic protected health information (e-PHI), electronic exchange, and privacy of e-PHI.

It applies to any care provider sending health information electronically in connection with transactions. Ultimately, HIPAA is a branch of the Privacy Rule, and covers all of the personally identifiable health information (PHI) related to patients.

Con: HIPAA covers only e-PHI.

Private Internet ACCESS®

Federal Trade Commission (FTC) Fair Information Practices

The FTC has enacted several fair information practices to protect your online privacy. Most relate to sites being transparent about what information they request, how it's used, and why they require the information. Site operators must provide a notice of the site's privacy practices, including if:

- Consumers can access, correct, and delete personal information
- Consumers have a say in how the site uses the information it collects
- Parents have control over the collection and use of information gathered from children
- The site safeguards any collected information, and how Sites must also have enforcement mechanisms to prove they're following fair information practices.

Con: While sites must let you know if you have a say in how they use the information collected, FTC practices don't prevent sites from sharing or selling your data to third parties. The site only needs to tell you if it does, if you have any control over it, and if it has security in place for collected information.

Private Internet ACCESS®

Electronic Communication Protections Act (ECPA)

Adopted in 1986, the ECPA originally protected telephone communications. The amended ECPA now protects electronic communications during creation, transit, and storage. It defines electronic communications as email, telephone calls, and electronically stored data.

The ECPA also contains an amendment called the Stored Communications Act (SCA) which protects all subscriber records kept by service providers, including names, billing information/records, and IP addresses.

Con: While ECPA covers email and electronically stored data are covered, it's unclear whether VoIP communications are protected.

FD&C Act, Section 524B

The FD&C Act was amended in 2023 to include Section 524B Ensuring Cybersecurity of Devices. Manufacturers (sponsors) developing medical devices must submit plans for addressing, identifying, and monitoring potential cybersecurity threats with their development plans.

It was amended after increasing concern from the federal government over the massive amounts of PII and ePHI transmitted by cyber medical devices (CMDs). The law requires manufacturers to make updates and patches available to cyber devices, as well as all related software and connected systems, to better prevent cyberattacks.

This includes addressing (a) unacceptable vulnerabilities in a timely manner or justified regular cycle, and (b) critical vulnerabilities that pose unnecessary risks as soon as possible.

Con: It doesn't address legacy CMDs as diligently as new technologies.

Children's Online Privacy Protection Act (COPPA)

Under COPPA, sites are required to verify parental or legal guardian consent if they intend to collect or use a minor's personal information. Other notable online privacy protections in COPPA include:

- Information on when and how verifiable consent must be acquired from a parent/legal guardian
- The responsibilities, if any, that the site's operator holds in regard to the online safety and privacy of the child
- Limits on how much data it's acceptable to collect about children under 13
- Requirements for site operators to post the privacy policy on any page data is collected

Con: COPPA doesn't provide a definitive set of rules for how verifiable parental/legal guardian consent must be collected, though the FTC does provide some guidelines and suggestions.

Federal vs State Laws

As a general rule, federal laws take precedence over state laws in the US. The Supremacy Clause states that when there's conflict, federal law will override state law. Unfortunately, this isn't an absolute rule, so loopholes exist for both branches.

States have the right to refute any federal law they can prove goes against the United States Constitution. The same precedent doesn't apply to federal laws that a state believes go against its Constitution. Individual states also have the right to include or modify requirements.

On the other hand, the federal government can sue states on behalf of the national government. An example of these loopholes in action is California's fight to keep its Internet Consumer Protection and Net Neutrality Act in place.

In September of 2018, the Justice Department sued the State of California to prevent its new net neutrality bill, despite the fact it had already been signed by Governor Jerry Brown. Then-Attorney General Jeff Sessions felt strongly that states didn't have the right to regulate interstate commerce, and that it should be the job of the federal government to do so.

The Attorney General believed the legislature was enacted illegally after the FCC abolished net neutrality protections nationwide. Ultimately, a lower court ruled that California could keep its net neutrality law in place and a federal appeals court upheld this ruling in January 2022.

Enter the American Data Privacy and Protection Act

A federal bill, the **American Data Privacy and Protection Act (ADPPA)**, could be a promising step forward for comprehensive data privacy protections across the US. The bill was first proposed in June of 2022 but has still not been passed as of this most recent legislative session. The proposed ADPPA and its legislative path are the closest US Congress has ever been to passing comprehensive federal privacy legislation.

The bill "establishes requirements for how companies, including nonprofits and common carriers, handle personal data, which includes information that identifies or is reasonably linkable to an individual." The bipartisan, bicameral bill was the first US consumer privacy bill to pass committee markup, which it did with near unanimity.

However, states with strong existing privacy laws, such as California and Colorado, fear that this law could water down their existing state data privacy requirements, which they have built to a high level. While the online privacy bill has yet to pass, it would limit data collection, processing, and transfer to what is absolutely necessary to provide and maintain products or services requested by consumers.

The ADPPA would also prohibit activities including the collection, processing, and transfer of social security numbers, biometric information, genetic information, and non-consensual sexual imagery. The transfer of geolocation information, passwords, browsing history, and even physical activity from smartphones and wearable devices will also be restricted.

The ADPPA is a bit murky when it comes to cohesive legislation for the policies and procedures around data collection, processing, and transfer, though. It calls for companies to consider reducing privacy risks to minors, and provides allowances dependent upon a company's size, the volume of data handled, and other criteria.

Unfortunately, the words “reasonable,” “necessary,” and “consider” appear frequently, and they all leave room for interpretation. What's reasonable for one is excessive for another, consideration doesn't mean compliance, and necessary is in the eye of the data broker. While it may be imperfect legislation, it will offer far more protection than what was previously available on a federal level.

Other outstanding questions to be resolved include:

1. How would enforcement occur, for example through the FTC or the Attorney General?
2. Will it include a private right of action for people to sue over violations?

FAQ

What does data privacy mean?

Data privacy refers to your ability to control how your personal information is collected, stored, shared, and used. While many US states have laws in place to protect people's online privacy, no national standard exists.

Is data privacy important?

Absolutely. Imagine people were allowed to follow you around tracking your day-to-day activities without you being able to do anything about it. No one would tolerate that in real life, so why accept it in the virtual world?

Unfortunately, restraining orders don't exist for online trackers, malicious software, or shady data brokers, so defending your right to online privacy and security is crucial. PIA provides the strong security you need to keep your online activity and data private.

Private Internet ACCESS®

FAQ

What's the difference between data privacy and security?

Data security focuses on how your data is protected in transit and ensures only authorized parties can access it. Data privacy focuses on the responsible collection, storage, and use of your information, such as your right to delete or modify collected data.

Basically, data security aims to protect your data from external threats while data privacy is focused on protecting your identity.

Are there data privacy laws?

There are data privacy laws at both the federal and state levels in the US, but individual state laws vary greatly from one state to the next. No federal or state law yet provides a singular set of regulations for data privacy, although the American Data Privacy and Protection Act is a promising bill which could provide a critical step forward for comprehensive online privacy protection across the United States.