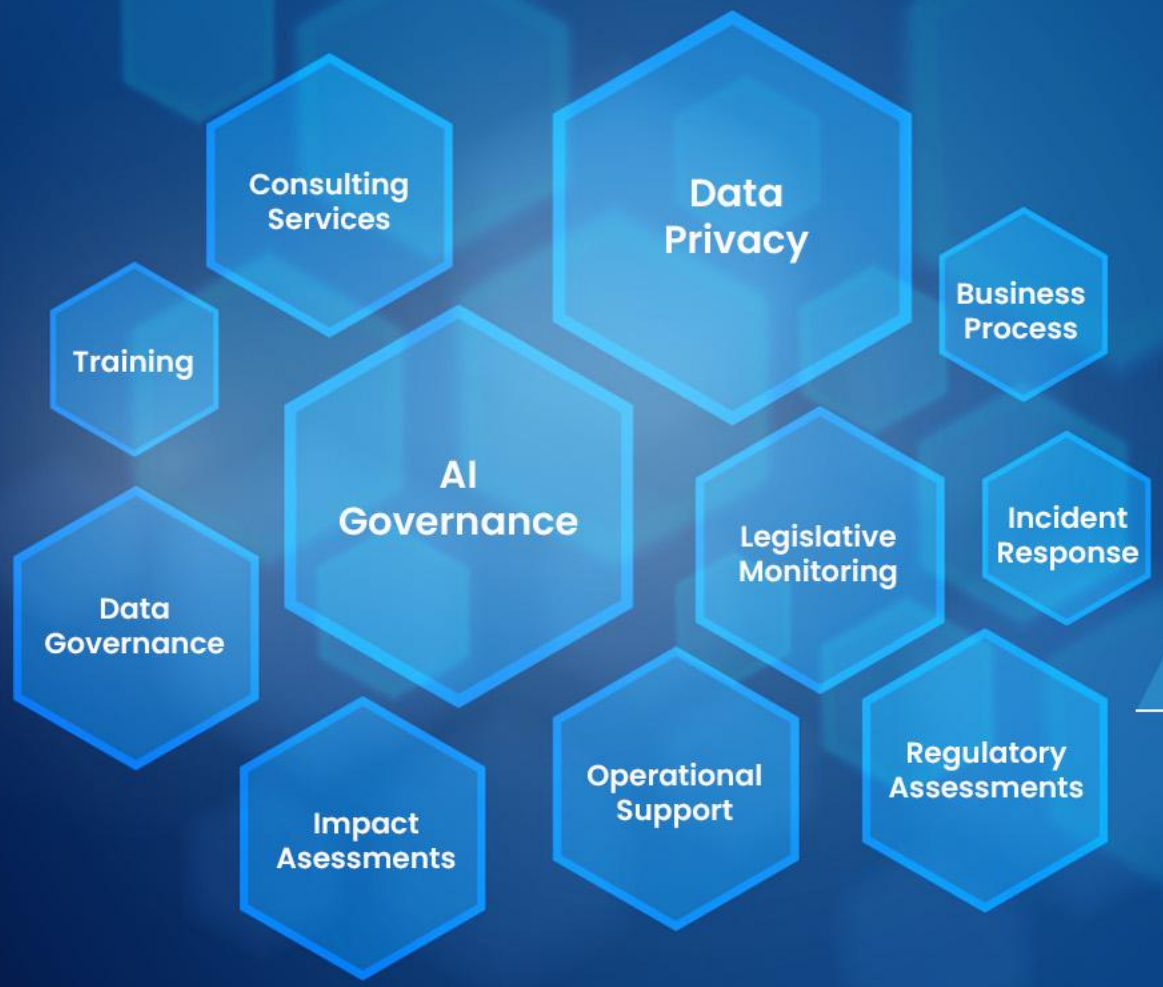
PRIVACY REF



Privacy Protection Online

Ben Siegel
Senior Privacy Consultant
Privacy Ref

PRIVACY REF

Do you have an internal privacy policy?

PRIVACY REF

What is Privacy?

The acceptable use of personal information given the circumstances

Privacy Policy	Privacy Notice
• Internal document • Policy and procedure • Sets expectations for employees • Can be included in security notices	• External document • Sets expectations for your customers and partners • Should reflect your policy

PRIVACY REF

Privacy Policy

- Acceptable use
- Data classification
- Data retention and destruction
- Classification
- Vendor / Procurement
- Security
- Incident response

PRIVACY REF

Common Threats

Malicious Actors	Human Error / Mismanagement
• Social engineering • Phishing • Hacks or malware	• Accidental disclosure • Misconfiguration of systems • Physical Loss

Perfect security is not possible.
We want reasonable security.

PRIVACY REF

Do your employees receive training on security and privacy threats?

PRIVACY REF

Social Engineering / Phishing

Social Engineering	Phishing
• Taking advantage of human behavior to gain access to information • Will try to leverage kindness or compassion • Relies on “acceptable noncompliance”	• Emails meant to appear as if they are legitimate • Regular phishing focuses on law of averages • Spear-phishing targets specific individuals

PRIVACY REF

Social Engineering / Phishing

Training is the solution

- Following policy and procedure brings consistency of service
- Openness of issues with employees arms them to handle them better

PRIVACY REF

Hacks and Malware

In some cases, malicious actors will take advantage of vulnerabilities in systems.

- Make sure systems are updated regularly
- Be aware of current threats and trends
- Third party vendors are a common vector for attacks
- Contractual remedies can assist with reducing harm, but may not stop attacks

PRIVACY REF

Hacks and Malware

Understand that “perfect security” is not tenable.

We want what is reasonable and appropriate.

- Security needs trained, knowledgeable personnel
- Monitor and document the use of systems
- Incident response policies and practices are key

PRIVACY REF

Accidental Disclosure

Why does it happen	How do we stop it
• Humans make mistakes • Lack of consistent procedure • Increased activity volume • Lack of checks	• Training • Establish procedures • Provide checks in procedure to ensure compliance • Audit process for efficacy

PRIVACY REF

Do you use cloud-based systems?

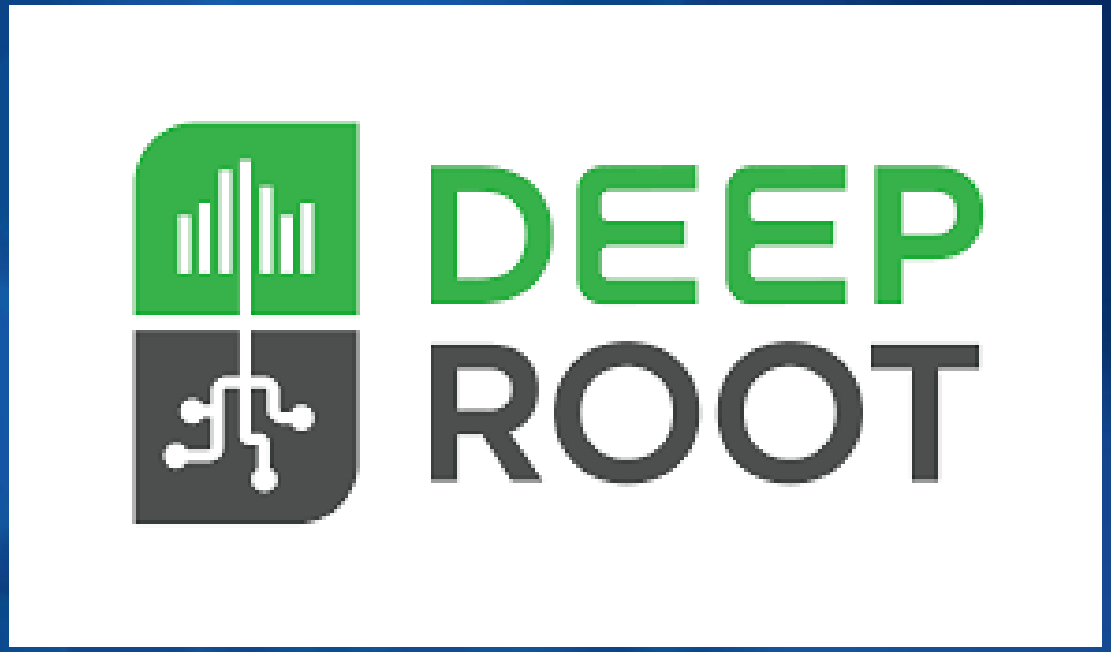
PRIVACY REF

Misconfiguration of Systems

Proper configuration avoids problems down the road. Failure to do so results in serious issues.

- Cloud systems can be exposed to the internet at large
- Information that is sensitive or restricted becomes available to users outside the intended scope

PRIVACY REF



PRIVACY REF

Physical Loss

Theft	Misplaced or Lost
• Physical security is just as important as technical security • Logs and access controls • Remote wiping and monitoring for electronic devices	• Chain of custody • Remote wiping or access • Employee responsibilities

PRIVACY REF

Does your state have a privacy law?

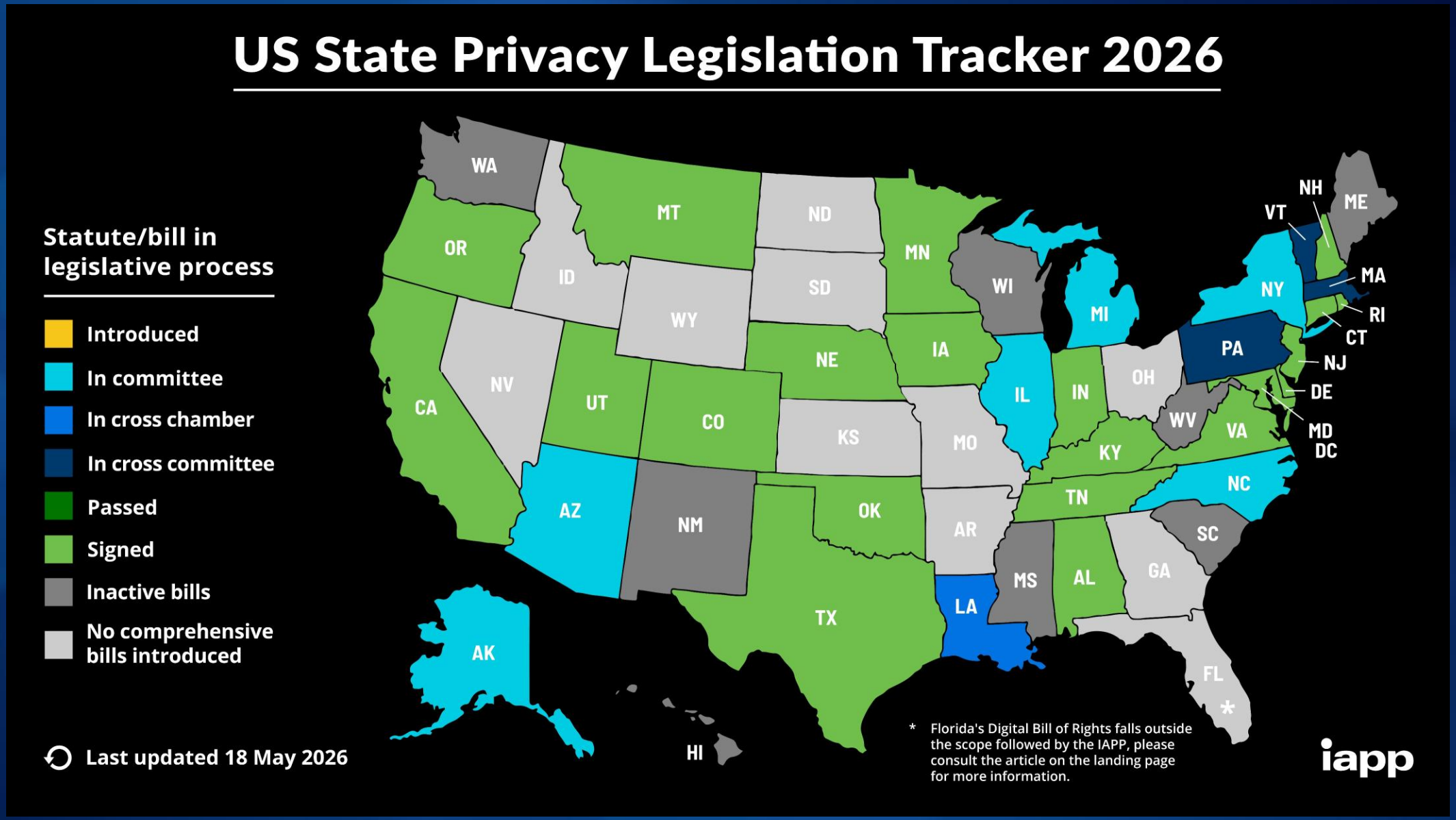
PRIVACY REF

Privacy Laws

In the United States, more than 20 states have a state-wide privacy law. Common trends in those laws include:

- Data subject rights
- Changes to the definition of consent
- Sensitive information provisions
- Service Providers
- Fines for non-compliance

PRIVACY REF


US State Privacy Legislation Tracker 2026
Statute/bill in legislative process
Introduced
In committee
In cross chamber
In cross committee
Passed
Signed
Inactive bills
No comprehensive bills introduced
Last updated 18 May 2026
WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
DC
AK
HI
* Florida's Digital Bill of Rights falls outside the scope followed by the IAPP, please consult the article on the landing page for more information.
iapp

PRIVACY REF

Data Subject Rights

Access	Deletion	Selling of Data
You can ask for access to your data, either confirming processing or providing a copy of the data.	Erase your data	Except where the information is provided to a service provider, you cannot provide the information to another organization for monetary or other valuable consideration.

PRIVACY REF

Data Subject Rights

1. Receive the request
2. Verify the request
3. Gather information (execute the request)
4. Return the information/results
5. Document everything

PRIVACY REF

Receiving Requests

Most state based privacy laws require two methods of receiving requests:

- Phone number (toll-free)
- Email
- Web form

Each form will have the same consideration

What are you asking for?

PRIVACY REF

Verification

Additional Information	Multi-Factor	Rejections
• Information that only your organization and data subject would be likely to know • Past purchases or payments • Security questions	• Use of systems or methods that require the individual to have access to an email or phone number can be reasonable choices	• If you do not believe the person is who they say they are • Information not provided • Request abandoned

PRIVACY REF

Execute

- Find the requested information
  - Check all systems
  - Check with processors/vendors
- Prepare information to be sent
  - Remove erroneous information
  - Remove information of other data subjects

Involved Teams

- IT
- HR
- Legal
- Customer service
- Vendors

PRIVACY REF

Response

During this step, you provide the information to the data subject

In some cases, a negative response is warranted.

- Failed to verify requestor's identity
- Legal obligations
  - Tax law
  - Employment Law
  - Legal defense
- Effects another data subject

PRIVACY REF

Documentation

Everything ***MUST*** be documented.

- When the request was received
- When was the data subject request acknowledged
- When it is verified
- What information is subject to the request
- When was a response sent
- Any communications internally/externally about the request
- Deleted information categories and evidence of such the request for legal compliance

PRIVACY REF

Consent

Consent is one of many legal basis we use to process someone's personal information. It is trending in laws towards an EU style definition.

- Freely Given
- Specific
- Informed
- Unambiguous
- **OPT-IN**

PRIVACY REF

Do you have an opt-out mechanism?

PRIVACY REF

Consent

In addition to trending towards opt-in consent, there is also the ability to revoke consent at any time.

This is similar to data subject rights, but can be done at any time, and must be as easy to revoke as it was to provide.

PRIVACY REF

Sensitive Information

Most laws refer to certain, high-risk forms of information

- Political, philosophical, or religious beliefs
- Medical information
- Biometric or genetic information
- Sexual orientation
- Government Identifiers

Risk is usually defined by the possible harms based on misuse of that type of information

PRIVACY REF

Sensitive Information

- If you do not need to process this information, don’t.
- Be aware of the possibility of inference
- If processing this information is necessary, restrict to only those necessary purposes
- Restrict access to the data

PRIVACY REF

Service Providers

Also called “processors”, organizations that process data on behalf of another organization.

- Must follow directions from the controller (business)
- Must have a written contract
- Cannot make decisions about the processing of information on behalf of another organization

PRIVACY REF

Fines and Penalties

The state privacy laws generally handle violations in two ways.

Fines

- Usually an amount per individual per violation.
- For example, California fines go up to $750/person/violation.

Penalties

- Orders to cease processing
- Orders to implement specific controls
- Requirements to audit program for prolonged period

PRIVACY REF

What are you looking forward to at the annual conference?

PRIVACY REF

Thank you!

www.privacyref.com

info@privacyref.com

888-470-1528

@PrivacyRef