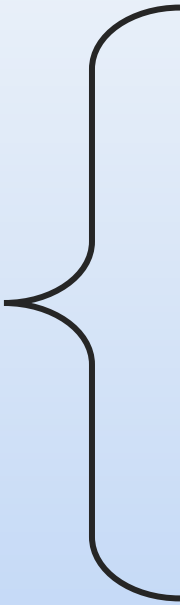


Data Privacy Laws

Ideas for today and tomorrow



Agenda



Data Privacy

Data Governance

Global Law overview

State Law overview

Future strategy

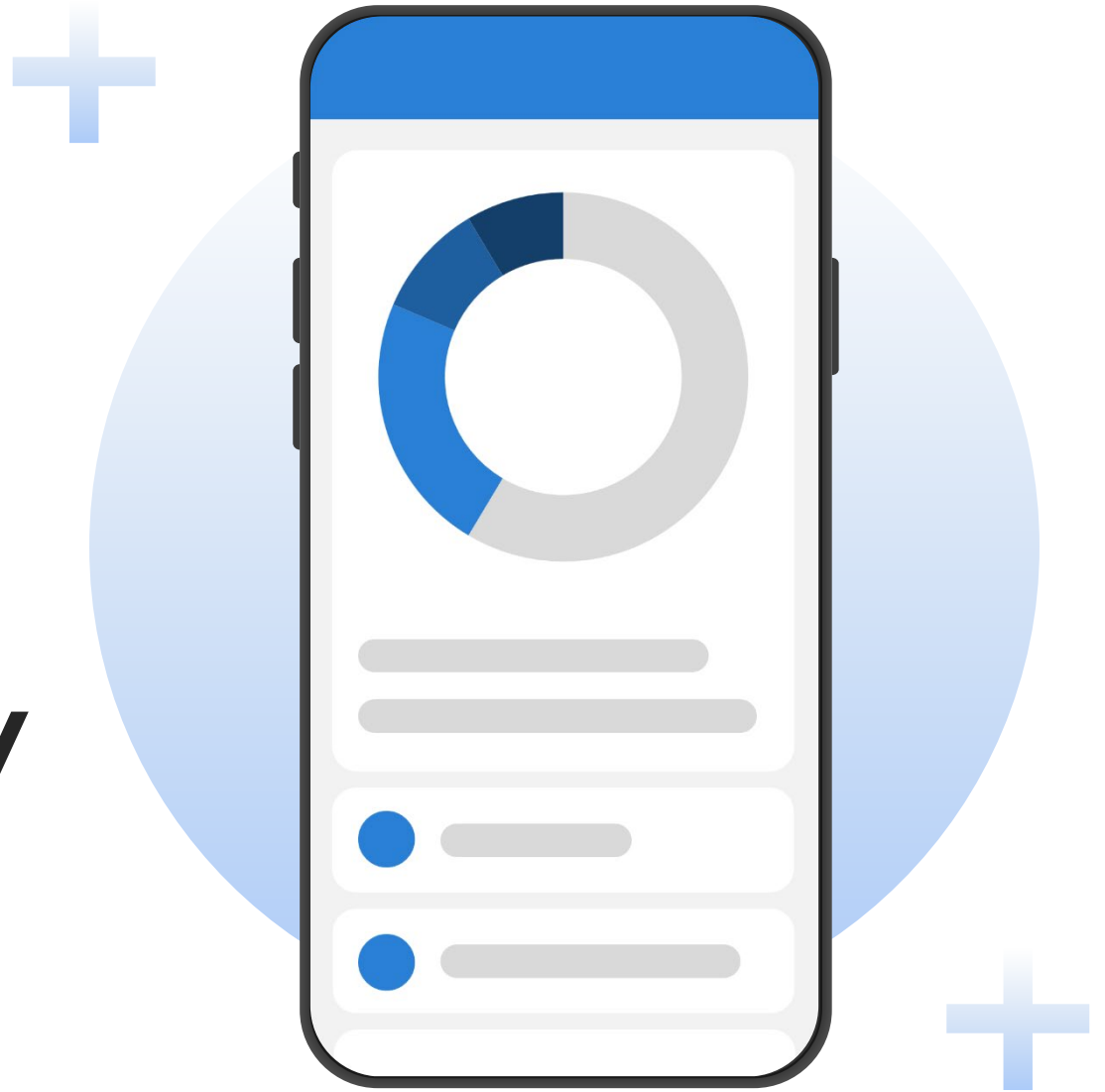
Summary

About Data Privacy

What is data privacy?

Why does it matter?

<https://teachprivacy.com/10-reasons-why-privacy-matters/>

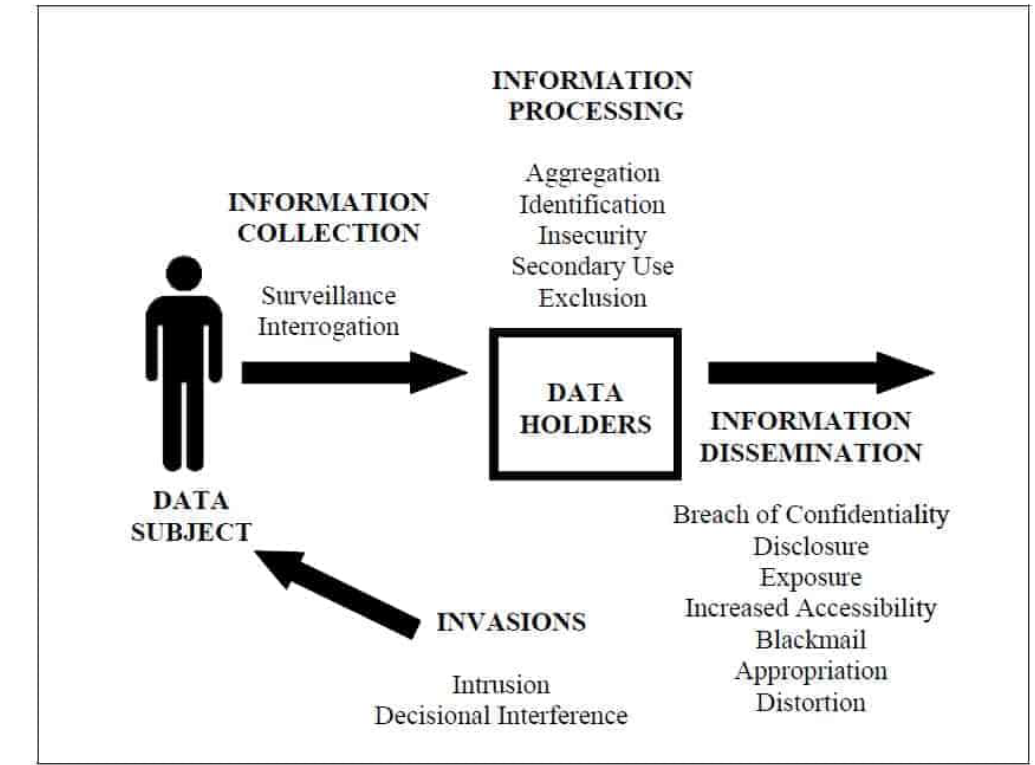


4

What is Privacy?

Privacy is a product of norms, activities, and legal protections. Privacy is about respecting the desires of individuals, where compatible with the aims of the larger community. Privacy is not just about what people expect but about what they desire. Privacy is not merely an individual right – it is an important component of any flourishing community. Privacy is valuable to a community because it provides space for individuals away from the constant impingement of the community. Without this zone of freedom, the community can become oppressive and stifling to people's freedom and welfare.

Privacy is not one thing, but a cluster of many distinct yet related things. Privacy involves the control, use, and disclosure of personal information. It involves issues such as surveillance, online gossip, identity theft, data security, online behavioral advertising, Big Data, access to records, use of cloud computing services, and much more.



<https://teachprivacy.com/what-is-privacy/>

None of the activities are inherently bad. Nor is privacy inherently good. The interests that sometimes conflict with privacy – free speech, security, transparency, and efficient consumer transactions – are all quite valuable. We must balance the value of privacy and conflicting interests to determine which should prevail in any particular situation.

Excluding or ignoring various dimensions of privacy generates bad policy results. If a problem isn't identified, then balancing might never take place or privacy might be undervalued in the balance.

In many cases, protecting privacy does not involve a zero-sum tradeoff. We can protect privacy without sacrificing a conflicting interest if we have procedures and limitations that address the problems. For example, the Fourth Amendment protects privacy not by forbidding the government from searching but by requiring procedures of oversight and limitation.

So whether or not you agree with my theory of privacy, take the time to think deeply about what privacy is. It is essential to any meaningful discussion about how to protect privacy or weigh it against other interests.

- Professor Daniel J. Solove – TeachPrivacy, Prof. George Washington University, Law

Privacy Harms?

Information Collection

the process of data gathering

Information Processing

the way information is stored, manipulated, and used

Information Dissemination

the spreading or transfer of personal data or the threat to do so

Invasion

impingements directly on the individual

Graphic by Anna Jacobson (2019)

1 SURVEILLANCE

the watching, listening to, or recording of an individual's activities

2 INTERROGATION

various forms of questions or probing for information

3 AGGREGATION

the combination of various pieces of data about a person

4 IDENTIFICATION

linking information to particular individuals

5 INSECURITY

carelessness in protecting stored information from leaks and improper access

6 SECONDARY USE

the use of information collected for one purpose for a different purpose without the data subject's consent

7 EXCLUSION

the failure to allow the data subject to know about the data that others have about her and participate in its handling and use

8 BREACH OF CONFIDENTIALITY

breaking a promise to keep a person's information confidential

9 DISCLOSURE

the revelation of truthful information about a person that impacts the way others judge her character

10 EXPOSURE

revealing another's nudity, grief, or bodily functions

11 INCREASED ACCESSIBILITY

amplifying the accessibility of information

12 BLACKMAIL

the threat to disclose personal information

13 APPROPRIATION

the use of the data subject's identity to serve the aims and interests of another

14 DISTORTION

the dissemination of false or misleading information about individuals

15 INTRUSION

invasive acts that disturb one's tranquility or solitude

16 DECISIONAL INTERFERENCE

the government's incursion into the data subject's decisions regarding her private affairs

Data Governance - [Data Life Cycle]

- Chief Privacy Officer (CPO)
[Organization Motivated]
- Data Privacy Officer (DPO)
[Compliance Motivated]

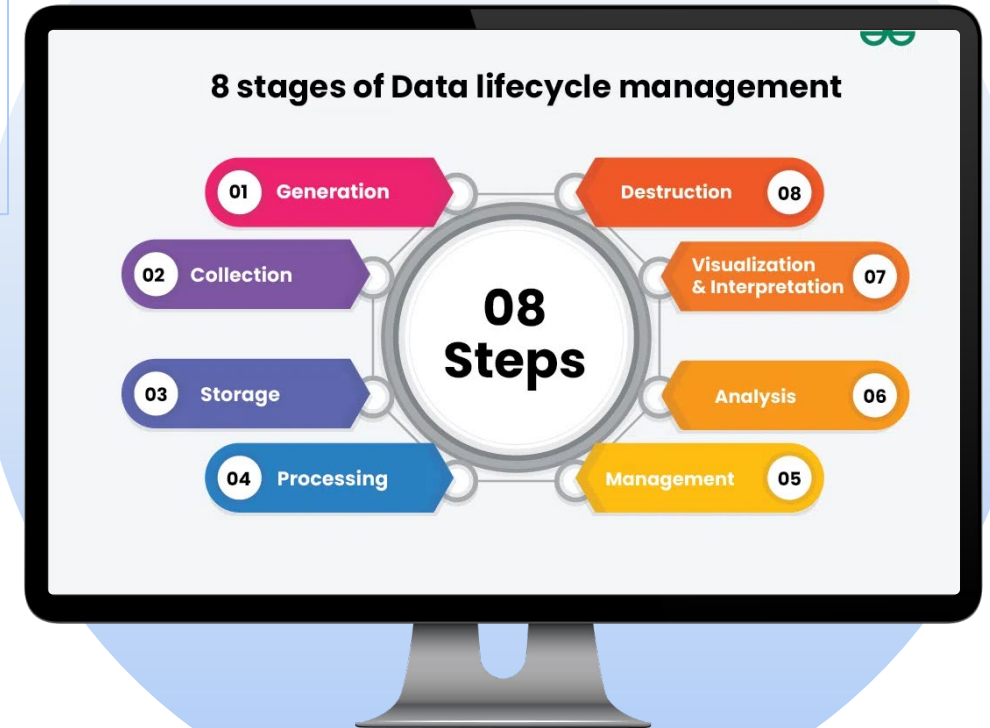
Focus

Scope

Purpose

Responsibility

Priority



Data Governance - [Data Life Cycle]

Focus – data (identifiable data)

Scope – collection to deletion (where, what)

Purpose – why to collect data (minimization)

Responsibility – who (internal, third-party)

Priority – data auditing / documentation



Data Governance - [Data Life Cycle]

- **Chief Privacy Officer (CPO)**
[Organization Motivated]
- Data Privacy Officer (DPO)
[Compliance Motivated]

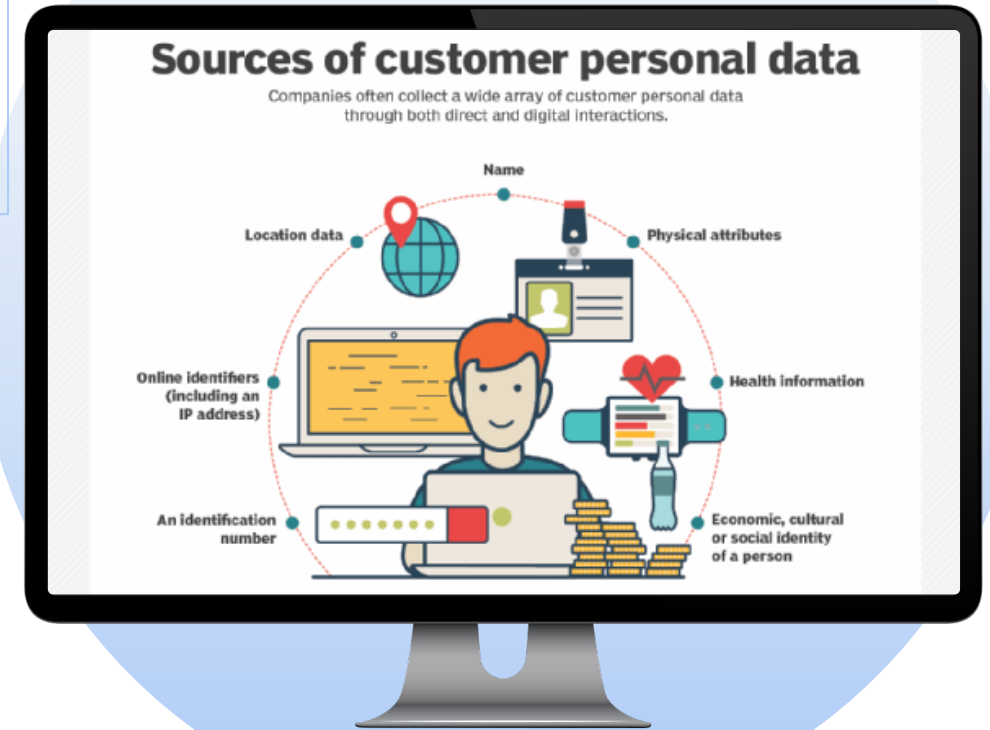
Focus – Business / Organization (financial, reputation, and compliance gray areas)

Scope – Organization data privacy practices, requirements, policies, and strategy

Purpose – Meeting minimums, business interests over consumer data use

Responsibility - ensuring the greatest financial opportunities for business while still meeting compliance

Priority - Greatest legal Return On Investment (ROI) from consumer data



Data Governance - [Data Life Cycle]

- Chief Privacy Officer (CPO)
[Organization Motivated]
- **Data Privacy Officer (DPO)**
[Compliance Motivated]

Focus – Business compliance with consumer data privacy laws and regulations

Scope – Organization data privacy practices, requirements, policies, and strategy – INDEPENDENT of organization

Purpose – Ensuring consumer data privacy compliance within an organization is known, followed, enforced, and established to the greatest extent of the organization

Responsibility – Awareness and compliance with individual data privacy protections for any individual in the system

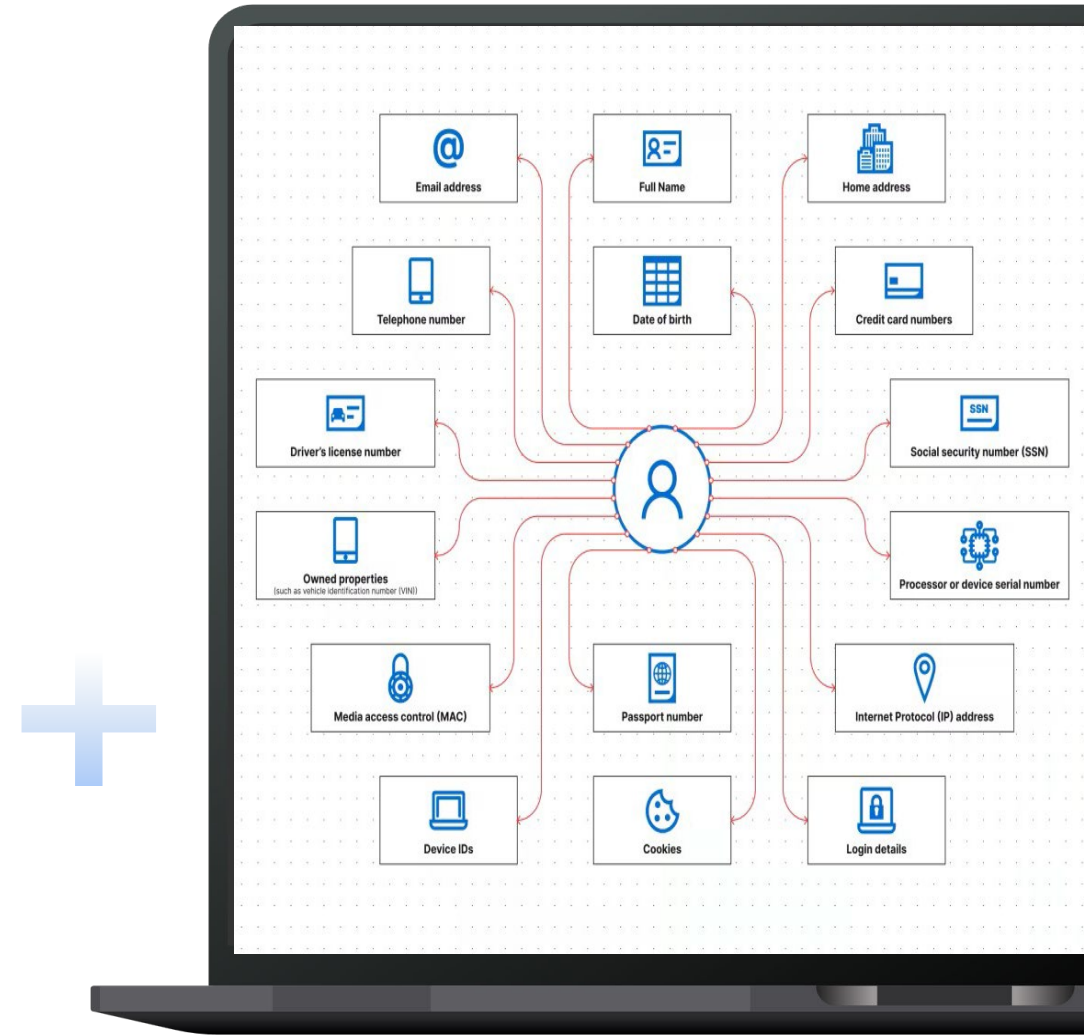
Priority – Data privacy protections for individuals from business or organizations that are not authorized or necessary, the right to be forgotten



NIST states that linked information can be “Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people”. That means cookies and device ID fall under the definition of PII.

General Data Protection Regulation (GDPR)
<https://gdpr.eu/eu-gdpr-personal-data/>

Personal Identifiable Information (PII)





Global Laws
Europe
China
Other (100+)

Data privacy law growth
Diversity of requirements
Governance and Compliance

Global Data Protection & Privacy



<https://oercs.berkeley.edu/privacy/international-privacy-laws>

Individual U.S. State Laws

Data privacy law growth

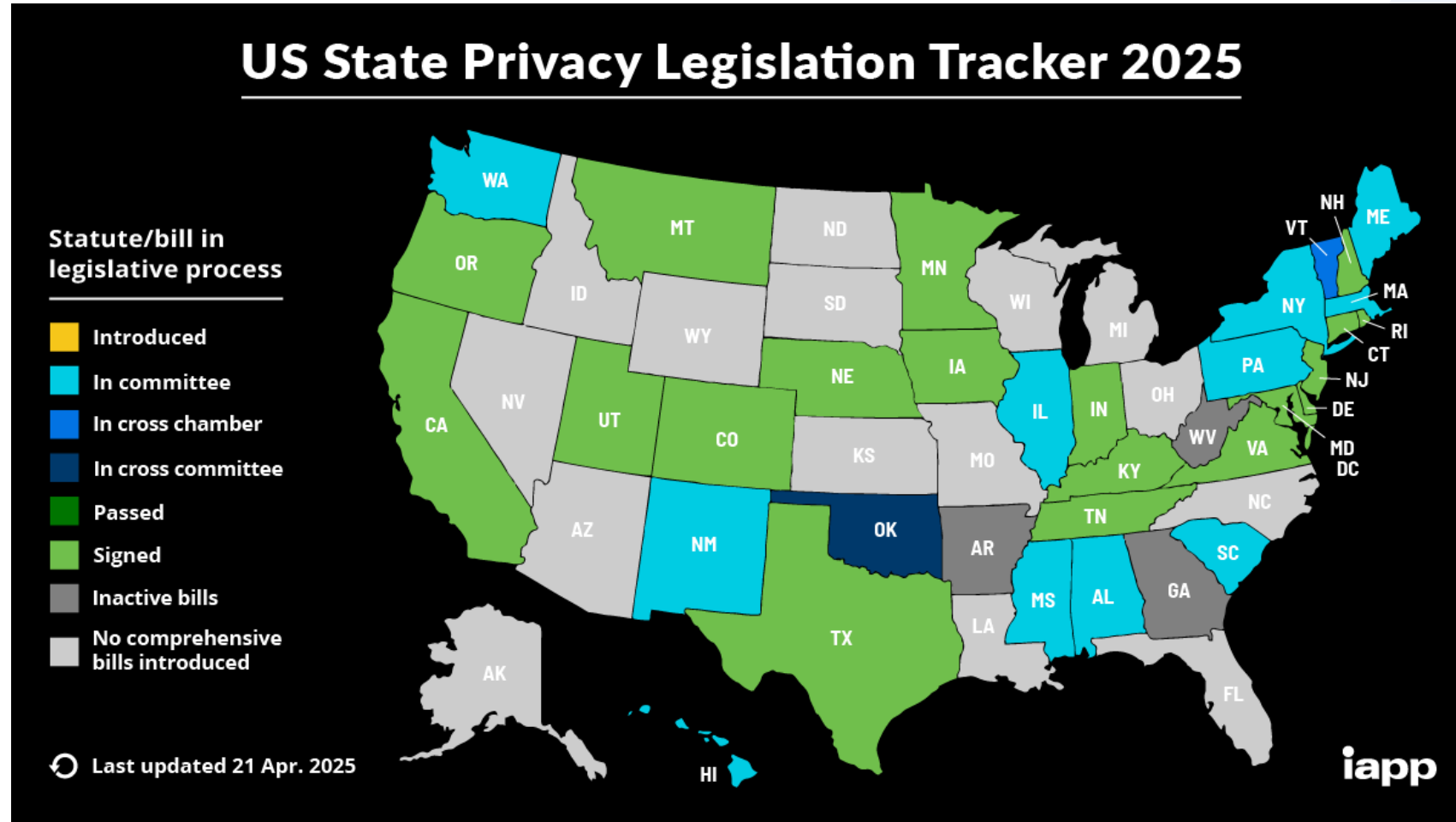
Many similar strategies

California, Colorado, Tennessee,
and Maryland

Vague / Weak

Enforcement

14 Global Data Protection & Privacy



<https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>

15 Future Privacy Law strategy

- Digital Privacy Perspectives
- “Brussels Effect”
- AI data sets
- Biometric Data
- Health Data
- Children
- Data Transfers



<https://fastercapital.com/topics/the-future-of-data-protection-in-the-eu-and-beyond.html>

<https://fpf.org/blog/what-to-expect-in-global-privacy-in-2025/>

16 Privacy Frameworks

Data Privacy Framework (DPF)

- Transatlantic personal data transfers
<https://www.dataprivacyframework.gov/Program-Overview>

NIST Privacy Framework

- Framework developed by US Government to assist with creating and maintaining a Privacy Framework
<https://www.nist.gov/privacy-framework/getting-started-0>

ISO 27701

- International Standard for Privacy Information Management framework
https://www.itgovernance.co.uk/iso-27701?_gl=1*4a8p1l*_up*MQ.*_ga*MTlwMTQ0MTMyNi4xNzQ2OTA4MTAy*_ga_MC7BZLZFSK*cze3NDY5MDgxMDAkbzEkZzAkDE3NDY5MDgxMDAkbzAkDAkaDA



Conclusion

Questions



- Data Privacy
- Data Governance
- Global Law overview
- State Law overview
- Future strategy