So, You Own a Privacy Program Now

Amber Welch

Director, Data Protection & Privacy @ Wiley

Twitter: @MsAmberWelch
LinkedIn: linkedin.com/in/amberwelch1
GitHub: github.com/MsAmberWelch

What’s privacy?

Privacy is not…

Privacy is not… “compliance”

Privacy is not… “legal”

Privacy is…

Privacy is… operational

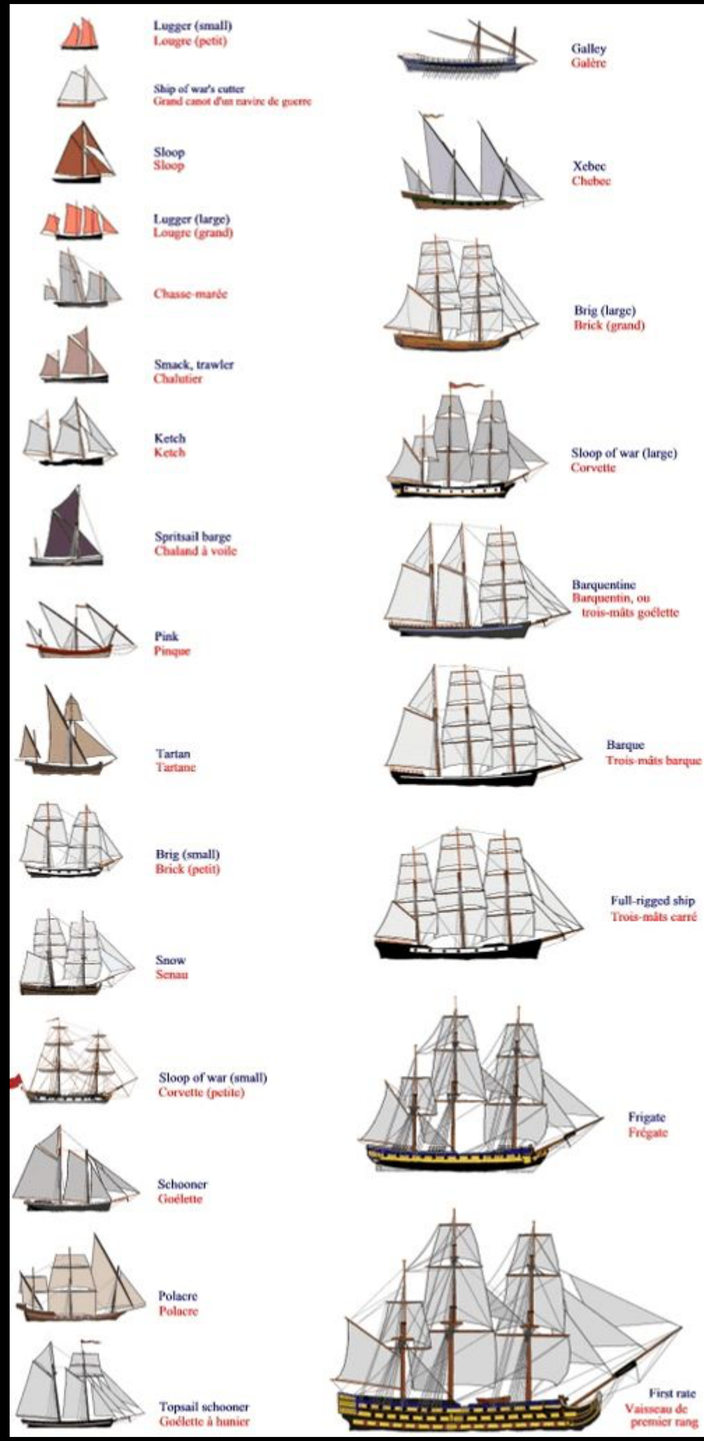
Privacy is… technical

Privacy is… subjective

What’s the plan?

Scope and Exposure

- What countries and regions?
- What industry sectors?
- B2C, B2B, or combined customer base?
- What type and volume of personal data?
- What type of sensitive data?
- What audits and certifications?
- Sales & marketing, product, and HR



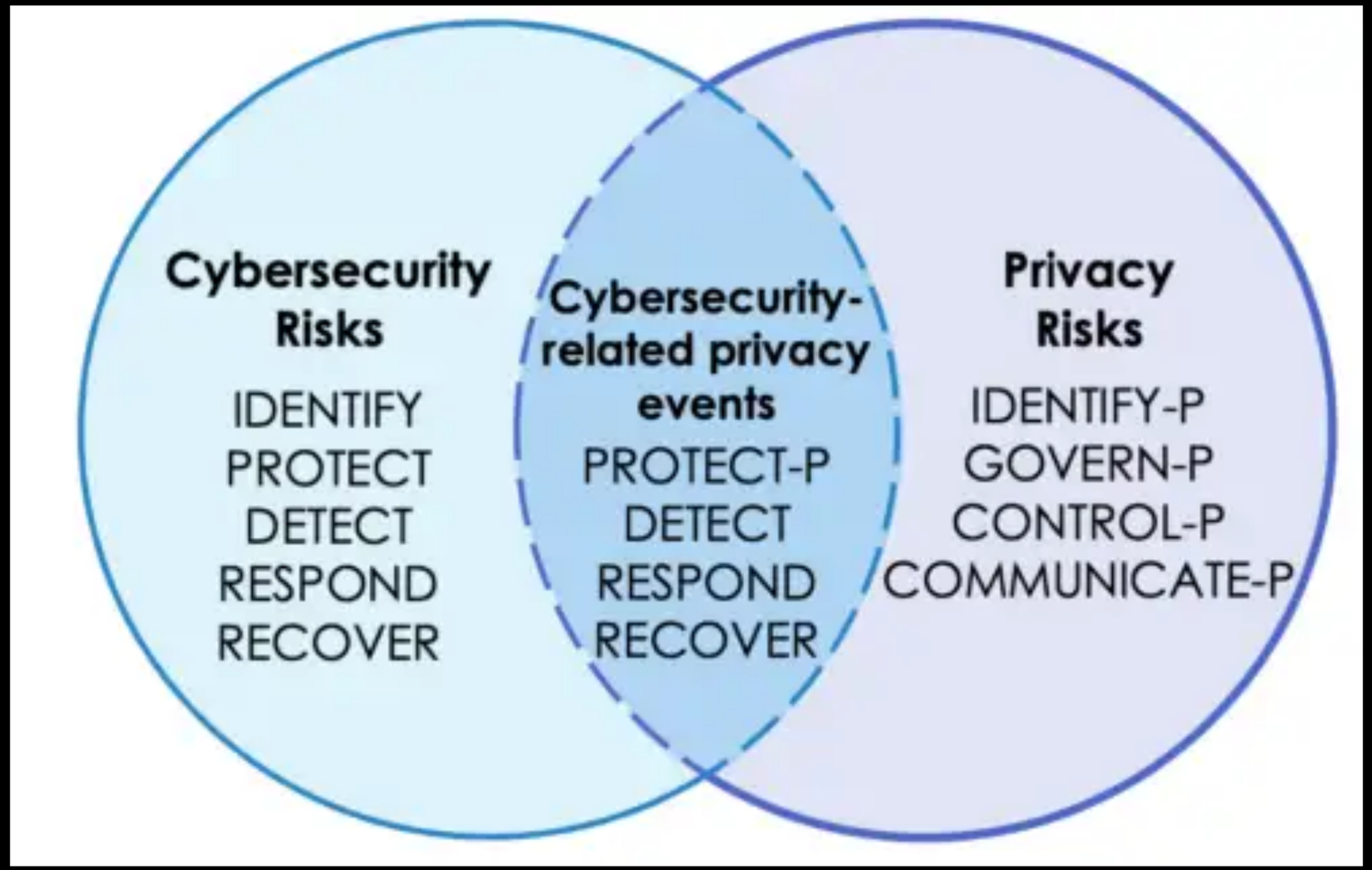
Legal Resourcing

- Internal vs external counsel
- Customer & vendor contracts and data protection agreements (DPAs)
- Transfer Impact Assessments & international transfer mechanisms
- Incident response privilege and breach communications
- Public and internal privacy policies & consent language

Frameworks

- Laws are not frameworks
- Extend security frameworks:
  - ISO 27001 ISMS > ISO 27701 PIMS
  - NIST CSF > NIST Privacy Framework (NIST-P)
  - SOC 2 > Privacy Criteria & AICPA Privacy Management Framework
- Generally Accepted Privacy Principles (GAPP) and OECD
- PCI DSS and HITRUST with modifications

Frameworks: NIST Combined Model



ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology

Low Hanging Fruit

- Name a Data Protection Officer with a privacy inbox

Low Hanging Fruit

- Name a Data Protection Officer with a privacy inbox
- Create an individual rights request mechanism & update public privacy policy

Low Hanging Fruit

- Name a Data Protection Officer with a privacy inbox
- Create an individual rights request mechanism & update public privacy policy
- Release general privacy awareness training and privacy by design training

Low Hanging Fruit

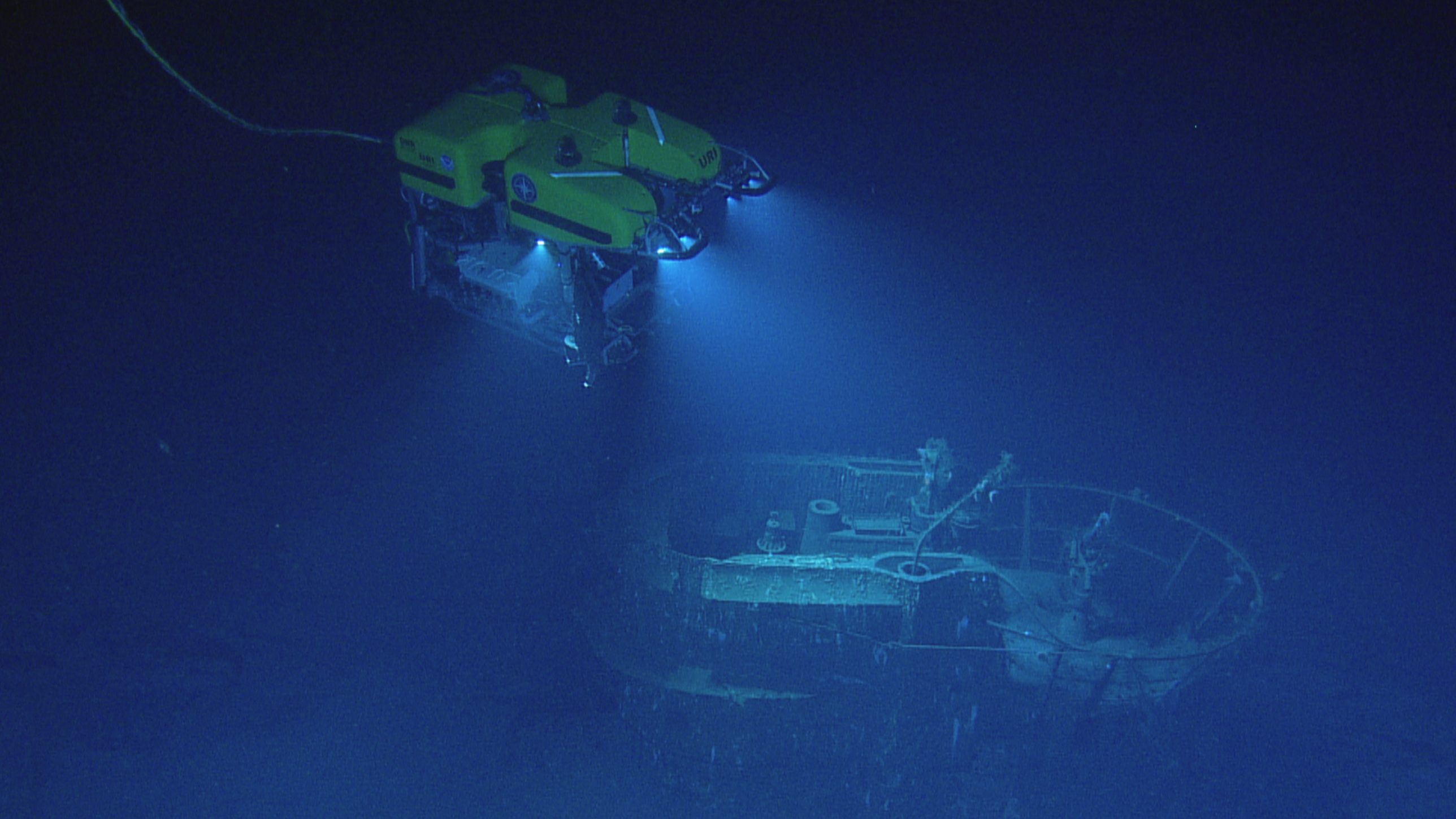
- Name a Data Protection Officer with a privacy inbox
- Create an individual rights request mechanism & update public privacy policy
- Release general privacy awareness training and privacy by design training
- Publish employee policies like acceptable use and data management

Low Hanging Fruit

- Name a Data Protection Officer with a privacy inbox
- Create an individual rights request mechanism & update public privacy policy
- Release general privacy awareness training and privacy by design training
- Publish employee policies like acceptable use and data management
- Add privacy criteria to vendor risk evaluation

Low Hanging Fruit

- Name a Data Protection Officer with a privacy inbox
- Create an individual rights request mechanism & update public privacy policy
- Release general privacy awareness training and privacy by design training
- Publish employee policies like acceptable use and data management
- Add privacy criteria to vendor risk evaluation
- Create an enterprise Data Privacy Champions community


URI

Risk Assessments

- Enterprise risk assessment & registry (e.g., FAIR Model)
- Processing-level assessments:
  - Privacy Impact Assessment & Data Protection Impact Assessment
  - Third party risk assessment (vendor, partner)
  - Specialty assessments (Legitimate Interest, Cross-Border Transfer Impact)
- Engage internal and perhaps external audit

Risk Assessments

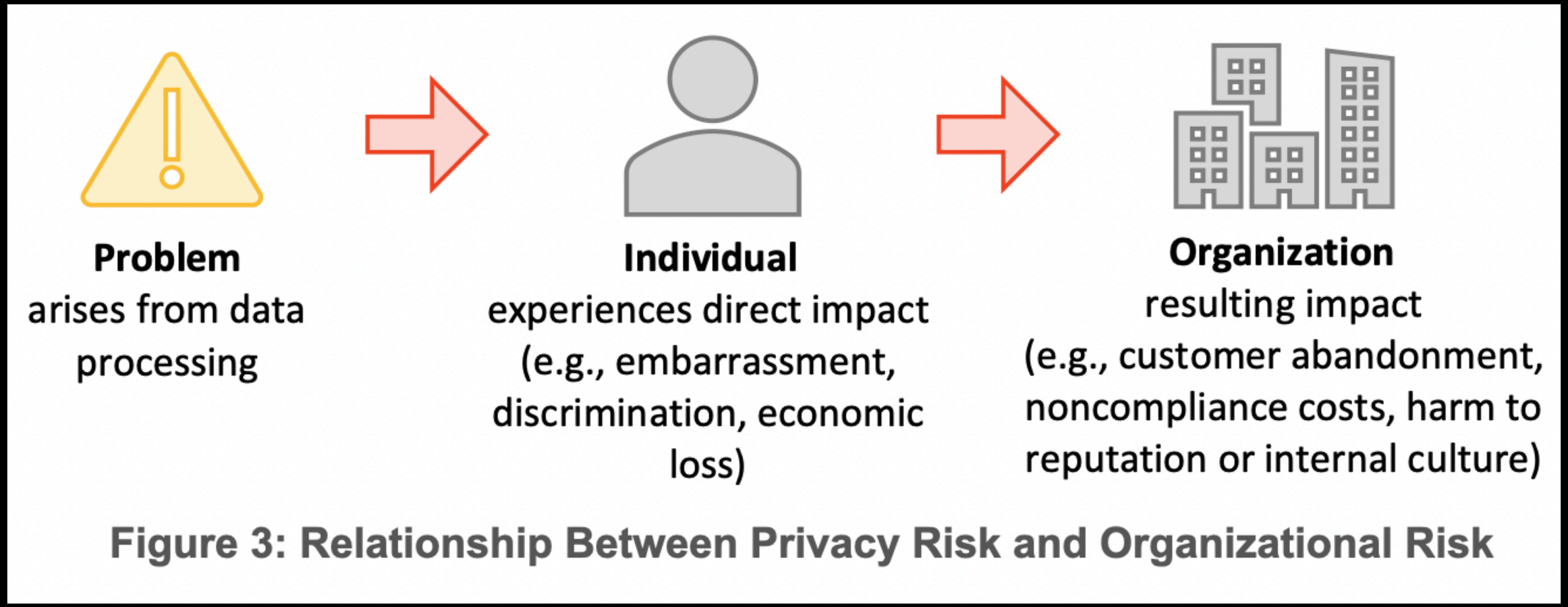


Figure 3: Relationship Between Privacy Risk and Organizational Risk

Data Identification and Governance

- Collaborate with sysadmins, DBAs, data scientists, and data architects

Data Identification and Governance

- Collaborate with sysadmins, DBAs, data scientists, and data architects
- Identify data collection points and basis for collection (consent, contract, etc.)

Data Identification and Governance

- Collaborate with sysadmins, DBAs, data scientists, and data architects
- Identify data collection points and basis for collection (consent, contract, etc.)
- Inventory data processing activities by system & service

Data Identification and Governance

- Collaborate with sysadmins, DBAs, data scientists, and data architects
- Identify data collection points and basis for collection (consent, contract, etc.)
- Inventory data processing activities by system & service
- Leverage DLP or metadata tools for discovery and classification

Data Identification and Governance

- Collaborate with sysadmins, DBAs, data scientists, and data architects
- Identify data collection points and basis for collection (consent, contract, etc.)
- Inventory data processing activities by system & service
- Leverage DLP or metadata tools for discovery and classification
- Apply retention policies to all data

Data Identification and Governance

- Collaborate with sysadmins, DBAs, data scientists, and data architects
- Identify data collection points and basis for collection (consent, contract, etc.)
- Inventory data processing activities by system & service
- Leverage DLP or metadata tools for discovery and classification
- Apply retention policies to all data
- Evaluate data and processes for minimization and purge opportunities

Data Identification and Governance

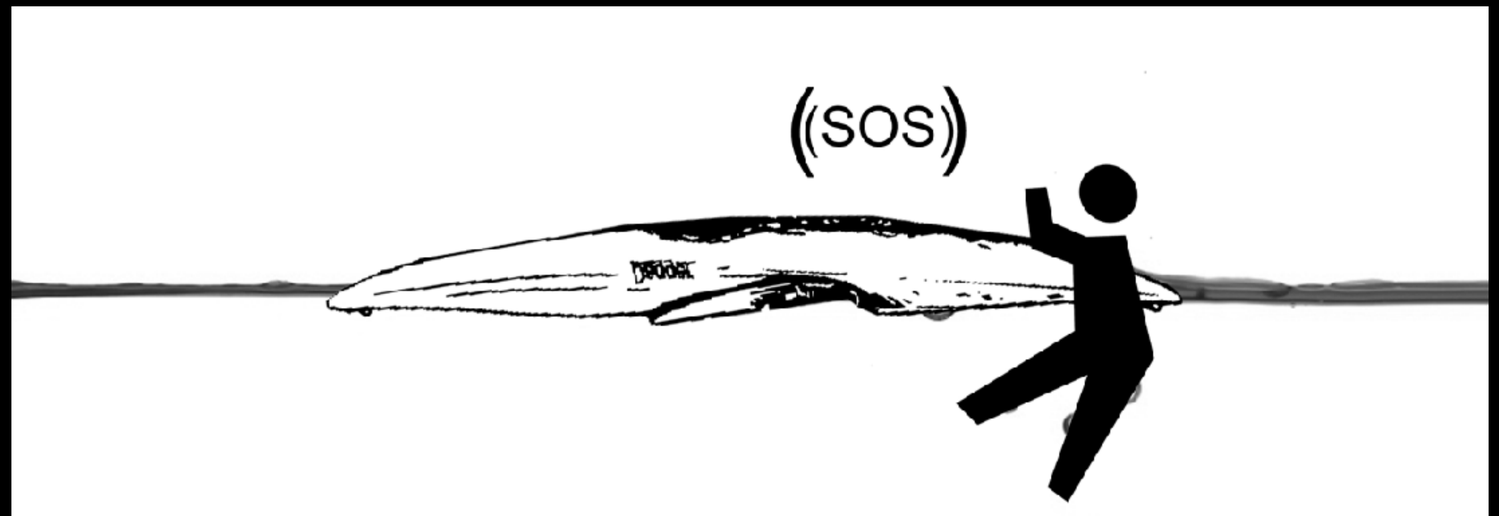
- Collaborate with sysadmins, DBAs, data scientists, and data architects
- Identify data collection points and basis for collection (consent, contract, etc.)
- Inventory data processing activities by system & service
- Leverage DLP or metadata tools for discovery and classification
- Apply retention policies to all data
- Look for opportunities to minimize and securely purge data
- Limit access and data use to what is strictly necessary

Privacy by Design

- Embed privacy reviews and checks through the SDLC from planning to CAB
- Make privacy the default option and give users notice and choice
- Introduce appropriate data-specific technical controls:
  - Data Loss Prevention (DLP)
  - De-identify: anonymize, aggregate, psuedonymize, tokenize, mask, hash
  - Encryption & granular/segregated access management
  - Logs and SIEM alerts for data exposure and abuse

Incident Response

- Add privacy roles to tabletop exercises and use data breach scenarios
- Update incident response plans for non-technical exposure and breach
- Use data governance processes to assess incident severity and response
- Train SOC and incident management teams to recognize personal data



What’s next?

71%
COUNTRIES WITH
LEGISLATION

9%
COUNTRIES WITH
DRAFT LEGISLATION

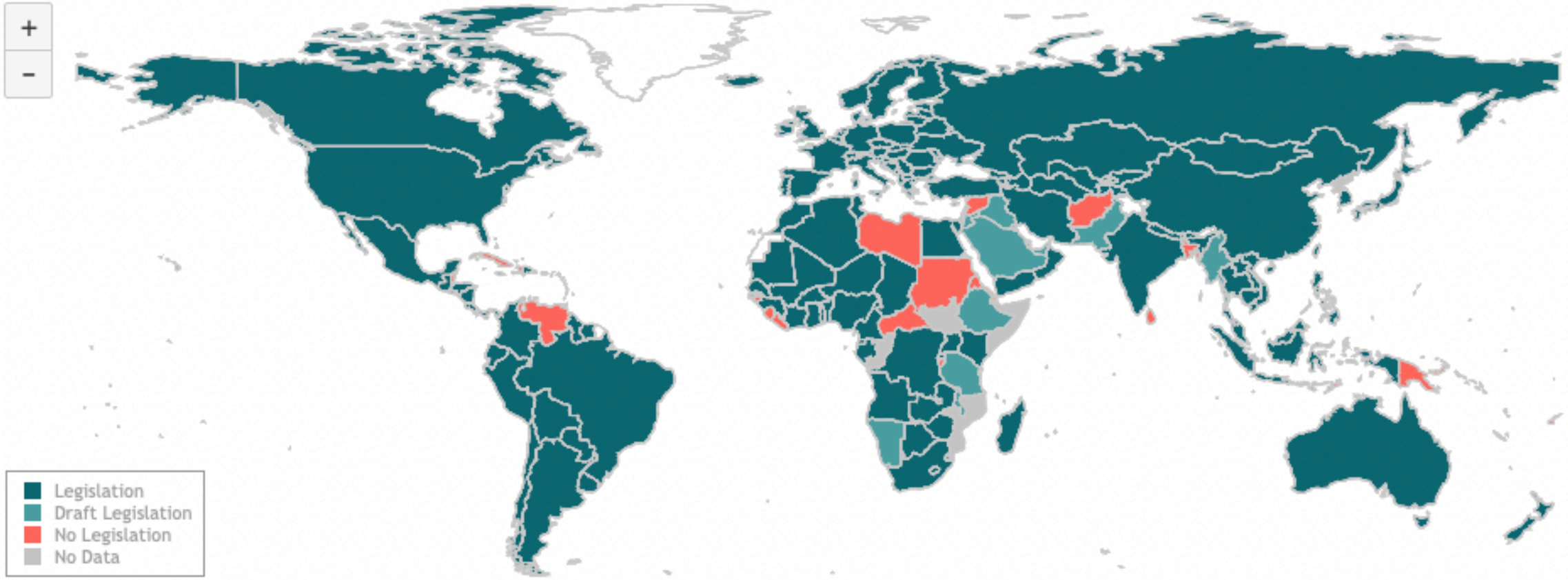
15%
COUNTRIES WITH
NO LEGISLATION

SELECT A COUNTRY

SELECT A REGION

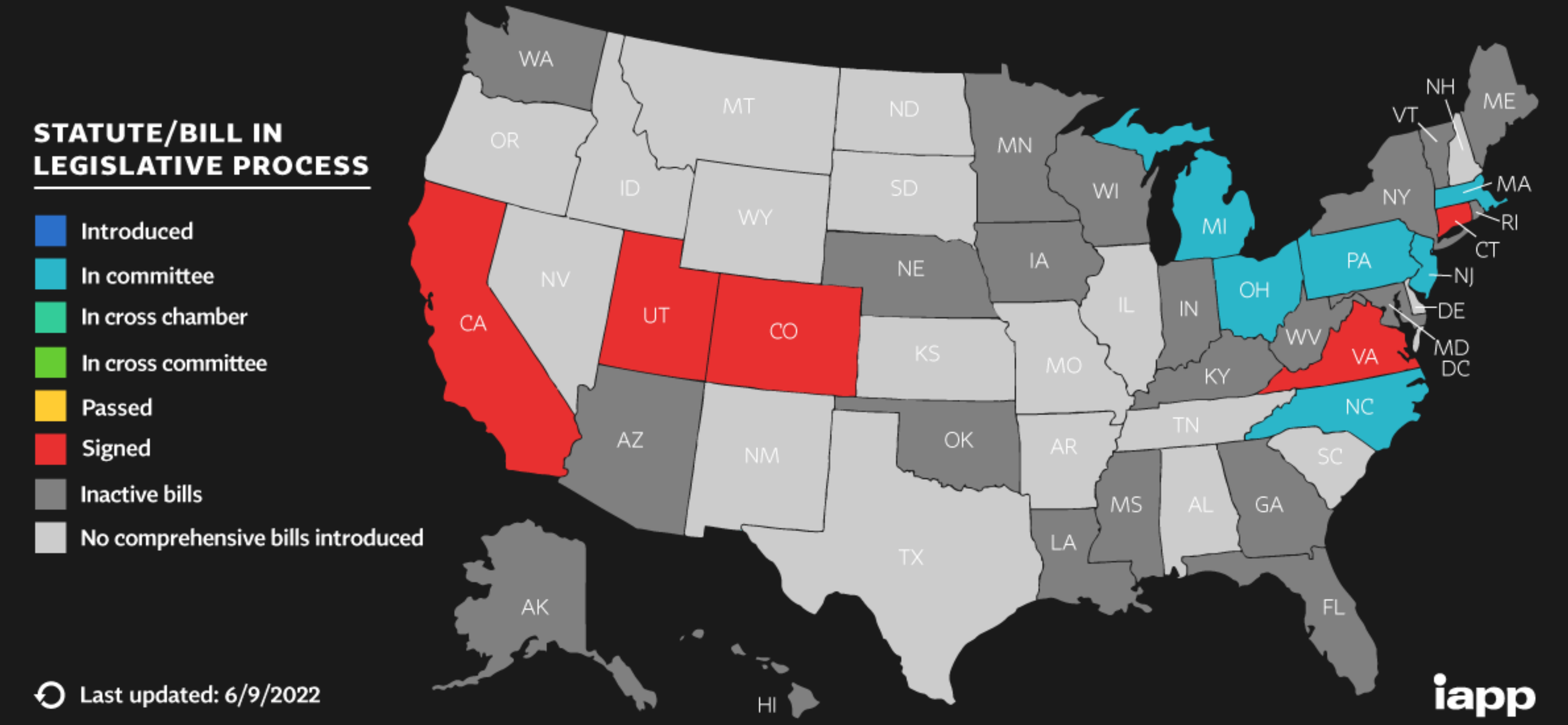
DOWNLO

Data Protection and Privacy Legislation Worldwide



Source: UNCTAD, 14/12/2021

US State Privacy Legislation Tracker 2022



Last updated: 6/9/2022

iapp

American Data Privacy and Protection Act

- Comprehensive federal law to preempt most state laws
- Broad privacy right of action for individual and class action lawsuit
- Executive-level representation for privacy and data security (CPO/CISO)
- SOX-style executive certification of compliance
- Public disclosure and impact assessments of personal data algorithms
- Anti-discrimination clauses and provisions for nonconsensual sexual images
- Ban of “dark patterns” and targeted marketing to minors under 17
- Public transparancy of data processing and third party data disclosures
- Expanded definitions of sensitive data

Follow

Lea Kissner

@LeaKissner

Head of Privacy Eng and CISO @Twitter. Privacy eng, security, crypto & build respect. they/them

California, USA Joined April 2017

406 Following **15.9K** Followers

Twitter: @MsAmberWelch
LinkedIn: linkedin.com/in/amberwelch1
GitHub: github.com/MsAmberWelch

Questions?

Resources

- International Association of Privacy Professionals (IAPP)
- USENIX Privacy Engineering Practice and Respect (PEPR) conference
- NIST Privacy Framework Version 1.0
- The Privacy Engineer’s Manifesto, Michelle Finneran Dennedy et al.
- Privacy Program Management (IAPP CIPM study guide), Russell R. Densmore
- https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

References

- https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
- https://twitter.com/LeaKissner
- https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Bipartisan_Privacy_Discussion_Draft_Bill_Text.pdf

- Images:
  - https://cdn8.dissolve.com/p/D145_207_836/D145_207_836_1200.jpg
  - https://michpics.files.wordpress.com/2021/06/sunset-sailing-by-tp-mann.jpg
  - https://apassionandapassport.com/clear-boat-los-cabos-mexico-baja-california/
  - https://www.travelers.com/resources/boating/5-things-to-know-when-buying-a-boat
  - https://www.bestproducts.com/parenting/kids/g20065129/kids-floaties-for-safe-swimming/
  - https://www.istockphoto.com/photo/two-african-american-happy-successful-mans-at-suit-rich-black-business-mans-against-gm991220344-268628588
  - http://kayakdave.com/wp-content/uploads/2012/09/bang-on-deck-6_edited-1.jpg
  - https://i.pinimg.com/550x/26/4e/e5/264ee5dcdfe47ac70cb5ec3a572cb24e.jpg
  - https://www.globalvillagespace.com/wp-content/uploads/2020/04/Historys-largest-shipbuilding-order-from-Qatar-to-a-Chinese-Company.jpg