November 10, 2023

Using Assessments to Tackle the Privacy Spin Cycle

Jamie Danker
Venable LLP

Kelly DeMarchis Bastide
Venable LLP

Lindsay Vogel
Bumble

Privacy+ Security Forum

Speakers

Jamie Danker

Senior Director of Cybersecurity and Privacy Services
Venable LLP

Kelly DeMarchis Bastide

Partner, Co-chair Privacy and Data Security Group
Venable LLP

Lindsay Vogel

Lead US Counsel, Privacy
Bumble

When everything feels like it's piling up...
Assessments can help sort through the mess.

Laundry List of Assessments

Legally Required

Programmatic

Other

GDPR and DPIAs

A Data Protection Impact Assessment (DPIA) is required under the Art. 35 of GDPR any time you begin a new project that is likely to involve “a high risk” to other people’s personal information.

WP 29 DPIA Criteria (aka “DPIA Triggers”)


Evaluation and Scoring


Automated Decision Making


Systematic Monitoring


Sensitive Data


Large Scale


Matching or Combining Datasets


Data of Vulnerable Subjects


Use of New/Innovative Solutions


Cross-border Data Transfers


Prevent Individuals from Exercising a Right/ Executing a Contract

Privacy+ Security Forum

Laundry List of Assessments

Legally Required

Programmatic

Other

Other Global Privacy Assessments

Check the Care Instructions!

Can you rinse and repeat your privacy assessment methodology to account for multiple jurisdictions?

Opportunities to conduct a single assessment to cover multiple jurisdictional requirements?

Privacy+ Security Forum

Laundry List of Assessments

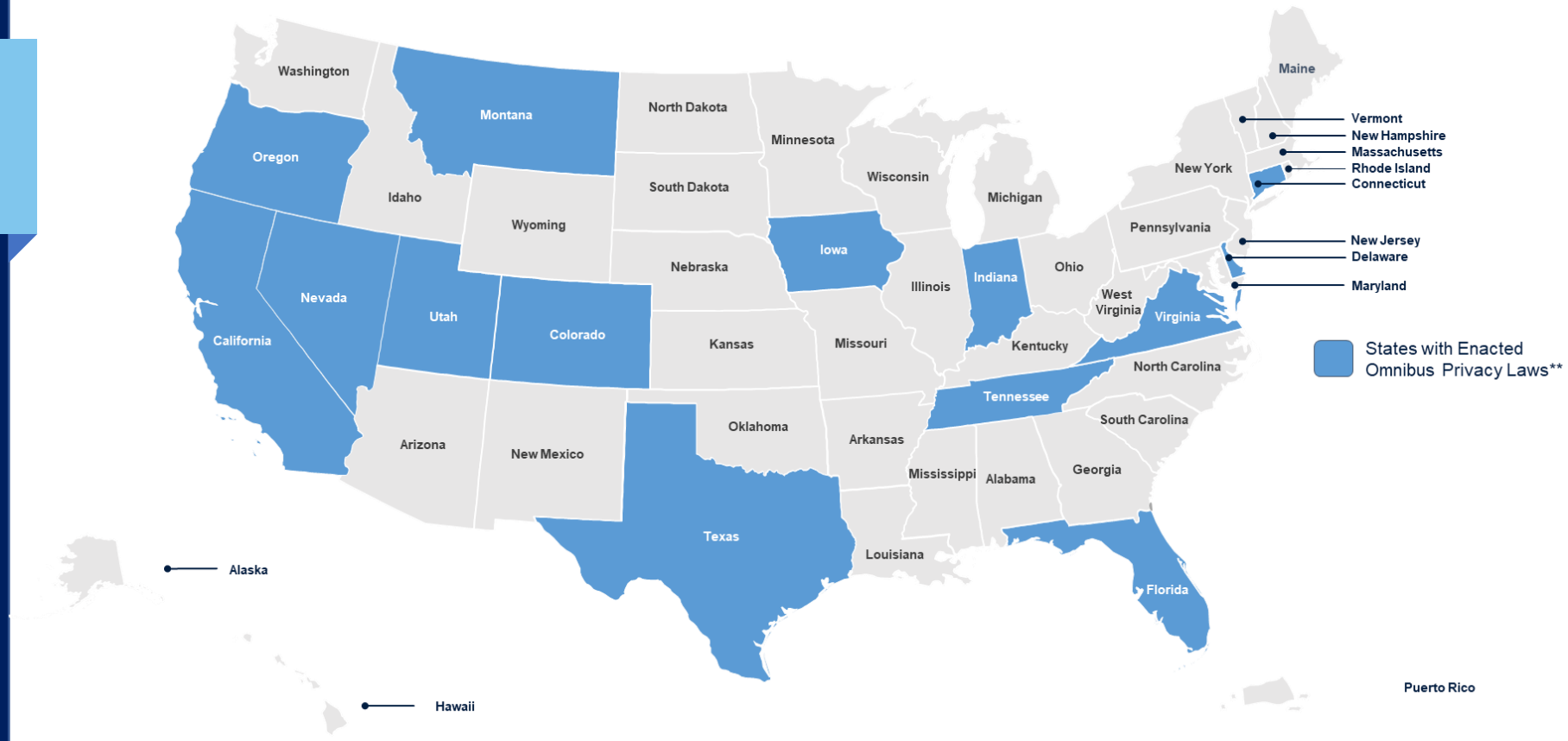
Legally Required

Programmatic

Other

State Privacy Laws

(As of October 1, 2023)



Privacy+ Security Forum

Laundry List of Assessments

Legally Required

Programmatic

Other

CA Draft Risk Assessment Regulations

Conditions for Conducting a Risk Assessment

Selling or sharing personal information

Processing sensitive personal information, with exceptions for certain employment-related purposes

Using automated decision-making technology for significant decisions

Processing the personal information of consumers known to be under 16 years of age.

Monitoring employees, contractors, job applicants, or students

Monitoring consumers' behavior, location, or actions in publicly accessible places

Using personal information to train artificial intelligence or Automated Decisionmaking Technology

Privacy+ Security Forum

Laundry List of Assessments

Legally Required

Programmatic

Other

CA Draft Risk Assessment Regulations

Risk Assessment Requirements

1. A short summary of how they plan to use consumers' personal information.
2. A description of the types of personal information they'll use and whether it includes sensitive data.
3. Information about the relationship between the business and the consumers.
4. What consumers reasonably expect regarding their data's use or why it aligns with how it was collected.
5. Details about how they'll collect and use personal information, why it's necessary, and how long they'll keep it.
6. The number of consumers involved, technology used, and any third parties they'll share data with.
7. The specific purpose for processing data, without vague descriptions.
8. Benefits and negative impacts on consumers' privacy, including potential sources of harm.
9. Safeguards to address negative impacts, how they work, and any remaining risks.
10. An assessment of whether negative impacts, with safeguards, outweigh the benefits, with a clear explanation.

Privacy+ Security Forum

Laundry List of Assessments

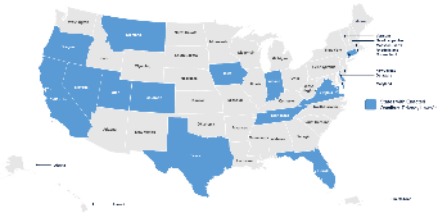
Legally Required

Programmatic

Other

Other State Privacy Laws

(As of October 1, 2023)



Assessments across the following state laws must consider the use of **deidentified data**, the **reasonable expectations of consumers**, the **context of the processing**, and **the relationship between the controller and the consumer**.

Colorado, Connecticut, Florida, Indiana, Montana, Tennessee, Texas, and Virginia require controllers to conduct and document data protection assessments for any processing activities involving:

- Personal data that present a **heightened risk of harm;**
- Processing personal data for purposes of **targeted advertising;**
- The **sale** of personal data;
- Processing personal data for purposes of **profiling**, where such profiling presents a reasonably foreseeable risk of certain impacts, injuries, or harms; and
- Processing **sensitive data**.

Privacy+ Security Forum

Laundry List of Assessments

Legally Required

Programmatic

Other

Tennessee Information Protection Act

TIPA creates a **first-of-its-kind affirmative defense** for controllers and processors. Specifically, the law provides controllers and processors that implement written privacy programs in reasonable conformance to the NIST Privacy Framework an affirmative defense in TIPA actions.

To qualify for the **affirmative defense**, entities must:

1. Create, maintain, and comply with a written privacy program;
2. Design this program in reasonable conformity to the **NIST Privacy Framework** (more on this later);
3. In doing so, consider the size and complexity of the business, the nature and scope of processing activities, the sensitivity of personal information processed, the cost and availability of tools for improvement, and compliance with comparable state or federal laws;
4. Provide consumers the rights granted by TIPA; and
5. Update this privacy program within two years of publication of future updates to the NIST Privacy Framework.

Privacy+ Security Forum

Laundry List of Assessments

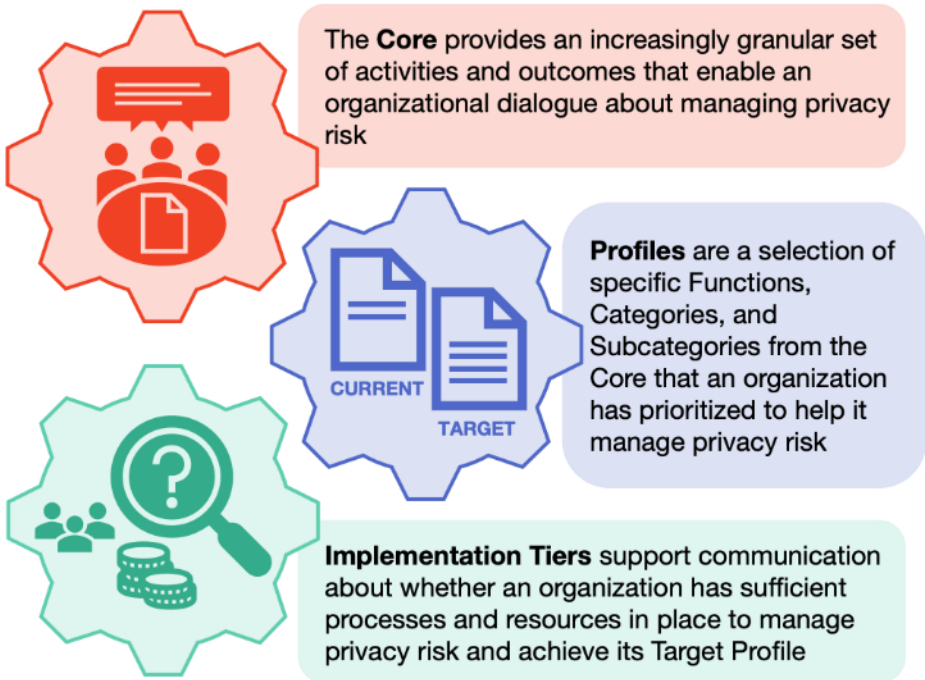
Legally Required

Programmatic

Other

NIST Privacy Framework

A flexible, outcome-based voluntary tool intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy.



Uses of the Privacy Framework

- Establish a new privacy program
- Improve an existing privacy program
- Build privacy into products and services
- Support compliance activities and easily adapt to new or changing privacy requirements
- Be proactive about privacy risk
- Strengthen accountability, collaboration, and communication
- Establish privacy as a differentiator

Privacy+ Security Forum

Laundry List of Assessments

Legally Required

Programmatic

Other

Privacy Threshold Assessment (PTA)

A Privacy Threshold Assessment (PTA) is a high-level evaluation of a process, system, or technology to identify potential privacy risks and determine whether additional reviews may be needed. These reviews are not as in-depth as a DPIA or PIA and can help a team prioritize their efforts.

Targeted Assessments

Rather than looking enterprise-wide, you can improve privacy in a specific area of your business (i.e., within a specific business unit or function).

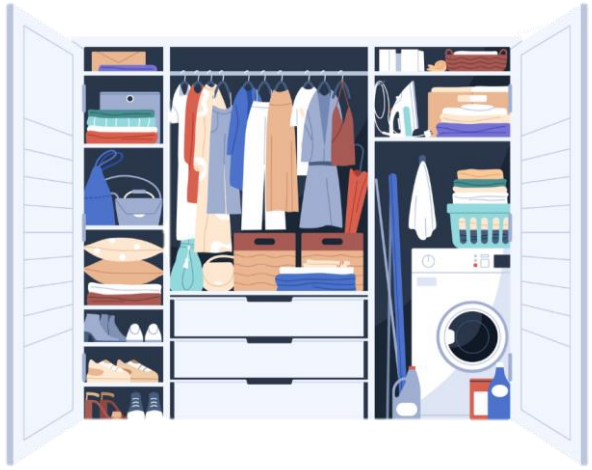
Testing Your Procedures

Assess and remediate potential privacy problems by reviewing the procedures in place (e.g., DSAR Request Response Times, privacy complaints).

Privacy+ Security Forum

Other Helpful Tools

Privacy+ Security Forum

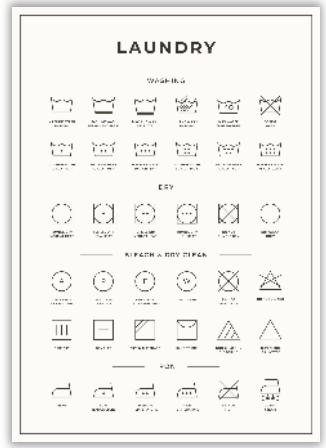


Data Mapping/Inventory

	Function	Category
	IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.

Data Classification Policy

A data classification policy is a sets forth the rules and guidelines for how data should be labeled, handled, stored, and protected according to its sensitivity, confidentiality, and criticality. Revisit, review, and revise, accordingly, to ensure it remains an accurate reflection of your organizations ’s data holdings.



Privacy Perspectives

Lindsay

In House Counsel

Kelly Bastide

Outside Counsel

Jamie Danker

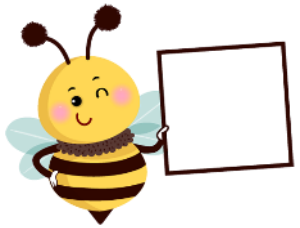
Auditor

Think Like an Auditor

Privacy+ Security Forum

Criteria

Controls
Policies
Legal Requirements
Standards



Evidence

Documentary
Testimonial
Testing

Finding

Criteria
Condition
Cause
Effect
Recommendation

NIST Resources

Using Assessments to Tackle the Privacy Spin Cycle

Privacy+ Security Forum

Questions & Contacts

Jamie Danker

Senior Director of Cybersecurity and Privacy Services
Venable LLP

Kelly DeMarchis Bastide

Partner, Co-chair Privacy and Data Security Group
Venable LLP

Lindsay Vogel

Lead US Counsel, Privacy
Bumble