# Masterclass
# Introduction to Privacy

**Jamie Danker**

Senior Director

Venable LLP

**Zack Martin**

Senior Advisor

Venable LLP

**Ivy Orecchio**

Project Manager

Venable LLP

# How do you identify professionally?

Privacy

Policy

Cybersecurity

Legal

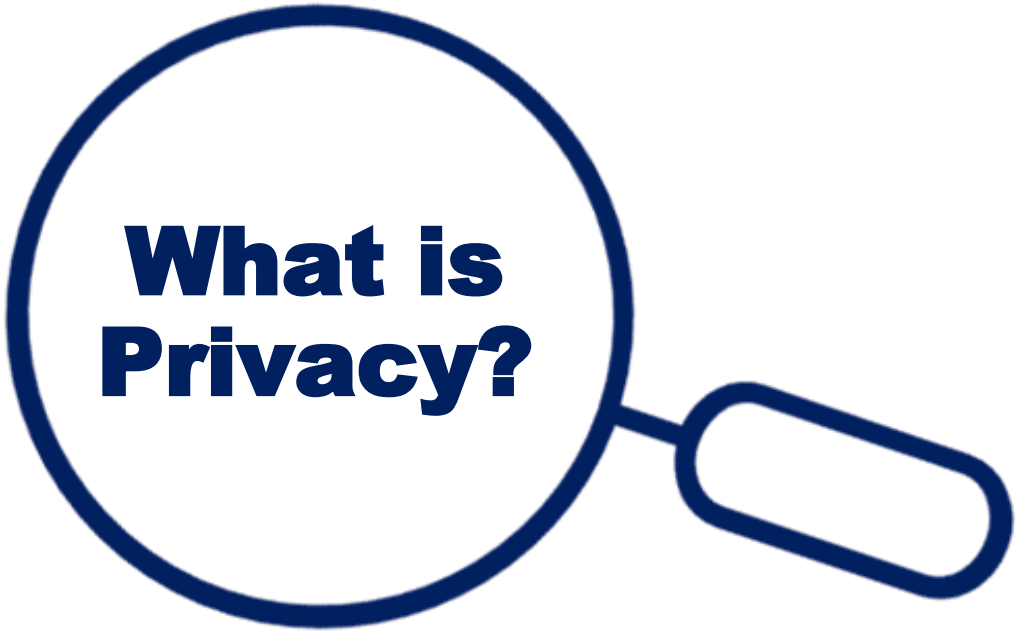
ICAM

I wear a different hat

Engineer

Don’t label me!

# What is Privacy?



**Personal data** - information regarding an individual that can either directly or indirectly be used to identify them

- **Name** - full name, maiden name, alias
- **Contact information** - telephone number, mailing address, email addresses
- **Numerical identifiers** - Social Security number, driver's license number
- **Personal characteristics** - photos, fingerprints, other biometric data
- **Other information that is linked or linkable to an individual**

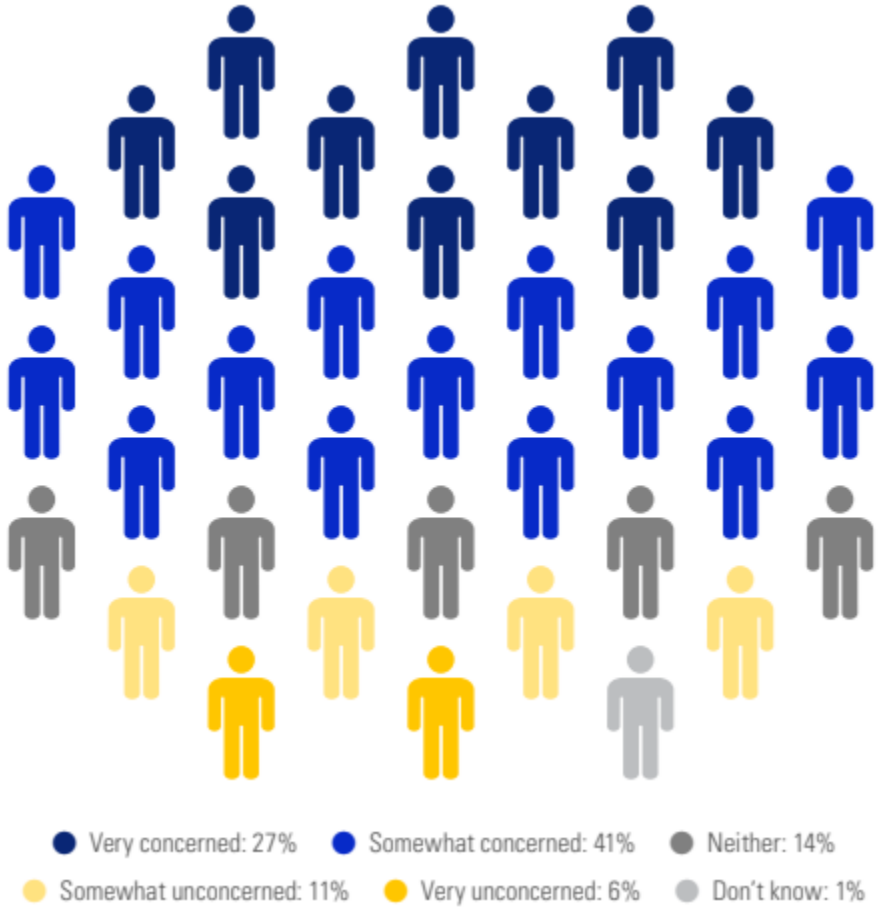




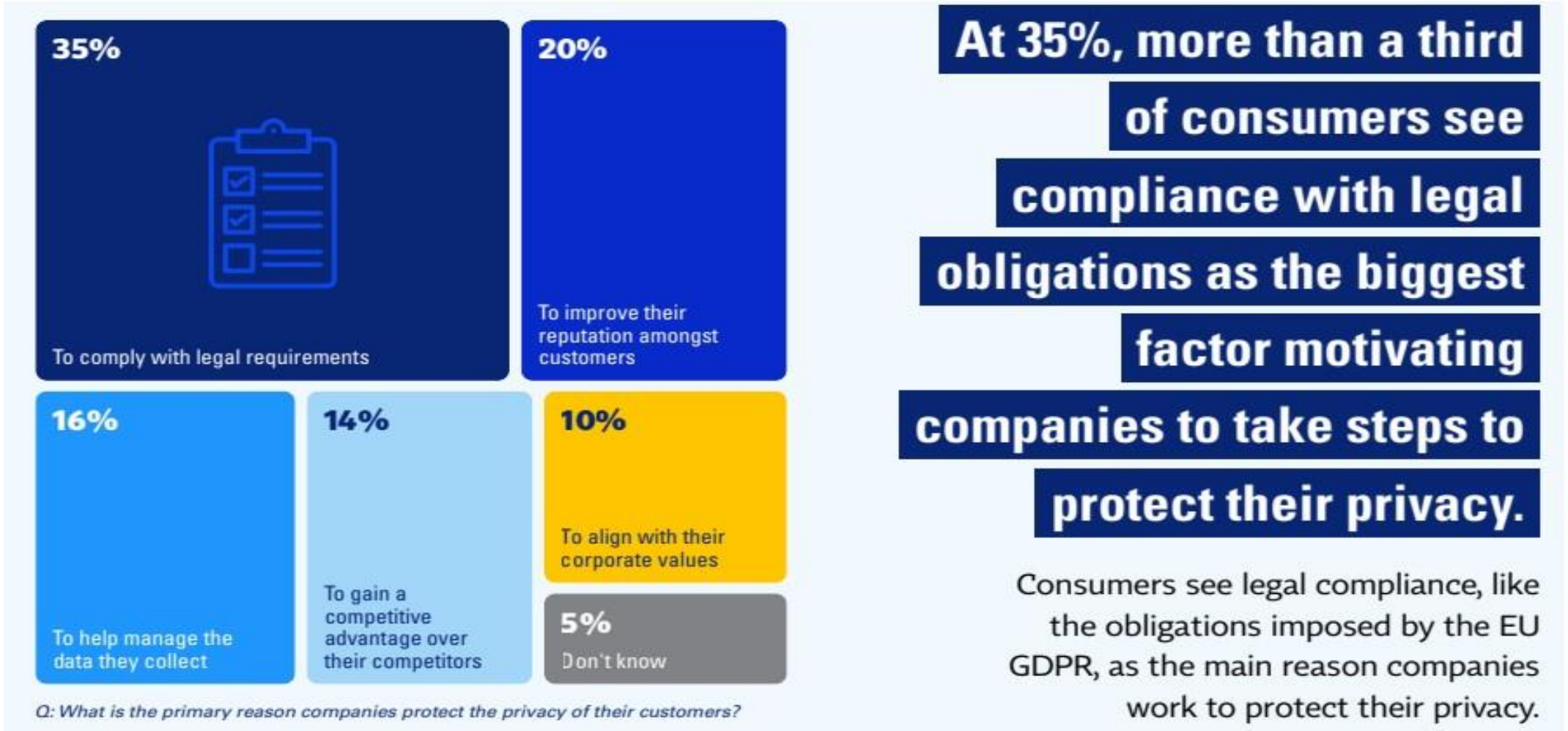
# Why Does Privacy Matter?


**Nearly 68% of consumers throughout the world say they are either somewhat or very concerned about their privacy online.**

Most consumers globally are concerned about their online privacy and, when threatened, will take steps to protect it.




**Source:** International Association of Privacy Professionals (IAPP) Privacy and Consumer Trust Survey (March 2023)




**Source:** International Association of Privacy Professionals (IAPP) Privacy and Consumer Trust Survey (March 2023)

# Why Does Privacy Matter in Digital Identity?

*"Digital authentication supports privacy protection by mitigating risks of unauthorized access to individuals' information. At the same time, because identity proofing, authentication, authorization, and federation involve the processing of individuals' information, these functions can also create privacy risks."*

*"Organizations should consider how decisions related to digital identity that prioritize organizational cybersecurity objectives that might affect or need to accommodate other objectives, such as those related to privacy, equity, usability and other indicators of mission and business performance"*

**Source**: NIST SP 800-63-3 and DRAFT Rev 4, Digital Identity Guidelines

# The Fair Information Practice Principles

| | | | | |
|---|---|---|---|---|
| Access & Amendment | Accountability | Authority | Data Minimization | Data Quality & Integrity |
| Individual Participation | Purpose Specification | Use Limitation | Security Safeguards | Transparency |

**Source**: OMB A-130 FIPPs

# Regulatory Landscape

- **EU** - General Data Protection Regulation (GDPR)
- **Canada** - Personal Information Protection and Electronic Documents Act (PIPEDA)
- **Brazil** - General Data Protection Law
- **China** - Personal Information Protection Law
- **U.S.** - Sector/State Approach
    - Financial (GLBA/SOX), Healthcare (HIPAA), Children's (COPPA), Student (FERPA)
    - State Privacy Laws - Illinois, California, Colorado, Utah, Virginia, Tennessee

**Source:** Global Data Privacy Laws 2023: 162 National Laws and 20 Bills" (2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146

# Biometrics

The identification technology is being used with increasing frequency and with that comes increasing regulation.

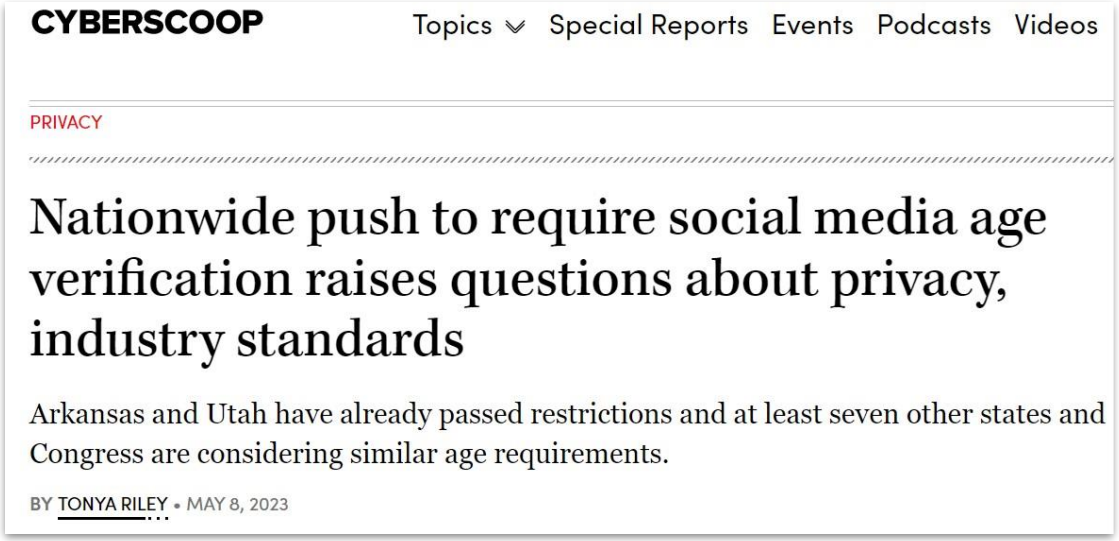
**Illinois' Biometrics Information Privacy Act (BIPA)** has cost companies hundreds of millions of dollars – $650 million for Meta alone – and more than a dozen other states are considering similar legislation. Compliance isn't rigorous, organizations need to:

1. Develop a biometric collection and retention policy.
2. Develop a biometric consent approval form.
3. Verify and document that the Biometric data is secure.
4. Create a written schedule for biometric data cleanup based on the BIPA Act to protect yourself and your employees.

# Age Verification Legislation

States are passing laws requiring age verification to access adult material and social media sites, a similar bill has been submitted in the U.S. Senate.

- **Privacy Fiasco** - Individuals will likely create digital copies of government-issued IDs and email them for verification providing too much information with no guarantee of deletion.
- **Siloed Approach** - Policymakers are taking a siloed approach to solve the problem instead of a comprehensive one with separate approaches for age verification, another to restrict access for teens to access social media, and yet again others for access to federal services, state services, and financial accounts.
- **No Infrastructure** - The digital identity infrastructure in the U.S. doesn't exist to enable a parent to be linked to a child.


CYBERSCOOP

Topics Special Reports Events Podcasts Videos

PRIVACY

Nationwide push to require social media age verification raises questions about privacy, industry standards

Arkansas and Utah have already passed restrictions and at least seven other states and Congress are considering similar age requirements.

BY TONYA RILEY • MAY 8, 2023

# Operationalizing Privacy

# Privacy Risk and Organizational Risk

## Problem

**arises from data processing**

## Individual

**experiences direct impact**

(e.g., embarrassment, discrimination, economic loss)

## Organization

**resulting impact**

(e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

identiverse

**Source**: NIST

#identiverse

# NIST Privacy Engineering Objectives

| | |
|---|---|
| Predictability | Enabling reliable assumptions by individuals, owners and operators about data processing by an information system |
| Manageability | Providing the capability of granular administration of data including alteration, deletion, and selective disclosure |
| Dissaccociability | Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system |

# The Fair Information Practice Principles

| | | | | |
|---|---|---|---|---|
| Access & Amendment | Accountability | Authority | Data Minimization | Data Quality & Integrity |
| Individual Participation | Purpose Specification | Use Limitation | Security Safeguards | Transparency |

**Source**: OMB A-130 FIPPs

# Authority

**Collection, use, processing, and disclosure of personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.**

## In Practice:

- Notice on a federal form identifying the legal authority for the collection (e.g., Form I-9, SSA forms, benefit application)
- Ties closely with purpose specification and use limitations
- Six legal bases within GDPR: Consent, Contract, Legal Obligation, Vital Interests, Public Task, Legitimate Interests

## DO:

✓ Consult with privacy/legal to ensure data processing is authorized.

✓ Obtain consent, when necessary.

## DO NOT:

🚫 Assume that secondary uses of information obtained from another source are authorized.

# Transparency (Openness)

**Organizations should be transparent about their privacy practices and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of personal data.**

## In Practice:

- Notice including UI/UX
- PIA/DPIAs*
- Publicly available reports/public statements

*PIAs and DPIAs can be transparency mechanisms if made publicly available

## DO:

✓ Let individuals know how you handle their data in user-friendly ways.

## DO NOT:

🚫 Change data processing practices without evaluating the need to update notices.

## Privacy Pro Tip:

Consider the NIST Privacy Engineering objective of **Predictability** - the ability for individuals to make reliable assumptions about their data processing.

# Which of the following are examples of transparency:

a. A product privacy notice
b. A sign indicating CCTV recording is in place
c. A generic statement about respectful data use

# Purpose Specification

**Organizations should inform individuals of the purpose(s) for which personal data is processed.**

## In Practice:

- Notice to user explaining the purpose for data processing (e.g., “for identity verification purposes”)
- Purpose and use limitations sometimes defined in law (e.g., biometric data)
- Often expressed in contract language

## DO:

✓ Let individuals know the purpose(s) for personal data.

## DO NOT:

🚫 Provide vague or “blanket” purposes to allow for flexibility.

## Privacy Pro Tip:

For identity implementations pay EXTRA attention to concepts they are foundational to user trust.

# Use Limitation

**Personal data should not be processed, disclosed, or otherwise used for other purposes except with the consent of the data subject or by the authority of law.**

## In Practice:

- Policies and procedures that limit who may have access to data and how that data may be used
- Limits on third parties with whom data is shared, often expressed in contract language

## DO:

✓ Safeguard data against unauthorized uses.

✓ Consult with privacy/legal to ensure new uses are permissible.

✓ Receive updated consent from individuals before using data for new purposes.

## DO NOT:

🚫 Assume that new uses are “covered” without consulting privacy/legal.

🚫 Collect identity data for one purpose and use it for another.

# Data Minimization

**Organizations should limit their data processing to what is necessary to accomplish the stated purpose – this includes minimizing retention.**

## In Practice:

- Risk assessment process
- Data element analysis
- Using attribute references vs. full values
- Retention schedule
- Anonymization/ De-identification
- Selective disclosure

## DO:

✓ Ask tough questions about what is necessary to accomplish your purpose.

✓ Consider privacy enhancing technologies to minimize risks.

## DO NOT:

🚫 Be a data hoarder (you could be increasing your organization's risk profile!!).

🚫 Collect any more data than necessary – just because you can doesn't mean you should!

## Privacy Pro Tip:

Consider the NIST Privacy Engineering objective of **dissassociability** when thinking about mechanisms and techniques to reduce privacy risks of data processing.

# True or False?

Deletion is the only way to truly accomplish data minimization.

# Data Quality & Integrity

**Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.**

## In Practice:

- The authoritative sources of data used to validate self-asserted data
- Accuracy rates/studies on data sources/coverage metrics

## DO:

✓ Reconsider redress processes if an inaccurate determination has been made based on poor data quality.

✓ Consider studies and metrics on data quality (and equity) in evaluating data sources.

## DO NOT:

🚫 Make automated determinations about individuals in situations where data quality issues exist.

## Privacy Pro Tip:

Consider equity and inclusion. Can your identity solution cover your user population?

# Individual Participation

**An individual should have the right to confirm whether or not a data controller has data relating to them, have access to their data, and make requests to erase, rectify, complete, or amend their data and appeal a denial of those requests.**

## In Practice:

- The mechanism for collecting information from the individual (e.g., directly from individual)
- Consents for different lifecycle uses (e.g., collection, disclosure)
- Privacy-related complaints/inquiries process
- Opt-in/Opt-out

## DO:

✓ Give people control of their information when possible.

✓ Establish repeatable processes to respond to requests.

## DO NOT:

🚫 Make the process of filing a privacy complaint or inquiry onerous.

🚫 Take a lengthy period to respond to requests for information.

## Privacy Pro Tip:

Consider the **predictability** and **manageability** privacy engineering objectives as you design your consent mechanisms.

# True or False?

When collecting personal data,
it is always necessary to obtain consent
from the individual.

# GDPR Consent Guidance

Consent must be:

- Freely given
- Specific
- Unambiguous
- With clear and plain language

An organization must:

- Maintain proof of consent
- Enable the right to withdraw consent


**Source:** https://gdpr.eu/gdpr-consent-requirements/

# Security Safeguards

**Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.**

## In Practice:

- Policies, processes and procedures around data handling
- Physical and logical access controls
- Encryption

## DO:

✓ Follow industry best practices to protect personal data

✓ Apply risk frameworks like NIST CSF

✓ Work collaboratively with security/privacy

## DO NOT:

🚫 Implement security measures without coordinating with privacy to ensure full scope of risks are addressed

# Accountability

**Organizations should be accountable for implementing or complying with measures that give effect to the Fair Information Practice Principles.**

## In Practice:

- Privacy Governance Structures – e.g., designating a Privacy Officer, Data Protection Officer, Oversight Board
- Publicly available reports (aligns with Transparency)
- Auditing practices
- Contract provisions to enforce use limitations
- Certification practices (e.g., Kantara Initiative, ISO, FedRamp, SCO)

## DO:

✓ Allocate sufficient resources to implement privacy activities

✓ Consider this principle in all other FIPPs

## DO NOT:

🚫 Overcommit responsibilities to the privacy role

# What Would Privacy Do?

# Scenario

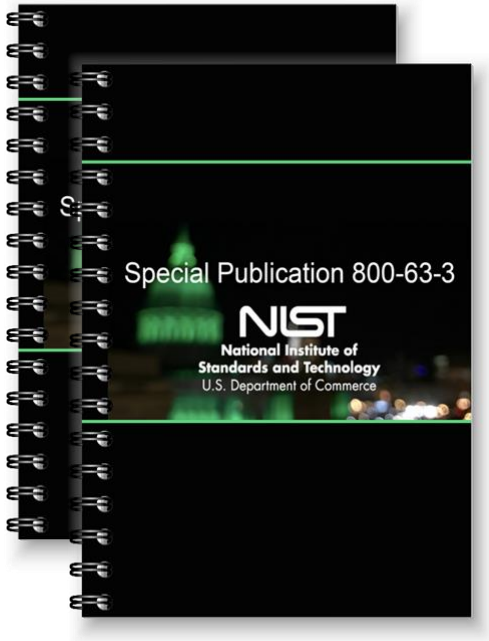
A new law requiring age verification and parental consent for individuals between 13 and 17 goes into effect in July 2024. Your product team must find a way to implement this new requirement but must also address privacy concerns expressed about capturing sensitive data from minors.

Leveraging what you've learned about the FIPPs in practice, how would you apply privacy protections to enabling this type of verification?

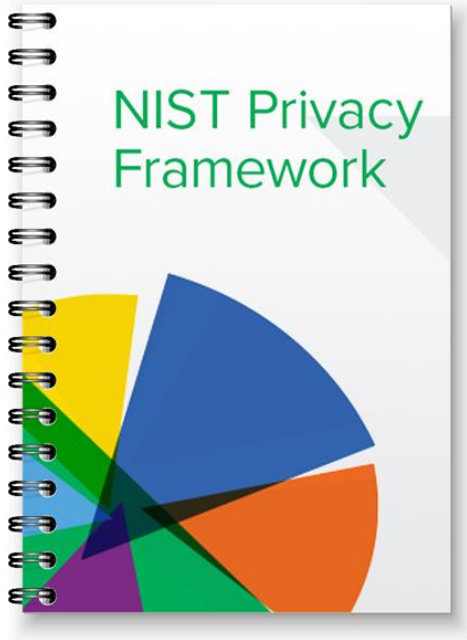
| | | | | |
|---|---|---|---|---|
| Access & Amendment | Accountability | Authority | Data Minimization | Data Quality & Integrity |
| Individual Participation | Purpose Specification | Use Limitation | Security Safeguards | Transparency |

# Questions?

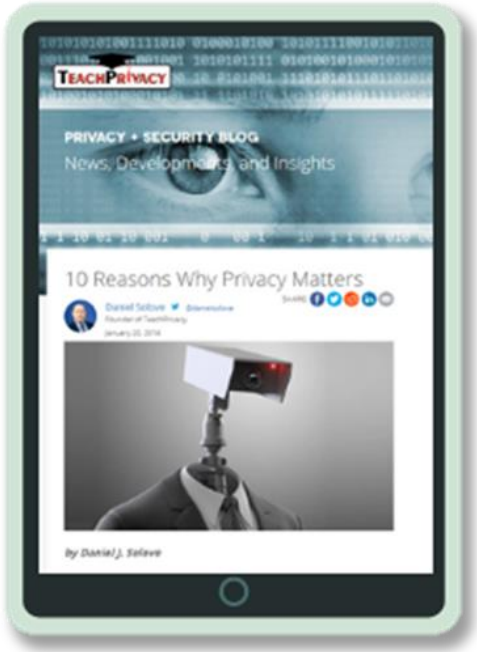
# Recommended Reading



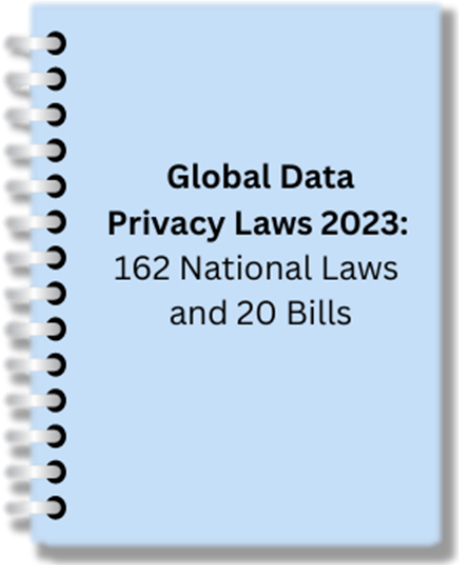

[NIST SP 800-63-3, Digital Identity Guidelines & Draft Revision 4]




[NIST Privacy Framework]




[Ten Reasons Why Privacy Matters] by Dan Solove



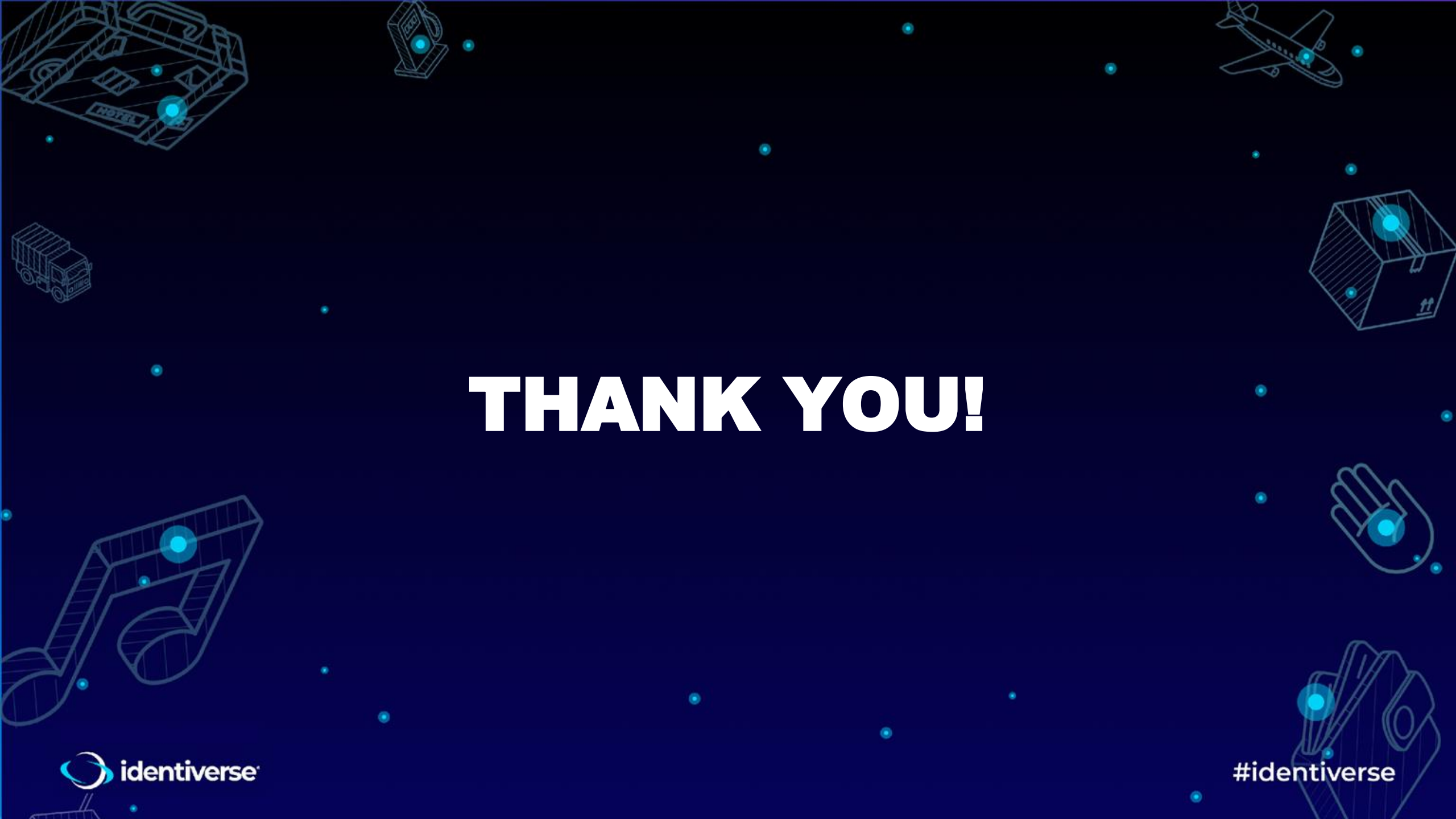

[Global Data Privacy Laws 2023: 162 National Laws and 20 Bills] (2023)


International Association of Privacy Professionals

identiverse

#identiverse


BE THE PRIVACY PRO
YOUR DOG THINKS YOU ARE


THANK YOU!
identiverse
#identiverse