FUTURE OF PRIVACY FORUM

Data Minimization

Jordan Francis
Senior Policy Counsel, U.S Legislation

ABOUT FPF

FPF is a global non-profit organization that advances principled and pragmatic data protection, AI and digital governance practices. We convene leaders across industry, academia, and the public sector to provide expert analysis, benchmarking, and best practices that support responsible innovation and regulatory compliance.

FUTURE OF PRIVACY FORUM

🔗 https://fpf.org/blog/fpf-unveils-paper-on-state-data-minimization-trends

Overview of Data Minimization Requirements

Origins in the Fair Information Practice Principles (FIPPs)⏩

Collection Limitation: Do not collect or retain personal information beyond what is adequate, relevant, and proportionate to accomplish a specified, lawful purpose

Purpose Specification: Provide notice of the specific purpose(s) for which personal information is being collected.

Purpose Limitation: Do not use personal information for purposes that are not compatible with the purpose at collection, except with the individual's consent

Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines

Foundation international framework established in 1980 (updated 2013) to protect personal data and facilitate cross-border data flows. Relevant principles—

- **Collection Limitation Principle:** 7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality Principle:** 8. 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.
- **Purpose Specification Principle:** 9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation Principle:** 10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

    a) with the consent of the data subject; or

    b) by the authority of law.

OECD/LEGAL/0188
Adopted on: 23/09/1980
Amended on: 11/07/2013

FUTURE OF PRIVACY FORUM

APEC Privacy Framework (2015)

- **Collection Limitation:** 24. The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.
- **Use of Personal Information:** 25. Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:

  a) with the consent of the individual whose personal information is collected;

  b) when necessary to provide a service or product requested by the individual; or,

  c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

Asia-Pacific Economic Cooperation (APEC) Privacy Framework (2015)

FUTURE OF PRIVACY FORUM

General Data Protection Regulation (GDPR)

One of many Article 5 principles

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;
- Accountability

Principles relating to processing of personal data

"Personal data shall be . . . adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"

FUTURE OF PRIVACY FORUM

Data Minimization in Practice

- Data Audits
  - Data inventory
  - Assessing data quality and adequacy
- Data Mapping
  - Identifying systems and documenting data flows
  - Documenting processing activities
  - Data tagging
  - Classifying data
- Partner/Vendor oversight

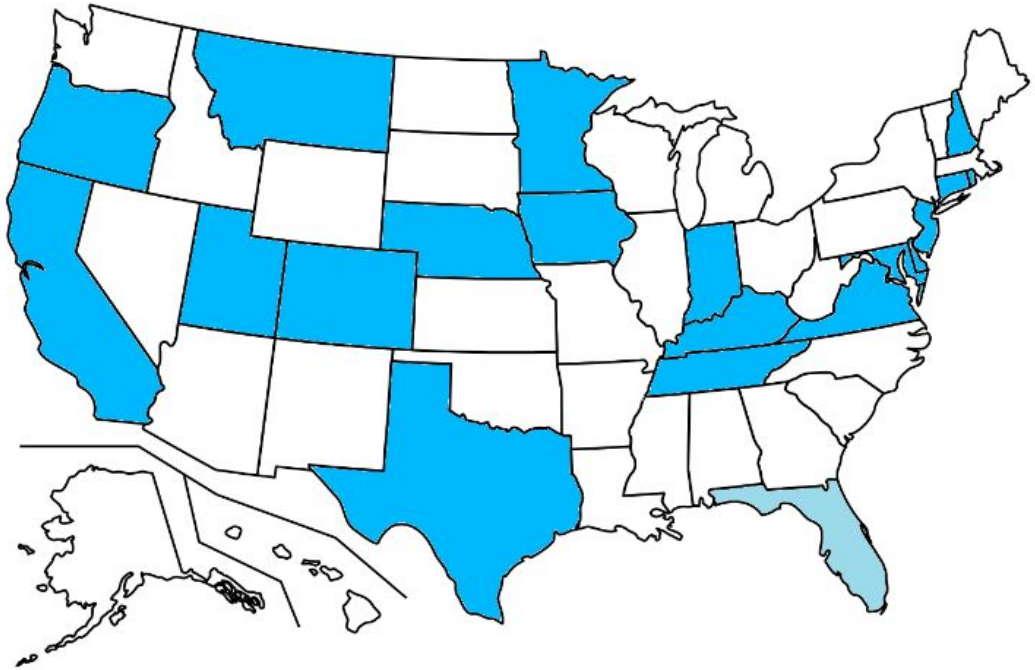
- Technical Safeguards
  - Use of privacy enhancing technologies (PETs)
    - Synthetic data, differential privacy, homomorphic encryption
  - Anonymization, Pseudonymization and Deidentification
  - Access controls

FUTURE OF PRIVACY FORUM

U.S. State Privacy Laws
→ Three Standards

19 State Comprehensive Privacy Laws in 6 Years

↳ 3 Distinct Data Minimization Standards



FUTURE OF PRIVACY FORUM

The Majority Requirement: Disclose, Get Consent

A controller must—

- **Data Minimization:** Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, *as disclosed to the consumer*
- **Purpose Limitation:** Not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's *consent*
- **Sensitive Data Opt-in:** Not process a consumer's sensitive data without first obtaining the consumer's *consent* (freely given, specific, informed, unambiguous)

This is the standard in **Colorado, Connecticut*, Delaware, Indiana, Kentucky, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Virginia**

➔ *Provides regulatory certainty to controllers*

* amended in 2025

"Procedural" Data Minimization

FUTURE OF PRIVACY FORUM

California: Reasonably Necessary and Proportionate

California Consumer Privacy Act, as amended by the California Privacy Rights Act (2020)

Expanded notice requirements and new, additional data minimization requirement—

- A business's collection, use, retention, and sharing of a consumer's personal information shall be *reasonably necessary and proportionate* to achieve
    - the *purposes for which the personal information was collected* or processed, or
    - for *another disclosed purpose that is compatible* with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

→ Regulations go further

FUTURE OF PRIVACY FORUM

CCPA Regulations § 7002: Reasonable Expectations

(a) . . . [A] business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve:

(1) *The purpose(s) for which the personal information was collected or processed*, which *shall comply with the requirements set forth in subsection (b)*; or

(2) Another disclosed purpose that is compatible with the context in which the personal information was collected, which shall comply with the requirements set forth in subsection (c).

Quasi- "Procedural" and "Substantive"

(b) *The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s)* whose personal information is collected or processed . . . based on the following:

(1) The relationship between the consumer(s) and the business . . .

(2) The type, nature, and amount of personal information that the business seeks to collect or process . . .

(3) The source of the personal information and the business's method for collecting or processing it;

(4) The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, such as in the Notice at Collection and in the marketing materials to the consumer(s) about the business's good or service; and

(5) The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s).

(c) [Factors for whether secondary use is compatible]

(d) [Factors for necessary and proportionate]

FUTURE OF PRIVACY FORUM

Maryland Online Data Privacy Act: What's Necessary?

Data Minimization (Personal Data): A controller must limit the collection of personal data to what is *reasonably necessary* and proportionate to provide or maintain a *specific product or service requested* by the consumer to whom the data pertains

Purpose Limitation: A controller must obtain consent to process personal data for a purpose that is neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed

Data Minimization (Sensitive Data): A controller must limit the collection, processing, and sharing of sensitive data to what is *strictly necessary* to provide or maintain a *specific product or service requested* by the consumer to whom the personal data pertains

"Substantive" Data Minimization

American Data Privacy and Protection Act (ADPPA) of 2022

➔ MODPA

FUTURE OF PRIVACY FORUM

MD Attorney General - MODPA FAQs

How is a business supposed to figure out what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by an individual consumer?

A violation of MODPA is a *per se* violation of Maryland's Consumer Protection Act, meaning a violation of MODPA is a Consumer Protection Act violation. A business can determine what is "reasonably necessary and proportionate to provide or maintain a specific product or service" based on the expectations of the reasonable consumer about how the data that is collected will be used.

→ Converging with CA's standard?

🔗 https://oag.maryland.gov/resources-info/Pages/data-privacy.aspx

FUTURE OF PRIVACY FORUM

More than Maryland: Similar Requirements in Sectoral Laws

Washington My Health My Data Act

A regulated entity may not *"collect"* (i.e., process) any *consumer health data* except:

(i) with a consumer's consent, or

(ii) to "the extent *necessary* to provide a *product or service* that the consumer to whom such consumer health data relates has *requested* from such regulated entity or small business."

Separate, signed "authorization" required to *sell* consumer health data.

New York Child Data Protection Act

An operator of a website, online service, online application, mobile application, or connected device cannot *collect* the *personal data* of a teen unless the *collection* is *strictly necessary* for one of nine *permitted purposes* listed in the act

E.g., providing a specific product or service requested by the covered user

or the operator obtains informed consent for the collection

➔ May 2025 guidance on how to interpret these provisions

FUTURE OF PRIVACY FORUM

FUTURE OF PRIVACY FORUM

Questions?

jfrancis@fpf.org