May 11, 2023

The Room Where it Happens: Privacy Meets Product Development

Stephanie Buholz
Southwest Airlines

Rachel Marmor
Holland & Knight

Maggie Gloeckle
HP Enterprises

Christin McMeley
Comcast Corporation

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Stephanie Buholz

Privacy Operations
Southwest Airlines

Rachel Marmor

Partner, Data Strategy, Security, and Privacy
Holland & Knight LLP

Maggie Gloeckle

Chief Privacy Officer
HP Enterprises

Christin McMeley

Chief Privacy and Information Security Officer
Comcast Corporation

Agenda

Privacy+ Security Forum

Objective: to share knowledge about how organizations have developed functionalities and processes to provide consulting to product teams on privacy and security issues.

- The Privacy Landscape
- Setting up the Privacy Function(s)
- The Product Counseling Lifecycle
- Processes and Technology

The Landscape

Overview

Explosion of Legal obligations

Privacy+ Security Forum

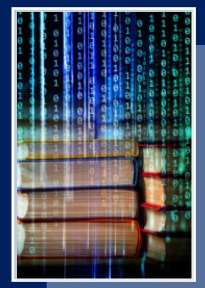
Emphasis on thoughtful use of data

Privacy+ Security Forum

Source	Legal Requirement
California Privacy Rights Act – Cal. Civ. Code § 1798.100(c)	A business' 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.
CCPA Regulations – 11 CCR § 7002(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. The consumer's reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following factors: (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. (5) The degree to which the involvement of service providers, contractors, third parties, or other entities in collecting or processing of personal information is apparent to the consumer(s).
Colorado Privacy Act – Color Rev. Stat. § 6-1-1308(3)	duty of data minimization. A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed.
CPA Regulations – Rule 6.06	A. Controllers shall specify the express purposes for which each category of Personal Data is collected and Processed in both external disclosures to Consumers, including privacy notices required by C.R.S. § 6-1-1308(1), as well as in any internal documentation required by this Part 6 B. The express purpose must be described in a level of detail that gives Consumers a meaningful understanding of how each category of their Personal Data is used when provided for that Processing purpose.
Virginia Consumer Data Protection Act – Va. Code Ann. § 59.1-578(A) Connecticut Act Concerning Personal Data Privacy and Online Monitoring – Sec. 6(a)	A controller shall: 1. 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; 2. Except as otherwise provided in [the law], 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.

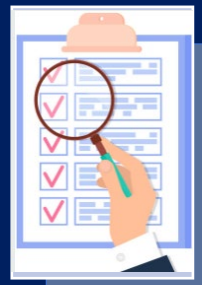
Key Data Risks

Data Integrity and Availability



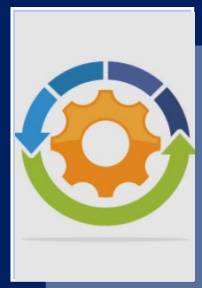
Lawfulness of Intended Use

Unintended Use or Secondary Use



Transparency and Consumer Expectations

Compliance with Law



Data Lifecycle Management

Getting Started

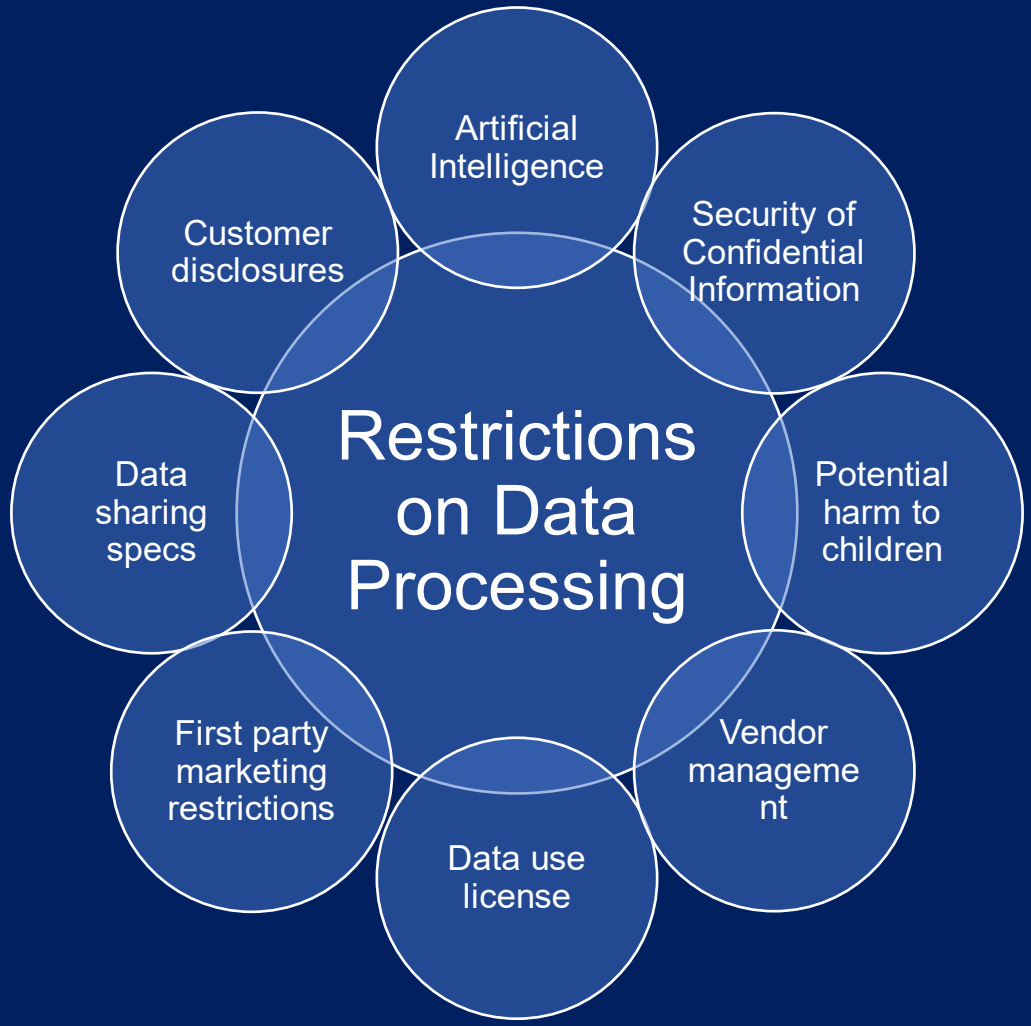
Roles and responsibilities in privacy product counseling

Poll

Privacy+ Security Forum

- What industry are you in?
- Where should responsibility for privacy compliance lie?
- Where does responsibility for privacy compliance lie?

What is Privacy?



The Privacy Machine

Privacy+ Security Forum

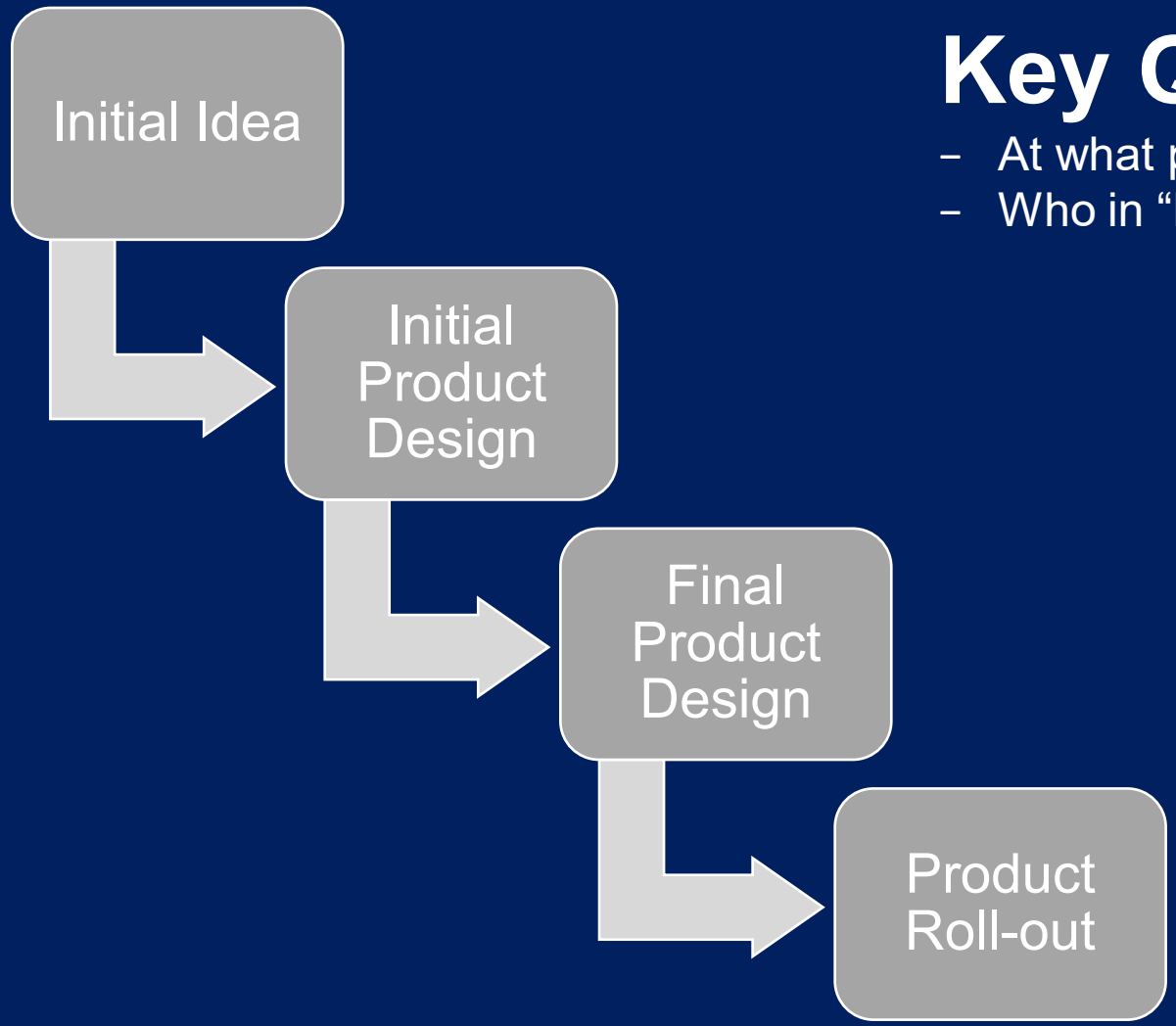
Key Questions

- Is the Chief Privacy Officer the head lawyer, or someone else?
- Is the legal structure centralized into one head?
- Should products have dedicated privacy operatives?
- What is Privacy Operations and where is it positioned?
- What other groups play a key role?

Product Counseling Lifecycle

Converting skeptics to the privacy way

Engagement model for Privacy



Key Questions

- At what point does Privacy get involved?
- Who in “Privacy” gets involved?

The Counseling Process

Creating efficiency, repeatability, and defensibility

The Privacy Tool Belt

Privacy+ Security Forum

- What is a DPIA?
  - GDPR: An assessment of the impact of a processing activity that is likely to result in a high risk to the rights and freedoms of individuals. The assessment must take into consideration the necessity and proportionality of the processing activity, risk, and measures to address identified risks.
  - CT: An assessment of a processing activity that presents a heightened risk of harm to an individual, including targeted advertising, sale of personal data, and profiling. The assessment must weigh the pros and cons of the processing activity for the controller, individual, and public.
  - CO: An assessment of a processing activity that presents a heightened risk of harm to an individual. The assessment must include detailed information about the processing activity, nature and purpose of the processing, source and nature of risk, measures to reduce identified risks, how benefits outweight the risks, any internal or external audit conducted, relevant actors contributing to the assessment, and the names and siagnatures of the individuals responsible for the assessment.

Framework

Privacy+ Security Forum

Consumer Experience

- What expectations is the average consumer likely to have regarding how the Business will process their data, based on the consumer's interaction with the product?
- What choices must be offered to the consumer under applicable law?

Proposed Business Use of Data

- How will data collected through the product be used? Does the proposed use comply with any restrictions under applicable law?
- Is the data being collected only what is reasonably necessary for the purposes of use? (must document)

Data Sharing

- What are the respective roles of the parties who send and receive data? Are compliant contracts in place?
- What Third Party Risk Management processes are in place?

Data Lifecycle Management

- What steps are taken to secure the data?
- What is the disposal policy to be applied to the data?
- How will purpose limitations be enforced?
- How will product data be integrated into business' protocol for responding to state privacy rights requests?

Questions?

Privacy+ Security Forum