Privacy and Security

Jason I. Epstein, Partner, Nelson Mullins

Roy Wyman, Partner, Nelson Mullins

Rob Rolfsen, Senior Director, Privacy Audit, and Compliance, Asurion

Topics

- The Current Sources of Privacy Guidance and Constraints
- Statutory Sources (+ see Ohio)
- Common Elements of Privacy and Security and Themes
- Evolution of State Laws
- Rise of the FTC
- Typical FTC Consent Order and Obligations
- Do you even know where you data is Napoleon? You don’t *even* know.
- How to Start and Benefits.
- Asurion Use Case.

Privacy

- Privacy and Security: know the difference
- The Current Sources of Privacy Guidance and Constraints
  - Common Law
    - *Intrusion of Solitude*: physical or electronic intrusion into one's private quarters
    - *Public Disclosure of Private Facts*: the dissemination of truthful, private information that is objectionable
    - *False Light*: the publication of facts that place a person in a false light, even if not defamatory
    - *Appropriation*: the unauthorized use of a person's name or likeness

Privacy and Security—Statutory Sources

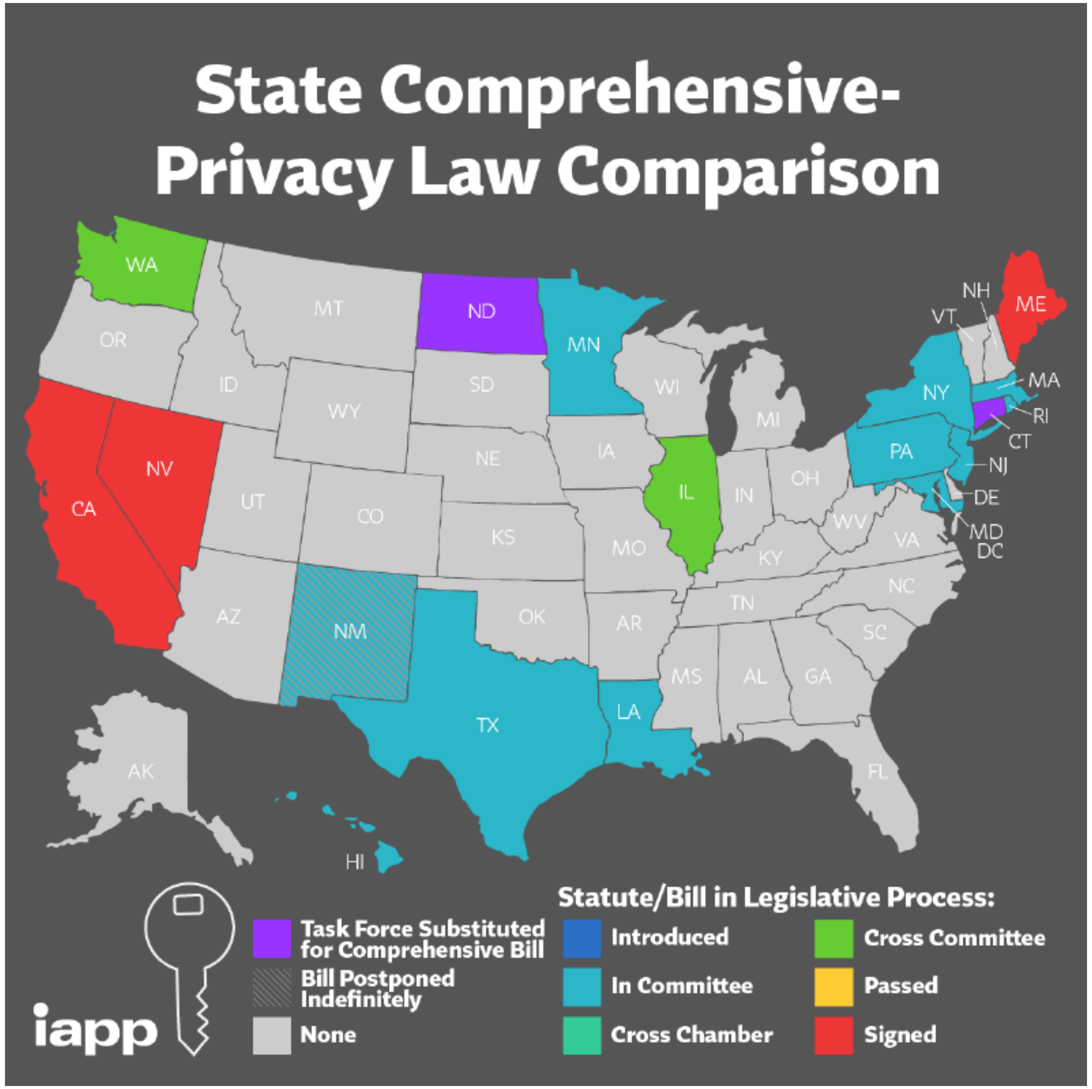
- Based on Type of Data/Industry
  - HIPAA
  - GLBA
  - SEC/FTC
  - PCI/DSS
  - GINA/Biometrics
  - NYDFS
- General Rights
  - GDPR/PIPEDA/Other International Law
  - California Consumer Privacy Act
  - Security: Massachusetts/California/Others

Privacy and Security—Some Common Elements

- In U.S.: Industry-Specific or By State
  - Definitions of Information Protected (PII; PHI; Financial; etc.)
  - Limits on Uses and Disclosures
  - Particular Rights of Individuals (Access; Amendment; etc.)
  - Notice of Policies/Rights
  - Security by Design
  - Privacy and/or Security Officer
  - Fines/Penalties
- Outside the U.S. (and Coming Soon to a State Near You!)
  - Consent
  - Right to be Forgotten/Delete Information
  - No Sale of Information without Consent
  - Private Right of Action

Upcoming States

- Hawaii
- Illinois
- Louisiana (Privacy Right of Action)
- Maryland
- Massachusetts (CA-like + Private Right of Action)
- Minnesota
- New Jersey
- New York
  - Comprehensive Rights
  - Fiduciary Duty
  - Private Right of Action
- Pennsylvania
- Rhode Island
- Texas
- Washington



Privacy and Security—The Rise of the FTC

- FTC has recently asked for more funding. It currently has around 40 lawyers.
- Consent Orders (Settlements):
  - Typically are for 20 years.
  - New: Addition that a senior officer must certify compliance.
  - New: Defendant must cooperate with 3rd party assessor and prohibition of making misrepresentations related to document preservation.
  - +More prescriptive requirements
- *But See*: LabMD v. FTC, where 11th Cir. Overturn consent order because it did not provide guidance on would be *sufficient* for guidance.

Privacy and Security—The Rise of the FTC

- The major FTC 2019 cybersecurity settlements: Unixiz, ClixSense, LightYear, Equifax, and D-Link.
- Equifax was the main event: $700M settlement and over 147M people affected.
- These Consent Orders provide much more prescriptive compliance, they do not state what would be *sufficient*.
- Facts of the cybersecurity cases.

The Anatomy of a FTC Consent Order

Typical Provisions include:

- Mandated Information Security Program
- Requirement of Information Security Assessments by a Third Party
- Requirements for Cooperation with Third Party Information Security Assessor
- Annual Certification of Compliance by Senior Corporate Manager
- Reporting of Covered Incidents
- For 20 years, deliver a copy of the Consent Order to all affected parties, including officers, applicable employees, and any successor companies.
- Requirement of Recordkeeping
- Compliance Reports and Notices
- Requirements around provision of additional compliance reports requested by Commission.

Do You Know Where Your Data Is?

- Supply chain ecosystems increasing in complexity
  - To deliver new services and leverage new technologies, developers regularly add new tools and vendors
  - These tools and vendors frequently require data access
- At the same time, data privacy requirements and consumer interest in their privacy are increasing; consumers want to know where their data is and who has access

Where to Start?

- Understand data lifecycle and data flows:
  - Common taxonomy
  - Vendor Inventory (and POCs)
  - Product Inventory
  - Data Maps
  - Data Use Cases
  - Data Governance
- When id’ing vendors, consider everything from communication providers to cloud solutions to logging and analytics tools
- 3rd party agreements should include appropriate controls for data privacy to include:
  - Audit Rights
  - Breach Notification
  - DSARs
  - Encryption
  - Data Sharing
  - Retention, etc.

How to Start

- Partner with:
  - Application Development Teams
  - Chief Data Officer
  - IT/Back Office Teams
  - Procurement
  - Product Development Teams
- Develop Record of Processing to document findings
- Integrate into Privacy by Design program
- Changes frequently, so update regularly – automate process
- Develop Privacy Champions Program to embed data privacy

Record of Processing Benefits

- Defines Applications/Vendors in Scope
- Component of Data Maps
- Vendor Inventory
- Application Inventory/POCs
- Retention Compliance
- Security Compliance
- ID’s Remediation

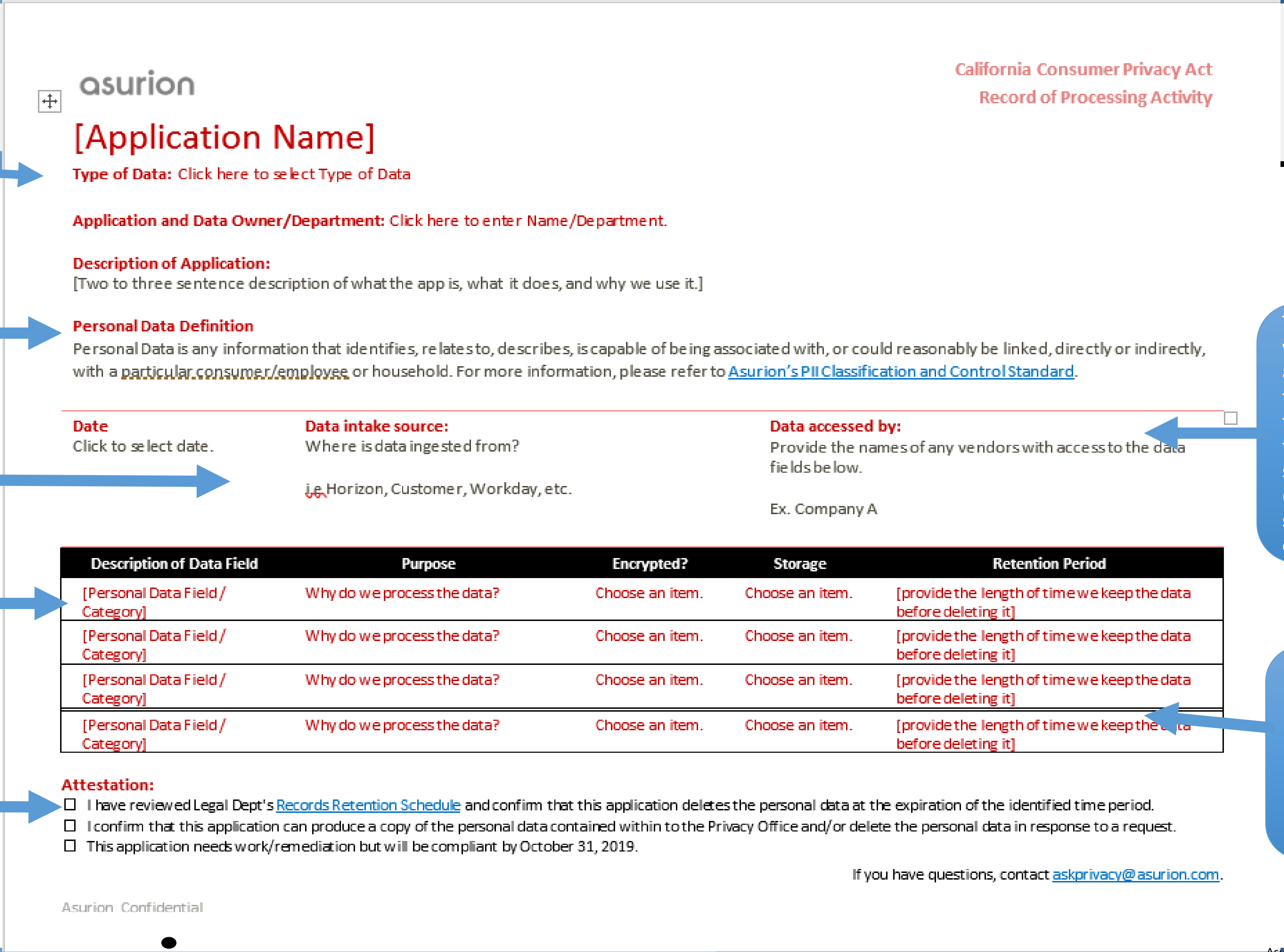
Employee and/or Customer

This information is provided for your reference when determining what personal data fields are being processed.

If there is more than one source, please list all.

You may group personal data fields on a single row if the purpose, encryption, storage, and retention period are the same.

This is an attestation of CCPA compliance. If you have additional work to do, please check box 3.
Box 1 = Compliance with retention period
Box 2 = Compliance with Individual Rights



asurion

California Consumer Privacy Act
Record of Processing Activity

[Application Name]

Type of Data: Click here to select Type of Data

Application and Data Owner/Department: Click here to enter Name/Department.

Description of Application:
[Two to three sentence description of what the app is, what it does, and why we use it.]

Personal Data Definition
Personal Data is any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer/employee or household. For more information, please refer to Asurion's PII Classification and Control Standard.

Date	Data intake source:	Data accessed by:
Click to select date.	Where is data ingested from? i.e Horizon, Customer, Workday, etc.	Provide the names of any vendors with access to the data fields below. Ex. Company A

Description of Data Field	Purpose	Encrypted?	Storage	Retention Period
[Personal Data Field / Category]	Why do we process the data?	Choose an item.	Choose an item.	[provide the length of time we keep the data before deleting it]
[Personal Data Field / Category]	Why do we process the data?	Choose an item.	Choose an item.	[provide the length of time we keep the data before deleting it]
[Personal Data Field / Category]	Why do we process the data?	Choose an item.	Choose an item.	[provide the length of time we keep the data before deleting it]
[Personal Data Field / Category]	Why do we process the data?	Choose an item.	Choose an item.	[provide the length of time we keep the data before deleting it]

Attestation:

☐ I have reviewed Legal Dept's Records Retention Schedule and confirm that this application deletes the personal data at the expiration of the identified time period.

☐ I confirm that this application can produce a copy of the personal data contained within to the Privacy Office and/or delete the personal data in response to a request.

☐ This application needs work/remediation but will be compliant by October 31, 2019.

If you have questions, contact askprivacy@asurion.com.

Asurion Confidential

This field can include vendors with direct access via API or any transfers; contractors that have access to the data; or any support access (screen sharing, support sessions, etc.) from vendors.

Please indicate the current time period the data Is kept before being deleted. If it is indefinite, please indicate that. i.e. 6 months, 12 months, 7 years, etc.

Questions