113 Days Countdown – Will You Be Ready to Comply with the California Consumer Privacy Act of 2018
and How it Compares to HIPAA and EU’s GDPR (2 CPE)

IIA San Diego Chapter Breakfast Meeting
Tuesday, September 10 | 8–10 am
Donnelley Financial Solutions
4350 La Jolla Village Drive, Ste 250, San Diego, CA 92122

Michael H. Cox, CIPP/US
President and Founder
Chief Privacy Consultant
Neil R. Packard, CISA
Chief Security Consultant
CPE Guidelines

- This training is CPE worthy, thank you for attending.

- In order to receive CPE credits
  - Sign-in with signature and time
  - Attend for entire session
  - Participate in exercises and activities
  - Complete and turn in the blue CPE form with required information
Bios of Principals

Michael Cox, CIPP/US

- President/Founder, Chief Privacy Consultant, SoCal Privacy Consultants
- Previous experience
  - Part-time Chief Privacy Officer, Pathway Genomics Corp.
  - VP of Enterprise Risk Management, Goal Financial
  - Business Risk Officer, Capital One Auto Finance
  - VP of Operations – multiple organizations, including 2 Fortune 200 companies
- Certified Information Privacy Professional (CIPP/US)
- Member of:
  - International Association of Privacy Professionals (IAPP)
  - IAPP Professional Privacy Faculty
  - Lares Institute, privacy think-tank
- Co-author, Security chapter for HIMSS Good Informatics Practices (GIP)
- Frequent speaker on privacy and security subjects
- B.S., Business Administration, Virginia Tech

Neil R Packard, CISA

- Chief Security Consultant, SoCal Privacy Consultants
- Previous experience
  - Deputy Assistant Director, Federal Trade Commission
  - IT Specialist (Security), Office of Inspector General, Department of Veteran Affairs
  - Founder, e-Diligent, Inc. (e-discovery & forensics)
  - Director of Information Technology, Seltzer Caplan McMahon Vitek
- Certified Information Security Auditor (CISA)
- Studying: Certified Information Privacy Professional - Europe (CIPP/E) exam
- Member of:
  - International Association of Privacy Professionals (IAPP)
  - Information Systems Audit and Control Association (ISACA)
  - InfraGard
- Business Administration, University of La Verne

About Us: SoCal Privacy Consultants

Educate – Assess – Operationalize - Transform
Lean, sustainable and defensible privacy and security programs

- Private / public customer-centric organizations in health care, Internet, technology services, financial services, etc.
- Conducts gap and risk assessments; and establishes programs for partners, service providers, and M&A buyers/sellers
- For an FTC consent order client, established multi-state information security programs and help pass four consecutive satisfactory biennial audits certifying compliance to the order
Scope

- Privacy Basics – Differences from Data Security
- FTC's $5B Facebook settlement sets new privacy governance precedents
- CCPA Act & Amendment
- Moving Target: Rulemaking & CA Legislative Bills in Progress
- Exemptions & Limitations: GLBA, HIPAA
- Status: Federal & Other State Privacy Laws
- How Much of GDPR Can Be Leveraged?
- How Is Reasonable Security Achieved?
- CCPA Action Plan with Practical Guidance
Learning Objectives

1. Describe how privacy & security are different
2. Understand implications of FTC's $5B Facebook settlement
3. Recognize who must comply with CCPA
4. Learn how Personal Information is defined under CCPA
5. Know the new consumer rights that businesses must honor
Learning Objectives

6. Know statutory penalties & scope of the private right of action

7. Recognize how GDPR compliance can be leveraged & what is different

8. Describe requirements to comply before Jan. 1, 2020 (effective date)

9. Know GLBA & HIPAA exemptions & limitations

10. Understand federal & state privacy landscape & how to be prepared for changes
Privacy Basics
## Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DSARs</strong></td>
<td><strong>Data Subject Access Requests</strong> (GDPR term)</td>
</tr>
<tr>
<td><strong>DPLC</strong></td>
<td><strong>Data Privacy Lifecycle</strong> – notice, collection, purpose, access, use, use, sharing, &amp; retention / disposal</td>
</tr>
<tr>
<td><strong>Data Mapping</strong></td>
<td>Mapping DPLC <strong>data flow, data inventory &amp; data locations</strong> (resources)</td>
</tr>
<tr>
<td><strong>SIPOC</strong></td>
<td><strong>Six Sigma tool</strong> used to get a process under control to avoid unintended consequences, e.g. adverse customer impacts - <strong>modified</strong> to identify data resources/locations – where data flows from (“inputs”) and to (“outputs”) during the DPLC (“process steps”) – and only capture process steps where personal data is involved (<strong>used during my ERM experience</strong>)</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td><strong>Products/services, processes, software/apps, databases, technologies, systems &amp; external resources</strong> (service providers/3rd parties) <strong>containing/involving PI</strong></td>
</tr>
<tr>
<td><strong>PbD / PIAs</strong></td>
<td><strong>Privacy-by-Design / Privacy Impact Assessments</strong> (DPIA or Data Protection Impact Assessment)</td>
</tr>
<tr>
<td><strong>Privacy-by-Default</strong></td>
<td><strong>Strictest privacy settings automatically apply</strong> once a customer acquires a new product / service</td>
</tr>
</tbody>
</table>
QUESTION: What is the purpose of brakes on a car?

not to slow a car down ...

but to allow it to go fast!
# Differences: Privacy vs. Security

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consumer focused</strong></td>
<td><strong>Data focused</strong>, includes Bus. Confid.</td>
</tr>
<tr>
<td>Consumer <strong>rights &amp; choices</strong></td>
<td><strong>Data protection</strong></td>
</tr>
<tr>
<td><strong>Notice / transparency (informed)</strong></td>
<td>IP, network &amp; asset protection</td>
</tr>
<tr>
<td>Legitimate purpose / consent for collection, use, access, sharing &amp; retention (DPLC management)</td>
<td>Confidentiality, integrity &amp; availability</td>
</tr>
<tr>
<td>▪ Authorized access governance</td>
<td>▪ Unauthorized access</td>
</tr>
<tr>
<td><strong>Laws, context, social norms/reasonable consumer expectations, principles &amp; risk oriented</strong></td>
<td><strong>Standards &amp; controls</strong> oriented</td>
</tr>
<tr>
<td>Includes security</td>
<td>Does not include privacy</td>
</tr>
<tr>
<td>Accountability / governance / trust</td>
<td>Often not included in standards</td>
</tr>
</tbody>
</table>
What does this tell you about the nature of the difference between privacy and security?
What Does This Tell You about the *Different Nature* of Privacy & Security?

- **Security** standards generally strengthen over time due to new technologies & trying to stay ahead of threats.

- **Privacy** as a concept is *ever evolving* due to new technologies, new contexts, new social norms, etc.
  - What may be *creepy in one context* may *not be creepy in another context*.
  - What is *acceptable changes over time*.
Facebook Settlement Raises Bar for Everyone

- Imposes unprecedented **structural safeguards** into corporate activities & fundamentally changes how Facebook appoints Board members & assigns duties
  - Required to **form Independent Privacy Committee** of solely independent members of Board of Directors meeting certain baseline knowledge/experience requirements
    - Committee tasked with **supervising privacy program & compliance** with the Order
  - Required to **create Independent Nominating Committee** with sole authority to recommend appointment of candidates to Board & put Directors on or remove them from Independent Privacy Committee
- Zuckerberg (or successor) & compliance executive must **quarterly & annually sign off on compliance reports**, exposing them to possible **personal liability**
- Required to report any unauthorized sharing of user data of 500 or more people to FTC within 30 days of discovery.
- **FTC**: The “*price of privacy violations just went up ... companies should consider whether to elevate privacy concerns to the board level or at least upper level management.*”

Facebook Settlement Raises Bar for Everyone

- Must **implement comprehensive & detailed privacy** program **overseen by compliance officers** - only removed by independent privacy committee

- Must **assess & document internal & external risks** to privacy & security, including via use of privacy impact assessments (**PIAs**) for any new/modified products where it presents a “material risk” to privacy
  - Similar to GDPR’s DPIA concept - EU data protection regulations continue to influence U.S.

- Other key takeaways -
  - **Do not misrepresent PI collected, its purposes & what is shared with 3rd parties**
  - **Do not use PI for undisclosed or unexpected purposes without consent, e.g. phone#**
  - **Facial recognition technology requires conspicuous notice & affirmative consent**
    - Facial recognition software can be created for as little as $100
  - **Keep records of data processing operations**

Sources:
https://www.lexology.com/library/detail.aspx?g=1cd67415-42f6-4b39-b73e-05c48c6249ca
https://www.jdsupra.com/legalnews/the-ftc-facebook-settlement-signals-68194/
Privacy Fundamentals

- Companies **underestimate the risk** - focusing on breach likelihood
  - **More than a compliance risk:** financial, regulatory, legal, operational-disruption & brand/reputation risks
    - Check-the-box compliance is not defensible

- Breaches are **inevitable** despite reasonable efforts
  - **Class action risk is rising – CCPA statutory damages risk is new**
    - CCPA will be “new oil for plaintiff attorneys”
  - Recent **FTC** settlement: "As we continue to pursue violations of law, we should prioritize uncovering the role of corporate officers and directors and hold accountable everyone who broke the law."
  - **State Attorneys General** now more active enforcers & have gained up

- Today’s **social media publicly hammers** companies for **poor data privacy & security practices**

- Requires **defensible & sustainable program** of policies/SOPs, governance & embedded practices
Privacy Fundamentals

- Regulators **ratcheting-up business accountability** for external party management

- Business development **due diligence “deal risk” is also increasing**
  - Organizations higher up Fortune 500 ladder or having suffered a breach want to avoid adverse consequences of selecting wrong business partner

- **SEC cybersecurity requirements** for public companies that may be your clients & if you decide to go IPO

- Must be **prepared to properly respond** to:
  - Partner due diligence
  - Breaches
  - Ensuing regulatory investigations & lawsuits

- Why not turn this into a **source of competitive advantage**?
  - **Part of Trust equation** - Privacy-by-Design is a functional requirement of products, processes, etc.
California Consumer Privacy Act of 2018, Amendments & Rulemaking (CCPA)
Background: CCPA & GDPR

- **GDPR** – comprehensive & very complex/specific
  - Negotiated over 4 years
  - Published 2 years in advance

- **CCPA** – *not comprehensive* & lacks some clarity
  - Negotiated virtually overnight to *avoid ballot initiative*
  - Published 1.5 years in advance of enforcement
  - Already amended once
    - Other amendment bills are in progress
CCPA Effective & Enforcement Dates

- **Effective Jan. 1, 2020** re: private rights of action
  - Effective July 1, 2020 re: regulatory enforcement (per Amendment)

- **Extra-territorial reach** – protecting CA consumers
CCPA Applicability & Impact

As 5th largest economy, CA will influence global privacy practices

- Applicable to “for profit businesses” (data controllers) -
  - Greater than $25M in gross annual revenue,
  - Annually handle PI of 50,000+ consumers or households, or
  - Derive 50% or more of annual revenue from “sales” of PI (no min. rev.)

- Will apply to many SMBs (IAPP estimates):
  - 500,000+ U.S. & 135,000+ CA businesses

- Website would only need 137 unique visitors per day from CA to reach threshold of 50K consumers
  - Collecting data via cookies is within broad definition of PI
Question...

- What are some ways an organization could trigger an average of **137 unique CA residents’ PI collected daily** to come under CCPA?

- What examples can you think of where businesses may derive **50% of revenue** from sharing PI with a 3rd party?
Answers

What are some ways an organization could trigger an average of 137 unique CA residents’ PI collected daily to come under CaCPA?

- Unique website visitors tracked by Google Analytics cookies
- Unique payment card purchasing & shipping information

What examples can you think of where businesses may derive 50% of revenue from sharing PI with a 3rd party?

- Interest based ads
Who Is Protected?

- **Consumers** – natural persons who are residents of CA (customer business relationship not necessary) including:
  - Employees & independent contractors (“employee data”)
  - Visitors to company premises, tenants, students, parents, children, etc.
  - BTB contact Individuals

- Thus, any organization processing data from CA consumers is in scope, including employers
  - Regardless of whether firm is physically located in CA

- Important to data map all of these data privacy lifecycles (DPLCs) – data flows and data & resource inventories
## CCPA: Accountability Model for Privacy

*Can outsource functions & activities, but not responsibility!*

<table>
<thead>
<tr>
<th>Party</th>
<th>Role</th>
<th>Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consumer</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Individual – state laws</td>
<td></td>
<td>Has data rights</td>
</tr>
<tr>
<td>- Patient - HIPAA</td>
<td></td>
<td>Exercise rights (control)</td>
</tr>
<tr>
<td>- Data subject – EU</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business</strong></td>
<td>Trusted organization</td>
<td>Defines data collected &amp; <strong>purposes &amp; means of processing</strong> - responsible thru-out delivery chain</td>
</tr>
<tr>
<td>- for profit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Covered entity - HIPAA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Data controller – EU</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Service provider</strong></td>
<td>Subcontractor</td>
<td>Processes <strong>strictly on behalf of data controller pursuant to certain contractual limitations</strong> - responsible for own security practices &amp; supports rights fulfilment - has direct liability</td>
</tr>
<tr>
<td>- Bus. associate - HIPAA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Data processor – EU</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3rd parties</strong></td>
<td>Advertisers, data brokers</td>
<td>Any other person/entity receiving PI from &amp; under control of business or service provider - when <strong>valuable consideration</strong> is involved, must offer an opt-out from “sale”</td>
</tr>
<tr>
<td>- New responsible party</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**External resources** = service providers & 3rd parties
Question...

Given a third party has a distinct meaning under CCPA different than we have used this term in the past, how will you refer to the combination of services providers and third parties in your organization?
CCPA Exemptions
General applicability, independent of industry sector with certain exceptions

- **Non-profits**

- **Federal privacy laws**
  - **HIPAA/CMIA** cov. entities (CEs)/bus. assoc. (BAs)
    - CEs (not BAs) can be exempted if voluntarily maintain non-regulated data in same manner as regulated data, e.g. PHI
  - **Federal “Common Rule” clinical trials** following certain good clinical practice guidelines
    - *Excludes research for commercial purposes*
  - **GLBA** entities
    - But are subject to CCPA requirements when engage in activities outside of GLBA
  - **FCRA & DPPA**
Basic Consumer Rights

Requires a process similar to GDPR’s Data Subject Access Request (DSAR)

- **Right to know** – requirements for:
  - Privacy notice & just-in-time *abbreviated disclosures*
  - Right to request *more specific disclosures of PI collected*
  - Right to request *more specific disclosures if PI sold or disclosed*

- **Right to (request) deletion**

- **Right to opt-out of “sale”** & for children to opt-in

- **Right of access & data portability** with “verifiable” request

- **Right to equal service & price** - *anti-discrimination* for exercising consumer rights

Requires **new data tracking, disclosure & management practices**
Corresponding Business Obligations

- Respond to *abbreviated disclosure requests in notice*
- Respond to *more specific disclosure requests*
- Respond to *requests for information from business that sell/disclose PI*
- Respond to *opt-outs of sale of data*
- Obtain *opt-in consent for sale of data of minors*
- Respond to *deletion requests*
- Respond to *requests for data access & portability*
- *Not to discriminate* vs. consumers exercising their CCPA rights
Key Rights Issues

- **“Sale” of PI:**
  - Releasing, disclosing, disseminating, making available or transferring PI **for monetary or other valuable consideration**
  - Requires disclosure & opt-out
  - Impacts some data-monetization business models

- **Operationalizing rights response**, e.g. disclosure & deletion
  - Identifying all PI data types, including that shared with 3rd parties
  - Requires effective data mapping, e.g. data & resource inventories
  - Requires internal data tracking system *(Salesforce can facilitate this)*
  - Creating designated methods for consumers to assert their rights
# Incredibly Broad Definition of PI

11 categories of PI to extent identify, relate to, describe, are capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer or household

<table>
<thead>
<tr>
<th><strong>Identifiers</strong></th>
<th>real name/alias, postal/email address, phone#, IP address, account name/#, SSN, driver’s license#, passport#, signature, insurance policy#, or other similar identifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commercial information</strong></td>
<td>records of personal property &amp; products/services purchased, obtained or considered, or other purchasing &amp; consuming histories &amp; tendencies</td>
</tr>
<tr>
<td><strong>Biometric identifiers</strong></td>
<td>DNA, biological/behavioral data, sleep, health &amp; exercise data (gait)</td>
</tr>
<tr>
<td><strong>Characteristics of a protected class under CA or Federal law</strong></td>
<td>race, national original, ancestry, marital status, sex, gender (sexual orientation), age, religion, physical or mental disability or other medical condition</td>
</tr>
<tr>
<td><strong>Internet or other electronic activity information</strong></td>
<td>browsing &amp; search history, &amp; info re: a consumer’s interactions with a website, application or advertisement</td>
</tr>
</tbody>
</table>

Also: gov’t public records including PI; records containing PI under FERPA (student privacy)
### Incredibly Broad Definition of PI

11 categories of PI to extent identify, relate to, describe, are capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer or household

<table>
<thead>
<tr>
<th><strong>Unique persistent identifiers</strong> that recognize a consumer or family over time &amp; across different services</th>
<th><strong>device identifier</strong>: IP address; <strong>cookies</strong>, beacons, pixel tags, mobile ad identifiers &amp; similar technology, customer#, unique pseudonym or user alias; other forms of persistent or <strong>probabilistic identifiers</strong> used to identify a particular consumer or device</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Geolocation data</strong></td>
<td>precise geolocation can be highly sensitive data</td>
</tr>
<tr>
<td><strong>Audio, electronic, visual, thermal, olfactory or similar information</strong></td>
<td>voice recordings, transcriptions, keystrokes, etc.</td>
</tr>
<tr>
<td><strong>Professional or employment-related information</strong></td>
<td>job applicants, benefits, compensation, performance reviews, education/resume (amendment may nullify this with one-year sunset)</td>
</tr>
<tr>
<td><strong>Inferences drawn</strong></td>
<td><strong>creating a profile</strong> reflecting preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities &amp; attitudes</td>
</tr>
</tbody>
</table>

Also: gov’t public records including PI; records containing PI under FERPA (student privacy)
Can you have PI without a name of a consumer? If so, what are examples?

What newly defined Personal Information might your organization currently collect that might be within CCPA’s scope?
Can you have PI without a name of a consumer? If so, what are examples?

- Trick question; *are many types of PI* in addition to name
- PI can also be: (to a particular consumer or household)
  - *Identifies, relates to or describes*
  - *Capable of being associated with*
  - *Directly/indirectly linkable*
- There can also be highly sensitive PI without name
  - E.g., *user ID/email address* + password
<table>
<thead>
<tr>
<th>WHAT MUST BE DISCLOSED</th>
<th>WHO MUST DISCLOSE</th>
<th>WHERE TO DISCLOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Collector of personal information</td>
<td>Seller of personal information</td>
</tr>
<tr>
<td>Categories of personal information collected about the consumer</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Categories of the sources from which the personal information was collected</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Business or commercial purpose for collecting or selling personal information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Categories of third parties with whom the business shares personal information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Specific pieces of personal information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Categories of personal information sold</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Categories of third parties to whom personal information was sold, by category or categories of personal information sold for each third party to whom personal information was sold</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Categories of personal information disclosed for a business purpose</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>A list of the categories of personal information sold about consumers in the preceding 12 months or, if no sale occurred, that fact</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>A list of categories of personal information disclosed for a business purpose in the preceding 12 months or, if no disclosure occurred, that fact</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>WHAT MUST BE DISCLOSED</td>
<td>WHO MUST DISCLOSE</td>
<td>WHERE TO DISCLOSE</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Collector of personal information</td>
<td>Seller of personal information</td>
</tr>
<tr>
<td>Consumers’ rights</td>
<td>To request access to their personal information, along with one or more designated methods for submitting such requests</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>To request deletion of their personal information</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>To opt out of the sale of their business information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not to be discriminated against for exercising any of their other CaCPA rights</td>
<td>X</td>
</tr>
<tr>
<td>Financial incentives programs</td>
<td>Notice of any financial incentives pursuant to Section 1798.125(b)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clear description of material terms of any financial incentive program</td>
<td>X</td>
</tr>
</tbody>
</table>

*See discussion of: Section 1798.110(c)*
Other State Laws also Define PI

EU’s GDPR defines **Personal Data** even more broadly

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> <strong>Persistent identifiers</strong></td>
<td>customer # held in cookie, IP address, a processor/device serial #, or unique identifier – when used for (re-targeting and behavioral) advertising – does not apply if used only for limited internal operations support - <strong>also cannot override</strong> browser privacy settings</td>
</tr>
<tr>
<td><strong>2.</strong> <strong>Medical / health Information</strong></td>
<td>conditions, treatments, therapies, prescriptions, drugs, medications, dosage, medical products/equipment used; prescribing physician name, address, &amp; contact info; health insurer’s name, insurance account#, or insurance policy#</td>
</tr>
<tr>
<td><strong>3.</strong> <strong>Geo-location information</strong></td>
<td>street name/town – does not have to be precise <strong>precise</strong> geolocation data is considered highly sensitive data</td>
</tr>
<tr>
<td><strong>4.</strong> <strong>Online logon information</strong></td>
<td>user ID/password, <strong>answers to common security questions</strong></td>
</tr>
<tr>
<td><strong>5.</strong> <strong>PII used for marketing purposes</strong></td>
<td>age, height, weight, race, religion, occupation, political party affiliation, children # of or gender, financial condition &amp; creditworthiness, kind of service provided, property &amp; products obtained (CA’s “Shine the Light “ Law § 1798)</td>
</tr>
<tr>
<td><strong>6.</strong> <strong>Security questions</strong></td>
<td>place of birth, <strong>DOB</strong>, mother’s maiden name, etc.</td>
</tr>
<tr>
<td><strong>7.</strong> <strong>PCI data</strong></td>
<td><strong>credit/debit/payment card information</strong> (PCI-DSS)</td>
</tr>
<tr>
<td><strong>8.</strong> <strong>Other</strong></td>
<td>personnel files; video / audio file</td>
</tr>
</tbody>
</table>
CCPA *Powerfully Boosts Class Action Risk*

When "nonencrypted and nonredacted" PI is "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the information”

Will address reasonable security near the end of this talk
Prepare Early to Mitigate Class Action Risk

Failure to undertake these efforts could lead to significant liability

- Place rigorous controls around highly sensitive consumer/employee PI
- Formalize/deploy end-to-end redaction & encryption everywhere to avoid having to notify (& safeguard PKI keys)
- Ensure policies/SOPs operationalize governance & practices adhering to an established framework, e.g. ISO 27001-2:2013
  - Integrate Top 20 Critical Security Controls into this framework
  - Document proof of compliance in a compliance repository
- Review/test your incident response plan
- Get the facts right in any data breach notification letter
- Obtain cyber-insurance & understand its limits & exclusions
  - Many cyber-insurance carriers authorize breach lawyer/breach vendors
  - For sub-servicers: due diligence; cyber-insurance; indemnification, etc.

https://www.lexology.com/library/detail.aspx?g=e4653681-84b2-4a78-9e45-6f22884a296f
Data Sensitivity Drives Risk-based Approach v.2

Determine strength of controls based on compilation of data sensitivity levels
Color-highlighted: CCPA & GDPR; CCPA alone; & GDPR alone (others include state breach laws)

<table>
<thead>
<tr>
<th>Quartile</th>
<th>4 Data Sensitivity Classifications</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><strong>Highly Sensitive</strong>&lt;br&gt;• harm: economic due to statutory data breach&lt;br&gt;• impacts: consumer &amp; business</td>
<td>1st name/initial &amp; last name (real/alias) plus any of following:&lt;br&gt;- gov’t issued ID # (SSN, passport ID#, state ID#, driver’s license#, tax ID#, birth/marriage certificate)&lt;br&gt;- health insurance ID#, genetic info (defined by GINA)&lt;br&gt;- medical/health info (medical history, physical/mental condition, test results/diagnosis, treatment/medications)&lt;br&gt;- criminal background check info&lt;br&gt;- certain biometric data/record or identifiers, e.g. iris/fingerprint, photo/video/audio file, etc.; digital signature&lt;br&gt;- precise geo-location data&lt;br&gt;- similar identifiers, e.g. instant message user ID&lt;br&gt;User name/D or email address with password or common security question answers (mother’s maiden name, DOB, place of birth)&lt;br&gt;Account name; financial acct # or payment card info+ any required security/access code or password; W-2</td>
</tr>
<tr>
<td>3-4</td>
<td><strong>Sensitive or Highly Sensitive</strong>&lt;br&gt;• harms: societal &amp; reputational often due to non-disclosure &amp;/or secondary uses&lt;br&gt;• impacts: business &amp; company</td>
<td>Invasion of privacy; e.g. re: private matters; surveillance/probing/profiling; discrimination; breach of confidentiality, improper disclosure, blackmail, etc. <a href="https://enterprivacy.com/wp-content/uploads/2018/09/A-Taxonomy-of-Privacy.pdf">https://enterprivacy.com/wp-content/uploads/2018/09/A-Taxonomy-of-Privacy.pdf</a>&lt;br&gt;Professional/employment data, e.g. job applicant, benefits, compensation, performance reviews, etc.&lt;br&gt;BTB contact information; racial/ethnic data; religion/political data; sex life/orientation&lt;br&gt;Purchasing &amp; consuming histories &amp; tendencies and browsing &amp; search history depending upon context</td>
</tr>
</tbody>
</table>
Data Sensitivity Drives Risk-based Approach v.2

Determine strength of controls based on compilation of data sensitivity levels
Color-highlighted: CCPA & GDPR; CCPA alone; & GDPR alone (others include state breach laws)

<table>
<thead>
<tr>
<th>Quartile</th>
<th>4 Data Sensitivity Classifications</th>
<th>Examples</th>
</tr>
</thead>
</table>
| 3        | Sensitive                          | Unique persistent or probabilistic identifiers, e.g. device/processor/serial ID, cookies/beacons/pixel tags, **IP address**, mobile ad identifiers & similar technology, customer#, unique pseudonym, vehicle ID/serial #  
Other personally identifiable dates, unique ID#/characteristic/code & non-precise geo-location data  
Profiling data (inferences drawn), e.g. preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities & attitudes |
| 2        | Slightly Sensitive                 | Published/public contact info: **name plus address, phone#, email address, fax#, URL address, any other PII used for marketing purposes** (see CA's “Shine the Light Law”) |
| 1        | Non-Sensitive                      | Non-personal information, such as **session** identifiers/cookies |
## Controls Effectiveness Scale

*The greater the risk, the stronger the controls should be*

<table>
<thead>
<tr>
<th>Scale</th>
<th>Controls Effectiveness</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>corrective, preventive &amp; detective</td>
<td>IDS/IPS with threat intelligence</td>
</tr>
<tr>
<td>3</td>
<td>preventive &amp; detective controls</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>preventive</td>
<td>privacy/security-by-design, policies/SOPs, training (awareness/on-the-job), keycards, authentication, RBAC system controls, encryption, hardening, firewalls/IPS/IDS, real-time log correlation/response, white/black-listing, code testing prior to release, DLP, database activity monitoring</td>
</tr>
<tr>
<td>1</td>
<td>detective</td>
<td>risk assessments, control evaluations, alerts, reports, periodic review of logs, file integrity monitoring, vulnerability scans, penetration testing, threat watch</td>
</tr>
<tr>
<td>0</td>
<td>inadequate</td>
<td></td>
</tr>
</tbody>
</table>

- Controls must be documented in a procedure, implemented, tested, monitored & trained on
- For lower risks, detective controls are adequate. Higher risks should have preventive & detective controls
Types of Controls
To manage cause-risk event-effect relationship

Corrective Controls automatically manage/mitigate in response to an alert, e.g., IPS

Preventive Controls are proactive controls established to stop or deter risk events/causes from occurring. Examples include:
- Procedures/process maps, Access Control Policy
- Segregation of Duties, e.g., dual control

Detective Controls are established to discover errors that have occurred and can be used to determine when/if a preventative control breaks down. Examples include:
- Alarms, e.g., email notification signaling error/out-of-pattern situation
- Reports, e.g., monitoring reports for validation/comparison purposes
- Sampling, e.g., quality assurance sampling
<table>
<thead>
<tr>
<th>Information</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate</td>
<td>information that relates to a group or category of consumers, from which individual consumer identities have been removed and is “not reasonably linkable” to a consumer or household</td>
</tr>
<tr>
<td>De-identified</td>
<td>information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer (eliminates “key-coded” data sets which are linkable)</td>
</tr>
</tbody>
</table>
CCPA: 4 Required Safeguards to Prevent Reidentification

1. **Implement technical safeguards prohibiting reidentification**
   a. Including the process or techniques by which data has been de-identified. May include some combination of hashing, salting, or tokenization.

2. **Implement business process specifically prohibiting reidentification**
   a. Might include an internal policy or procedure preventing employees or vendors from attempting to reidentify data.

3. **Implement business processes to prevent inadvertent release of deidentified information**
   a. Might include safeguards to help prevent de-identified information from being accessed or acquired by unauthorized parties.

4. **Make no attempt to reidentify the information**
   a. Requires business to follow policies enacted to prohibit reidentification.
How does this definition of de-identified differ with HIPAA’s?
Answer

How does this definition of de-identified differ with HIPAA’s?

- HIPAA only requires **18 PHI identifiers** be removed
- However, **if not under HIPAA, CCPA rules apply**
- Experts aren’t certain how this will play out for HIPAA covered entities seeking **exemption** by treating non-regulated data the same as PHI
  - **Might be wise to get advice of a qualified statistician**
Data Minimization via Privacy-by-Design

- **Anonymized**: low risk of identification due to *singling out, link-ability or inference*
  - EU/CaCPA: *irreversible* to prevent identification
    - Randomization & generalization

- **Not-PI**: *excluded from scope of CaCPA!*
  - **Aggregate data** – summarized group data with no identifiers
  - **De-identified** – remove direct/indirect identifiers & not re-identify

- **PI**: do not disclose as anonymous in notice/consent/marketing
  - **Pseudonymized** – replace identifiers with unique numbers or other value that does not allow direct identification
  - **Key-coded** with restricted access to key-code
  - **Limited data set with data use agreement**
  - **Minimum necessary**: collection; access; use; sharing; retention
Don’t Use Terms: **Anonymous or Anonymized**

*Recent study published in Nature Communications -*

- **99.98%** of Americans *re-identifiable* from any “anonymized” data set *using only 15 demographic attributes* (recent study)

- **83%** re-identifiable using only gender, DOB & ZIP code

- **Calls into question whether any data set can be truly anonymized**

Source: [https://www.jdsupra.com/legalnews/is-anonymized-data-truly-safe-from-re-55837/](https://www.jdsupra.com/legalnews/is-anonymized-data-truly-safe-from-re-55837/)
Definitions: Devil is in the Details

<table>
<thead>
<tr>
<th>Activity</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collection</strong></td>
<td><strong>buying, renting, gathering, obtaining, receiving, or accessing</strong> any personal information (PI) pertaining to a consumer by any means</td>
</tr>
<tr>
<td><strong>Sale</strong></td>
<td>selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s PI by business <strong>to another business or a 3rd party for monetary or other valuable consideration</strong> (almost always “contractual consideration”)</td>
</tr>
<tr>
<td><strong>Disclosure</strong></td>
<td>providing PI to another person for operational purposes, or other notified purposes, provided use of PI shall be reasonably necessary &amp; proportionate to achieve operational purpose for which PI was collected or processed or for another operational purpose compatible with context in which PI was collected</td>
</tr>
</tbody>
</table>

Releasing, disclosing, disseminating, making available or transferring PI for monetary or other valuable consideration is considered a “sale” under CaCPA, requiring disclosure & opt-out.
Question...

Show of hands – how many organizations are providing PI to 3rd parties for monetary/other valuable consideration?

Examples?
Data Mapping Is Critical for Data Discovery & Rights Management

- **Data map** & update immediately before Jan. 1, 2020 and annually thereafter (12 mo. lookback)
  - Identify what PI is collected/processed & where stored

- **Update privacy notices** based on data mapping

- **Establish governance** -
  - **DPLC owners** to maintain data map accuracy
  - **DSAR coordinator** to log, track & respond to DSARs
    - Also report metrics to privacy official & governance committee
  - **Resource/data custodians** to retrieve/delete/port PI
Other CCPA Internal Business Impacts

- Also data map & establish governance around these DPLCs, e.g. establish data owners, honor rights, etc.:

  - **BTB Contact Information** (CRM: marketing, sales & bus dev)
    - No distinction between PI held in **B2B** vs. B2C relationship
  - **Employee Data**
    - Employee privacy notices, handbooks & posters
    - Employee intranet/repository
      - Send link to employment applications/resumes vs. including in emails & calendar invites - *may have clean-up work to do*
    - No breach exception
Operationalizing Consumer Rights

- Provide **2 or more designated methods** for submitting requests including at a min. **toll-free PH# & Web address** (if have a website)

- **Verifying** requesting consumer **without undue hindrance**
  (will be tricky & subject to enforcement if get it wrong)

- Request be made **in writing** & info should be provided:
  - **Free of charge**
  - **In readily useable/portable format allowing data transfer** to another entity **without undue hindrance**
  - **Within 45 days** of request - can be extended once for an additional 45 days with notice to consumer
  - **Via customer’s existing account or by mail/electronically** at consumer’s option - cannot require account creation to make request
Operationalizing Consumer Rights

- Develop/implement internal **data tracking infrastructure** & rights operational processes
  - Identify all pieces of consumer PI to fulfill disclosure requests & for opt-ins/outs - record date, timestamp & authentication
- Requires training of staff -
  - Consumer-facing representatives re: inquiries about rights & privacy practices
  - DSAR coordinator logging/tracking/responding & reporting
  - Resource/data custodians retrieving/deleting/porting data
- Conduct table-top exercise re: each of the rights
Enforcement with Large Civil Penalties

- Exclusively enforced by **CA Attorney General**
  - If fail to cure within **30-day cure period** - face penalties:
    - Up to $2,500 for each violation per consumer, or
    - Up to $7,500 for each *intentional* violation
  - Also subject to an **injunction**
  - **20% of penalties** collected to fund enforcement

- To avoid statutory damages - provide *substantive evidence of compliance*
CA AG Has Rule-making Authority

- CCPA’s specific implementing rule-makings:
  - First: opt-out, notice, access/portability & exception provisions
  - Second: adding categories of PI to address changes in technology, data collection, obstacles to implementation & privacy concerns

- General authority to issue rules as necessary to further Act’s purposes
Right to Sue for *Large Civil Damages*

- Individuals can bring a *civil action*
  - *Greater of statutory damages of $100-$750 or actual damages* per consumer per incident
  - Applies only to “data breach” violations & not technical violations of Act as a whole
    - Definition of breached PI is narrower than CCPA’s PI definition
  - If consumer provided *30-day written notice* & business has not provided “express written statement” that violation is cured & “no further violations (will) occur”
    - *Can sue if business continues to violate* based on written statement
  - For actual (quantifiable) damages, no notice required
Private Right of Action’s PI Definition is much more limited than the broader CCPA definition

- Private right of action only applies to a breach of the following data elements:
  - 1st name/initial & last name in combination with (when either not encrypted/ redacted):
    - SSN; Driver's license # or CA ID card #
    - Financial account #; credit/debit card # (in combination with required security/access code or password)
    - Medical info; health insurance info
  - Username or email address in combination with password or security question & answer permitting access to online account
CA Amendment Bills *High-Level Update*

*deadlines: 9/10 bill sponsored; 9/13 vote into law; Gov. sign or veto*

- Appears dead or stalled at least for this legislative session
  - Expanding class actions to statutory violations
  - Deidentification – not “reasonably” linkable or capable of being associated with & removes “household” from definition

- Still alive, but not yet passed or signed into law
  - Employee data carveout, however:
    - Requires privacy notice & permits class actions
    - No DSARs - but one-year sunset when reinstated
  - Use of PI in loyalty programs with consent & voluntary participation
  - Allowing exclusively online DTC businesses to provide just one method for consumers to submit DSARs (email)

- Should prepare for full compliance
Imagine 50 Versions of CCPA!

- Expect additional amendments

- Ballot initiative’s sponsors pledged to **revive initiative if CCPA is watered down**
  - Appears new law’s core requirements & approach will stay intact

- Other states considering bills with material differences leading to a **patchwork**, akin to breach notification laws

- **Tech giants pushing for** **U.S. omnibus privacy law** preempts state laws
  - Consumer advocates want federal law to simply be a floor
  - Congress appears too dysfunctional to act
  - Not likely going to achieve EU’s “adequacy” standard
Privacy Bills in Progress

Imagine a patchwork of 50 states having data privacy laws

Modeled on CCPA

- **Hawaii** – no applicability thresholds
- **Maryland** – 100k user threshold
- **Massachusetts** – no employee data; $10M revenue & no user threshold
- **New Mexico**
- **Rhode Island** – $5M revenue threshold
- **Connecticut**
- **New York** – $50M revenue/100k users
- **Pennsylvania** – $10M revenue
- **Texas**

Varies more with CCPA

- **Illinois**
- **New Jersey**
- **New York**
- **Oregon**
- **Virginia** – minors’ rights
- **Louisiana**
- **Nevada**: signed 5/29, effective 10/1/19 – Sale Opt-out
- **Washington** (2 bills) – control/process 100K users or derive 50% of gross revenue from sales of PI & control/process 25K users – more complicated & GDPR-like - has serious traction & could get passed in next month or so; adjourned

Many other more limited or undeveloped bills in progress – one to note: **Arizona** (500 user data access & correction portal)

Sources

text links...
## Integrate CCPA into GAPP Privacy Principles

Requires data governance to enforce these principles

<table>
<thead>
<tr>
<th>No.</th>
<th>Principle Areas</th>
<th>Description</th>
<th>CCPA Sections</th>
<th>GDPR Articles</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Management</td>
<td>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</td>
<td>1798.100(b) 1798.110 (c)</td>
<td>5, 6, 14, 24, 27, 32, 36-39</td>
<td>14</td>
</tr>
<tr>
<td>2</td>
<td>Notice</td>
<td>The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.</td>
<td>1798.120 1798.120(d)</td>
<td>5,12-15, 21</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Choice &amp; Consent</td>
<td>The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.</td>
<td>1798.120 1798.120(d)</td>
<td>6, 7, 8</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>Collection</td>
<td>The entity collects personal information only for the purposes identified in the notice.</td>
<td>1798.100(b)</td>
<td>5, 6, 9, 21, 25, 35, 89</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>Use - Retention - Disposal</td>
<td>The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.</td>
<td>1798.100(b)</td>
<td>5, 6, 10, 22, 39</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>Access</td>
<td>The entity provides individuals with access to their personal information for review and update.</td>
<td>1798.100(a) 1798.110(a)(1)-(5)+ (b) 1798.130(a)(1)-(7)</td>
<td>7, 12, 14-18, 20-22, 26, 38</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>Third Party Disclosure</td>
<td>The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.</td>
<td>1798.140(v)+ (w) 1798.145(h)</td>
<td>28, 29, 32</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>Security for Privacy</td>
<td>The entity protects personal information against unauthorized access (both physical and logical).</td>
<td>1798.81.5(b) 1798.150(a)(1)</td>
<td>5,6,24,32,46</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>Quality</td>
<td>The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.</td>
<td></td>
<td>5, 16</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>Monitoring &amp; Enforcement</td>
<td>The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints and disputes.</td>
<td></td>
<td>17, 19, 20, 30, 33-35, 37,39, 47</td>
<td>7</td>
</tr>
</tbody>
</table>
CA AG’s Office re: Enforcement of CCPA

Companies cannot be complacent in their efforts

- Comments by Eleanor Blume, Special Assistant to CA AG’s Office, on Dec. 4, 2018:
  - Start now - will evaluate steps companies have taken to comply before CCPA’s effective date which reflects on how seriously they view their obligations
  - When mapping data and establishing compliance mechanisms, document any overly burdensome technical barrier not allowing for perfect compliance
    - Defenses relying on the technical burden or infeasibility of CCPA compliance will need to be specific & significant
    - Be prepared to demonstrate compliance by & through their policies, procedures & incident response plans, etc.

- CA AG’s 2/25/2019 press release:
  - “Effective January 1, 2020, businesses must comply with the CCPA’s key requirements
Apply CCPA with CA Residents only?

- **Consider alternative business models & web/mobile presences**, including
  - CA-only sites & offerings & charges for formerly free services to address complex & seemingly self-contradictory restrictions on company's ability to impose service charges on CA residents who object to alternate forms of data monetization

- However, also consider:
  - **Impact on customer relations** of differentiating service to residents of CA & other states
  - **Legal implications of voluntarily representing & applying CA law across other states**
    - Keep in mind that other states following CA’s lead may impose differing privacy laws
Comparing CCPA to EU’s GDPR
And HIPAA & GLBA Impacts
Commonalities: CCPA & GDPR

- Applies to businesses determining “purposes & means of processing” & covers many SMBs
- Protects residents & thus have extra-territorial reach
- Includes HR/employee data in scope
- Creates new consumer rights, e.g. right of access to PI
- Additional protections for individuals under 16 years of age
- De-identification definitions very similar & cannot re-identify
- Must track & document compliance, but in a very different manner
### Key Differences

**Compliance can be leveraged, but recognize differences**

<table>
<thead>
<tr>
<th>CaCPA</th>
<th>GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business applicability thresholds</td>
<td>Offering goods/services or profiling/monitoring</td>
</tr>
<tr>
<td>11 Categories of PI</td>
<td>Personal Data defined broadly</td>
</tr>
<tr>
<td>Informed privacy notice &amp; consumer rights oriented</td>
<td>Legitimate purpose analysis</td>
</tr>
<tr>
<td><strong>12 mo. look-back</strong> at data collected for disclosure requests</td>
<td>Privacy-by-Design/DPIA</td>
</tr>
<tr>
<td>Anti-discrimination</td>
<td>Demonstrable compliance proof</td>
</tr>
<tr>
<td>Service provider contractual obligations</td>
<td>Data retention</td>
</tr>
<tr>
<td></td>
<td>Explicit data processor contractual requirements</td>
</tr>
<tr>
<td></td>
<td>DPO, local legal representative</td>
</tr>
<tr>
<td></td>
<td><strong>X-border data transfer rules</strong>, e.g. PS</td>
</tr>
</tbody>
</table>

See Appendix for a deeper comparative analysis
## Rights Similar, But Must Account for Differences

<table>
<thead>
<tr>
<th>Privacy Rights</th>
<th>GDPR</th>
<th>CCPA</th>
<th>HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to <strong>Notice &amp; Choice</strong>: (provide notice &amp; inform of rights): <strong>CCPA – Notice/Disclosures; HIPAA - NOPP</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Right to <strong>Access</strong> (quality; correction / amendment)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Right to <strong>Notifying External Resources</strong> re: Corrections, Erasure or Restriction (opt-in/out)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Right to <strong>Data Portability</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Right to <strong>Object to Processing</strong>: direct marketing; scientific, historical or statistical purposes (opt-in/out)</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Right to <strong>Erasure</strong> (&quot;right to be forgotten&quot;): applies in limited cases but must erase without undue delay</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Right to <strong>Restrict Processing</strong> (opt-in/out of sale)</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Right to <strong>Not Be Evaluated via Automated Profiling</strong></td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Right to <strong>Complain</strong> (Right to Redress)</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Right to Restrictions, Restrict Disclosures &amp; Request Confidential Communications</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Right to Accounting of Disclosures</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Response timeframes, exceptions, & denial reasons are different
HIPAA Covered Entities: Qualifying for CCPA Exemption

- Treat Non-Regulated PI Same as PHI
  - CCPA provides no specific guidance

- Include CCPA’s PI definition scope in:
  - Privacy notices
  - Confidentiality agreements
  - Privacy & security policies/SOPs & practices, e.g. AUP
  - Training
  - Business associate agreements (protection flow down)
  - Watch for clarification via rule-making, etc.

- Lots of vagueness, for example re: deidentification rules
GLBA Entities & CCPA

- Apply CCPA to all PI not collected, process, sold or disclosed pursuant to GLBA, e.g.
  - Targeted online advertising
  - Tracking web page visitors
  - Collecting geolocation data
  - Etc.
Question...

Does a company with a direct-to-consumer health care mobile app that has voluntarily chosen to adhere to HIPAA standards also have to comply with CCPA?
Does a company with a **direct-to-consumer health care mobile app** that has *voluntarily chosen to adhere to HIPAA* standards also have to comply with CCPA?

- Pre-CCPA, many organization adhered to HIPAA standards for defensibility purposes,

- However, now these organizations are squarely within the scope of CCPA, if meet applicability threshold
Develop a sense of what a “reasonable” cybersecurity posture means
Program Elements

- **Sustainable** (NIST: repeatability)
  - Most clients have *ad-hoc or risk informed* practices
  - Goal: establish *repeatable* practices based on
    - *Demonstrated* executive commitment and support
    - Governance with clearly defined roles and responsibilities for oversight, execution and monitoring
    - Requires *organizational, cultural & operational changes*
    - Program *matures over time*, not a short-term project *(3-5 years)*

- **Defensibility**: build proactive *risk management & Privacy/Security-by-Design processes* on top of compliance
  - *Check-the box compliance is not enough*
“Reasonable” (& Defensible) Security

- Select a comprehensive set of standards
  - 96-99% of breaches avoidable by simple & intermediate controls (Verizon DBIRs)

- Identify what is reasonable under the circumstances & exceptions based on:
  - Company size, complexity & capabilities; industry, DTC/BTB; jurisdictions
  - Nature & sensitivity of PI
  - Technical, hardware & software infrastructure
  - Costs of security measures (vs. benefit)
  - Probability & impact of likely risks to PI
  - Insurance & client due diligence requirements (Fortune 500)
“Reasonable (Defensible) Security” Requirements

As federal & state laws require “reasonable security” (but generally no specific measures), it is critical to select a defensible standards-framework.

- CA State AG Office’s Feb. 2016 CA Data Breach Report:
  - “failure to implement all the Top 20 (Critical Security) Controls that apply ... constitutes a lack of reasonable security” and “define(s) a minimum level of information security ...”
    - Matches well with root causes of breaches, but is not a comprehensive framework

- Ohio: 1st state to pass cybersecurity safe harbor law inoculating businesses proving compliance to recognized security standards

- ISO 27001-2:2103 is well-accepted internationally standard
  - Recommend integrating Top 20 CSCs within the ISO framework

- IoT security standards are rapidly emerging
### Basic CIS Controls

1. Inventory & Control of Hardware Assets
2. Inventory & Control of Software Assets
3. Continuous Vulnerability Assessment & Remediation
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware & Software on Mobile Device, Laptops, Workstations & Servers
6. Maintenance, Monitoring & Analysis of Audit Logs

### Foundational CIS Controls

7. Email & Web Browser Protections
8. Malware Defense
9. Limitation & Control of Network Ports, Protocols & Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers & Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on Need to Know
15. Wireless Access Control
16. Account Monitoring & Control

### Organizational CIS Controls

17. Implement a Security Awareness & Training Program
18. Application Software Security
19. Incident Response & Management
20. Penetration Tests & Red Team Exercises

Now includes **implementation group tiers:**

1. SMB w/ limited IT/cybersecurity resources (crawl/walk - 43 sub-controls);
2. Moderate SMB with individuals responsible for managing/protecting IT infrastructure w/ regulatory compliance burdens (run - 139);
3. Larger mature organizations employing multiple cybersecurity experts (171).

[https://www.cisecurity.org/controls/](https://www.cisecurity.org/controls/)
NY’s SHIELD Act Defines Reasonable Security effective 3/2020

- **Administrative Controls** (NY General Business Law § 899-aa & State Technology Law § 208)
  1. designates one or more employees to coordinate security program
  2. identifies reasonably foreseeable internal & external risks
  3. assesses sufficiency of safeguards in place to control identified risks
  4. trains & manages employees in security program practices & procedures
  5. selects service providers capable of maintaining appropriate safeguards, & requires those safeguards by contract
  6. adjusts security program in light of business changes or new circumstances

- **Technical safeguards**
  1. assesses risks in network & software design
  2. assesses risks in information processing, transmission & storage
  3. detects, prevents & responds to attacks or system failures
  4. regularly tests & monitors effectiveness of key controls, systems & procedures

- **Physical Safeguards**
  1. assesses risks of information storage & disposal
  2. detects, prevents & responds to intrusions
  3. protects against unauthorized access to, or use of, private information during or after the collection, transportation & destruction or disposal of the information
  4. disposes of private information no longer needed for business purposes within reasonable amount of time, by erasing electronic media so information cannot be read or reconstructed

Private right of action for actual damages; AG fines for delayed notice
A small business with fewer than 50 employees, less than $3M in annual revenue in each of last 3 fiscal years, or less than $5M in year-end total assets will be deemed compliant if data security program is appropriate in light of size & complexity of business, nature & scope of its activities, & sensitivity of PI collected
“Reasonable” (& Defensible) Security

- Follow **AWS Shared Responsibility Model**
- Conduct **periodic controls evaluation** against standards/controls
  - Identify exceptions based on specific **compensating controls**
- Conduct **periodic risk assessment** with x-functional team
  - Identify material risks & corresponding mitigation plans
  - **Prioritize & track timely completion of mitigation plan**
- Use **encryption & redaction everywhere** – a breach “safe harbor”
- Use **data minimization practices**, e.g. data masking, de-identification, pseudonymization, minimum necessary, etc.
- Review/ **test your incident response plan**
- **Monitor critical activities**, e.g. patching
- **Document** all of this in a restricted repository
Cyber Insurance *Limited in Protections*

- No established standards, so policies vary widely

- Cyber insurance coverage **includes many exclusions & limitations**, *e.g.* caps
  - Attack traced to certain nation-states excluded as *“acts of war”*
  - Intentional acts, *e.g.* business email attacks, such as phishing
  - Fines & penalties

- A savvy broker or specialist cyber insurance lawyer should be able to explain exclusions & limitations and may recommend *additional coverage* if desired

- After a breach, many insureds & their insurance carriers have sued & countersued each other over coverage issues

- Also, **ensure compliance to any representations** made in any cyber insurance application and/or reps and warrants in the policies regarding things such as encryption, period risk assessments, timely patching, etc.
  - **Failure to adhere to these will likely void the policy**
  - *Ensure representations are defined as requirements in policies/procedures*
Roadmap to CCPA Compliance

GDPR Lessons Learned
Will You Be Ready?

- **Prepare for more robust due diligence** based on CCPA compliance requirements
  - Business partners
  - Service providers
  - Third parties
  - M&A deals

- **Creates competitive advantage & helps meet business goals**
  - Revenue goals via business development
  - Expense containment goals by mitigating liability (positive ROI)
Apply Lessons Learned from GDPR

- **Analyze** whether the CCPA applies to you

- **Prepare to comply** prior to Jan. 1, 2020
  - Understand *compliance will take longer than you believe*, e.g. tagging & tracking data elements, fulfilling data subject rights
  - Requires *organizational, cultural & operational changes*
  - Check-the-box compliance will fail

- **Strong sr. leadership support & cross-functional collaboration is critical**
  - Gain *commitment* for heavy use of enterprise-wide resources

- **Budget** appropriate funds **early**
High-Level CCPA Action Plan

- **Document data flows, resource & inventory mapping, and tracking infrastructure** with a 12-mo. lookback
  - Assign DPLC process owners & resource/data custodians
  - Identify “sales” of PI as defined by CCPA

- Establish **data-tracking-system** based data mapping

- Update **privacy notices annually** based on 12-mo. lookback
  - Provide clear/conspicuous “Do Not Sell My Personal Information” link
  - Direct DSARs to designated methods, e.g. web page, toll-free phone#, email, etc.
  - Record opt-in/out, date/time stamp & authentication and suppress as appropriate; avoid requesting opt-in consent for 12 months (address minors)
High-Level CCPA Action Plan

- Establish, standardize & test DSAR process with clear roles & responsibilities as described earlier
  - Define proportionate verification
  - Develop consumer communications playbook

- Start service provider & 3rd party inventory & management early
  - Update service provider agreements to avoid “sale” of PI to provide liability safe harbor

- Re-evaluate:
  - Deidentification rules
  - Potential discriminatory pricing & services
High-Level CCPA Action Plan

- Update privacy policies to comply with CCPA

- Train workforce members as described earlier

- Expect uncertainty until common understanding evolves
  - Leverage counsel & operational-oriented consultants & compliance tools to gain needed expertise, avoid re-inventing the wheel & save time
Don’t Wait –
There is less time than you think to become compliant
as anyone who has worked on GDPR compliance knows full well
IAPP Certifications
https://iapp.org/certify/programs/

- The “what” of privacy laws & regulations
  - CIPP/US
  - CIPP/E – EU (GDPR)
  - CIPP/C – Canada
  - CIPP/A - Asia

- The “how” of privacy operations
  - CIPM – Certified Information Privacy Manager

- The ‘how’ of privacy & technology
  - CIPT – Certified Information Privacy Technologist (PbD)
ANY FINAL QUESTIONS?

If you would like to have a copy of our *data mapping whitepaper*, please note which this on your business card and provide it to us or let us know – happy to share it, we do not follow-up unless asked.

Michael Cox, CIPP/US  
mcox@socalprivacy.com  
619.318.1263

Neil R Packard, CISA  
npackard@socalprivacy.com  
619.208.2529

www.socalprivacy.com

SoCal Privacy Consultants  
Operationalizing Privacy and Security Programs
Appendix

Supplemental Information

About Us
2019 Cost of Breach Study by the Ponemon Institute
2019 Cost of Breach Study by the Ponemon Institute

Ponemon targets breaches that do not exceed 100,000 records and thus excludes catastrophic mega breaches, e.g. Equifax & Facebook

<table>
<thead>
<tr>
<th>Avg. U.S. Data Breach Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
</tr>
<tr>
<td>$3.54M</td>
</tr>
</tbody>
</table>
Breach Impacts Can Be Severe
Avg. 2019 U.S. total data breach costs: $8.19M (32,434 records/Ponemon Inst.)

- **Operational resource disruption/distraction** risk
  - CEOs lost 1-1.5 yrs of productivity winning back stakeholder confidence (interviews)

- **Regulatory** risk

- **Legal** risk

- **Financial** risk: avg. U.S. breach cost *per compromised record*: $242
  - Healthcare: $408 / $13.85M (1.75Xs - highest of any industry for 8th straight year) – **WHY?**
  - Lost sales & business opportunities - 12-22% avg. loss in brand value

- **Brand/reputation** risk: *uninsurable* & can be catastrophic to SMBs

- **Officer & director liability** risk *on the rise*

*How many total consumer records do you have?*
Breach Cost Components & Examples

- Detection & escalation costs: 31.1% of global cost
  - Forensic and investigative activities
  - Assessment and audit services
  - Crisis team management
  - Communications to executive management & board of directors

- Notification costs: 5.4%
  - Emails, letters, outbound telephone calls, or general notice to data subjects that their personal information was lost or stolen
  - Communication with regulators; determination of all regulatory requirements, engagement of outside experts

- Post data breach response costs: 27.3%
  - Help desk activities / Inbound communications
  - Credit report monitoring & identity protection services
  - Issuing new accounts or credit cards
  - Legal expenditures
  - Product discounts
  - Regulatory interventions (fines)

- Lost business cost: $1.42M or 36.2% - biggest cost factor for last 5 years
  - Cost of business disruption & revenue losses from system downtime
  - Cost of lost customers & acquiring new customers (customer turnover)
  - Reputation losses & diminished goodwill
SMBs Breach Costs are Higher

- Chance of experiencing a data breach within 2 years: 29.6%
  - Nearly 1/3 more likely than in 2014

- SMBs face disproportionately larger costs relative to larger organizations
  - Globally: average breach costs
    - Less than 500 employees: $2.74M
    - 500-1000 employees: $2.65M
    - 1001-5000 employees: $3.63M
    - 5001-10,000 employees: $4.41M
  - Total cost for largest organizations (more than 25,000 employees) averaged $5.11M or $204 per employee
  - SMBs (500 - 1,000 employees) averaged $2.65M or $3,533 per employee

- Thus, SMBs have higher costs relative to their size than larger organizations, which can hamper their ability to recover financially from the incident
General Factors Affecting avg. Breach Cost per Record

- **Unexpected loss of customers** following a data breach
- **Size of data breach:** number of records compromised
- **Time it takes** to **identify & contain** a data breach
  - Average time to **identify a breach:** 196 days
  - Average time to **contain a breach:** 49 days (245 days total)

Globally, breaches with lifecycle less than 200 days were on average $1.22M less costly than breaches with lifecycle of more than 200 days ($3.34M vs. $4.56M respectively), a difference of 37%

- **Effective management of:**
  - Detection & escalation costs.
  - Post data breach costs

Ponemon Institute’s 2019 Cost of a Data Breach Study
507 companies (64 in U.S.) studied that experienced a breach in last year & 3,211 individuals interviewed
### Factors Decreasing avg. Cost per Record

<table>
<thead>
<tr>
<th>Cost Mitigators</th>
<th>$</th>
<th>Cost Mitigators</th>
<th>$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formation of the IR team</td>
<td>$360,000</td>
<td>Use of security analytics reducing human intervention</td>
<td>$200,000</td>
</tr>
<tr>
<td>Extensive use of encryption</td>
<td>$360,000</td>
<td>Board-level involvement</td>
<td>$180,000</td>
</tr>
<tr>
<td>Extensive tests of the IR plan</td>
<td>$320,000</td>
<td>Extensive use of DLP</td>
<td>$180,000</td>
</tr>
<tr>
<td>Business continuity management</td>
<td>$280,000</td>
<td>CISO appointed</td>
<td>$180,000</td>
</tr>
<tr>
<td>DevSecOps approach in design &amp; testing</td>
<td>$280,000</td>
<td>Insurance protection</td>
<td>$160,000</td>
</tr>
<tr>
<td>Employee training</td>
<td>$270,000</td>
<td>Data classification schema</td>
<td>$130,000</td>
</tr>
<tr>
<td>Participation in threat sharing</td>
<td>$240,000</td>
<td>CPO appointed</td>
<td>$50,000</td>
</tr>
<tr>
<td>Artificial intelligence incident detention &amp; response platform</td>
<td>$230,000</td>
<td>Identity theft protection provided compromised consumers</td>
<td>$10,000</td>
</tr>
</tbody>
</table>

Companies *without automated incident detection & response* had **95% higher costs**

Cost decreases are **based on global costs**, *so U.S. cost savings would be greater*.
Factors *Increasing* avg. Cost per Record

<table>
<thead>
<tr>
<th>Cost Amplifiers</th>
<th>$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party breach</td>
<td>$370,000</td>
</tr>
<tr>
<td>Compliance failures</td>
<td>$350,000</td>
</tr>
<tr>
<td>Extensive cloud migration</td>
<td>$300,000</td>
</tr>
<tr>
<td>System complexity</td>
<td>$290,000</td>
</tr>
<tr>
<td>OT infrastructure</td>
<td>$260,000</td>
</tr>
<tr>
<td>Extensive use of mobile platforms</td>
<td>$240,000</td>
</tr>
<tr>
<td>Lost or stolen devices</td>
<td>$180,000</td>
</tr>
<tr>
<td>Extensive use of IoT devices</td>
<td>$160,000</td>
</tr>
<tr>
<td>Rush to notify</td>
<td>$150,000</td>
</tr>
<tr>
<td>Consultants engaged</td>
<td>$110,000</td>
</tr>
</tbody>
</table>

Cost increases are based on global costs, so *U.S. cost increases would be greater*. 
Long Tail Breach Costs

- In a sample of 86 companies:
  - Average of 67% of costs incurred within 1\textsuperscript{st} year
  - 22% of costs incurred in 2\textsuperscript{nd} year
  - 11% of costs occur more than 2 years after data breach

- Organizations in high regulatory environments experienced a longer tail:
  - 53% in 1\textsuperscript{st} year
  - 31% in 2\textsuperscript{nd} year
  - 16% more than 2 years after incident
Ponemon: Recommendations to Help Minimize Financial Consequences of a Data Breach

- Have an incident response team & routinely table-top test incident response plans in various breach scenarios *(have detailed playbook)*

- Programs that preserve customer trust pre- & post-breach will help reduce unexpected loss of customers following a data breach

- Discover, classify & obscure/encrypt sensitive data & identify database misconfigurations *(vulnerability scanning, etc.)*

- Invest in technologies that help improve the ability to rapidly detect & contain a data breach *(increased visibility across extended perimeter)*

- Invest in governance, risk management & compliance programs

- Beware of IT complexity & disconnected security solutions *(use CASBs with cloud services, provide IoT & mobile security, etc.)*
Other Slides

- Risk Management & Control Framework
- Data Mapping
<table>
<thead>
<tr>
<th>Essential Elements of Corporate Compliance</th>
<th>Evaluation Guidance – (Eees = employees)</th>
</tr>
</thead>
</table>
| **Leadership**                           | **Senior & Middle Management** actions & statements  
  - “Tone at the top”  
  - Organizational Governance  
  - Accountability  
  - Designate Privacy/Security Official for day-to-day compliance and clearly defined roles & responsibilities for staff, mgmt & responsible executive/governance committee  
  - Autonomy/Resources – independent, experienced, qualified & well-funded compliance |
| **Risk Management**                      | **Process & procedures** for regularly identifying & effectively mitigating risks:  
  - continuous Privacy/Security-by-Design & periodic risk assessments |
| **Standards & Controls**                 | **Policies & Procedures** – design & accessibility; operational responsibilities & integration (stakeholder involvement)  
  - Data & Resource Governance – data mapping, data privacy lifecycle management  
  - HR Governance (4 stages): pre-boarding, onboarding, employment, and termination  
  - External Resource Management – engagement, screening, monitoring & management  
  - Mergers & Acquisitions – involvement in identifying risks & integration  
  - Documentation to support compliance and legal defensibility |
| **Training & Communications**            | **Training effectiveness & customized to high risk Eees**  
  - senior mgmt communications to Eees re: misconduct; resources available to guide Eees |
| **Monitoring, Detecting, & Response**    | **Confidential Reporting & Investigation** – open lines of incident reporting (anonymous hotline & exit interviews)  
  - Incentives & Disciplinary Measures/Sanctions – fairness & consistency  
  - Periodic Testing & Review (type & frequency) for Continuous Improvement  
  - Analysis & Remediation of underlying root causes & misconduct |
**Privacy Program**

Establishes governance with clear roles & responsibilities creating a sustainable foundation based on Framework

**Sustainable, Defensible and Trustworthy Privacy (& Security) Program**

**Risk management program** requires risk owners who identify & acceptably mitigate foreseeable risks (& document same) to be defendable to regulator & plaintiff judge/jury, based on COSO’s ERM approach & methodology

<table>
<thead>
<tr>
<th>Privacy Program</th>
<th>Privacy Practices</th>
<th>Security Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data &amp; resource mapping</td>
<td>• Data privacy lifecycle controls</td>
<td>• Administrative safeguards</td>
</tr>
<tr>
<td>• Governance structure</td>
<td>– notice, data collection, use, sharing &amp; retention controls</td>
<td>– e.g., RBAC design, authorization &amp; periodic review</td>
</tr>
<tr>
<td>• PI sensitivity classification</td>
<td>• Data subject rights &amp; choices</td>
<td>• Physical controls</td>
</tr>
<tr>
<td>– drives strength of controls</td>
<td>– data infrastructure &amp; management</td>
<td>– e.g., review of facility’s physical controls</td>
</tr>
<tr>
<td>• Risk management: P/SbD, periodic</td>
<td>• Data minimization (avoid re-identification)</td>
<td>• Technical controls</td>
</tr>
<tr>
<td>• Sanctions &amp; complaints</td>
<td>– e.g. min. necessary, key coding, de-identification, pseudonymization</td>
<td>– e.g. use of encryption</td>
</tr>
<tr>
<td>• External resource management</td>
<td>• Verification &amp; authentication</td>
<td>• Engineering controls</td>
</tr>
<tr>
<td>• Monitoring, auditing &amp; oversight</td>
<td></td>
<td>– e.g. implementation of Privacy/Security-by-Design/SDLC</td>
</tr>
<tr>
<td>• Incident &amp; breach management &amp; response</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Compliance** establishes baseline, however alone is not defensible as laws, regulations & standards cannot keep pace with emerging technologies – an effective risk management program closes this gap

**Enterprise cross-functional collaboration & coordination**
## Foundational Program Governance

Next slides include operational recommendations for governance elements

<table>
<thead>
<tr>
<th>#</th>
<th>Privacy</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Organizational Governance</td>
<td>Same</td>
</tr>
<tr>
<td>2</td>
<td>Governance via Policy</td>
<td>Same</td>
</tr>
<tr>
<td>3</td>
<td>HR Governance: pre-onboarding, onboarding, employed &amp; termination</td>
<td>Same</td>
</tr>
<tr>
<td>4</td>
<td>Data Privacy Lifecycle &amp; Resource Governance</td>
<td>Data &amp; Resource Mapping portion</td>
</tr>
<tr>
<td>5</td>
<td>Privacy Rights Governance</td>
<td>N/A</td>
</tr>
<tr>
<td>6</td>
<td>Privacy-by-Design Governance</td>
<td>Security-by-Design Governance</td>
</tr>
<tr>
<td>7</td>
<td>Same when dealing with Co-Data Controller (GDPR/CaCPA)</td>
<td>External Resource Mgmt Governance</td>
</tr>
<tr>
<td>8</td>
<td>Monitoring &amp; Evaluation/Auditing Governance</td>
<td>Same</td>
</tr>
<tr>
<td>9</td>
<td>Event &amp; Incident Management Governance</td>
<td>Same</td>
</tr>
<tr>
<td>10</td>
<td>Documentary Evidence of Governance</td>
<td>Same</td>
</tr>
</tbody>
</table>

External Resource Management means governance of **service providers & 3rd parties** under CaCPA

Other related governance scopes include M&A, outsourcing, system architecture, change management, project management, etc.
Raw Data Mapping SIPOC

Ask “follow the data” questions for each unique DPLC

<table>
<thead>
<tr>
<th>S</th>
<th>I</th>
<th>P</th>
<th>O</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Suppliers</strong> – Data Sources</td>
<td><strong>Data Resource From / Data Location</strong></td>
<td><strong>Data Inputs, Formats &amp; How Moved / Transferred</strong></td>
<td><strong>DPLC Process Steps</strong></td>
<td><strong>Data Outputs, Formats &amp; How Moved / Transferred</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Notice</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Collected</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Used / Processed / Accessed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Used / Processed / Accessed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Shared / Transferred</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Stored / Backed-up</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Disposed / Destruction</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Rename each process step** as organization commonly refers to it

**Add as many rows as necessary** to capture all DPLC process steps

Process managers should **update/maintain** this **and archive** each version with a revision date
<table>
<thead>
<tr>
<th>S</th>
<th>I</th>
<th>P</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Suppliers / Sources</td>
<td>Data Inputs</td>
<td>Data Flow Steps</td>
<td>Data Outputs</td>
</tr>
<tr>
<td>Location From / Data State</td>
<td>Signed Consent</td>
<td>Notice</td>
<td>Signed Consent</td>
</tr>
<tr>
<td>S</td>
<td>I</td>
<td>P</td>
<td>O</td>
</tr>
<tr>
<td>Clinic / Practice</td>
<td>FedEx / UPS</td>
<td>Receive Sealed Sample Kit</td>
<td>Locked File cabinet, Scanned to:[Shared Folder:/consents/month-year]</td>
</tr>
<tr>
<td>Accessioning</td>
<td>Receiving Area</td>
<td>sample kit w/Patient name, activation code</td>
<td>Receiving Area</td>
</tr>
<tr>
<td>Accessioning</td>
<td>Lab Work Bench</td>
<td>Open Kit: Assign barcode to sample</td>
<td>Accessioning</td>
</tr>
<tr>
<td>Lab</td>
<td>Lab Work Bench</td>
<td>Open Kit: Scanning paperwork with sample kit</td>
<td>Lab Work Bench</td>
</tr>
<tr>
<td>Lab</td>
<td>Lab Work Bench</td>
<td>sample w/Patient name, barcode, activation code</td>
<td>Lab Processing</td>
</tr>
<tr>
<td>Data Customers / Endpoints</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sample Data Flow Diagram

Our Data Mapping whitepaper is in IAPP's Resource Center available to 40,000+ global members.
# Data Resource Map

Data inventory / data sensitivity level & resource owners / custodians for each resource

## Data Resource Map:
_________________ (Name of DPLC)

Document Owner: ________________  Rev Date: __________

<table>
<thead>
<tr>
<th>Data Locations</th>
<th>Database</th>
<th>Shared folder</th>
<th>Box</th>
<th>Share Point</th>
<th>File cabinet</th>
<th>AWS S3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource owner</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource custodian</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data inventory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Data identifiers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Classification

- Highly sensitive
- Sensitive
- Slightly sensitive
- Non-sensitive

- Develop at the **end of data mapping session** – add as many columns / rows of columns as necessary
- List all **data identifiers** for each resource
- **Identify highest data sensitivity level** which determines required strength of controls
Data Mapping Benefits
Most entities have inadequate understanding of end-to-end DPLC

- Informs counsel/advisors to better advise business
- Informs controls evaluations, risk assessments & other compliance efforts
- Informs privacy notices / customer choices (opt-ins/outs & preferences)
- Informs Privacy-by-Design of new/enhanced resources (via PIAs/DPIAs)
- Informs of needed security (discover & protect unknowns)
- Informs e-discovery & breach response pre-planning
Data Mapping Benefits

Most entities have inadequate understanding of end-to-end DPLC

- Helps establish & maintain governance of DPLC processes, data & resources (data management, retention & sharing policies & practices)

- Demonstrates governance & controls with regulators, internal/external auditors & prospective business partners & investors

- Shortens new hire learning curve with product/project manager, system admin, DBAs, engineers & others

- Facilitates organizational communications & understanding about end-to-end DPLC (breaks down organizational silos)

- GDPR/CaCPA: Helps identify data collected & all DPLC processes to inventory, analyze & document re: lawful processing/business purposes
Limitations of Data Maps

- **Quality & accuracy** of manual data maps depend upon the right SMEs participating, properly vetting diagrams, & ultimately owning these going forward.

- **Automated data mining tools**
  - Produce **false positives & cannot capture all data types**
  - Remains to be seen whether future tools can replicate all the *benefits from using an interactive, highly participatory data mapping interview process*
  - **Even if** future tools *work flawlessly, would still use it to only validate data elements* identified during data mapping interviews *to get the aforementioned benefits*
More Detailed CCPA Slides
## Basic Consumer Rights

*Extends right to privacy in CA constitution by establishing first-in-kind U.S. consumer rights over data ownership and control (EU-like but not as extensive)*

| Right to **know** | • right to know **at or prior to collection** via privacy notice or just-in-time disclosure, purpose of collection, categories of PI collected, if PI is sold & to whom, and rights & methods for submitting requests  
• right to **request additional information**, including specific pieces of PI collected |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to (request) <strong>deletion</strong></td>
<td>right to request <strong>deletion of PI collected</strong> from business servers &amp; service providers upon receipt of a verified request with some exceptions</td>
</tr>
<tr>
<td>Right to <strong>opt-out of “sale”</strong></td>
<td>right to say <strong>“no” to sale</strong> of PI (or for children under 16, right to no have PI sold absent parent/guardian opt-in)</td>
</tr>
<tr>
<td>Right of <strong>access &amp; data portability</strong></td>
<td>right to access to <strong>specific pieces</strong> of PI in format allowing transfer to another entity</td>
</tr>
<tr>
<td>Right to <strong>equal service &amp; price</strong>  (anti-discrimination)</td>
<td>right to receive <strong>equal service &amp; pricing, even if exercise rights</strong>, but does permit offering financial incentives if reasonably related to value provided by consumer’s data</td>
</tr>
</tbody>
</table>

**Research:** subject commercial research (but not non-commercial research) to PII deletion requirements; and exclude disclosures of PI to external resources for commercial research purposes from business purpose exception for disclosures)
Right to know via:

- **Privacy notice at or at point of collection**
  - Consumer rights & methods for submitting requests; categories of PI collected, sold or disclosed for bus. purposes in prior 12 mos.
  - May **not** collect additional PI or use for additional purposes without proper notice & choice

- **Just-in-time disclosures at or before collection**
  - Categories of PI to be collected & purposes PI will be used

- **More specifics upon request**
  - Categories & specific pieces of PI is being collected; categories of sources from which PI is collected; bus. purposes for collecting or selling PI; categories of 3rd parties which PI is shared with
  - Consumers **do not have right to request names of actual 3rd party entities**
Notice & Choice Rights

Right to opt-out of “sale” of PI

- Sale means **for money or other valuable consideration** to “for-profit”, **3rd party or another business** (affiliate)
  - CA law provides that a written instrument is presumptive evidence of consideration
  - Does not include service providers – includes sharing PI for online advertising
  - After 12 months, may request **reauthorization**
  - Excludes M&A, except opt-out required if resulting entity uses PI in materially inconsistent manner with promises made at time of collection

- Must add clear & conspicuous homepage **button/link** titled “Do Not Sell My Personal Information” **to opt-out**

- Excludes disclosure for business purpose if specified in privacy notice & protected by written contract with appropriate obligations & certification

- Third parties receiving PI through a sale **cannot sell** that PI unless consumer has received **notice & had an opportunity to opt out** of sale

What does ‘valuable consideration’ mean under the CaCPA?

To sell or disclose children’s PI to 3rd party requires:

- **Age 16 & older** requires **Opt-out** consent
- **Ages 13 – 16** requires **express Opt-in** consent
- **Under 13** requires **parent/guardian** consent
  - Consistent with COPPA

Cannot disregard knowledge of age

Requires **further age verifications & restrictions beyond** the Children’s Online Privacy Protection Act (**COPPA**)
Right of Access & Data Portability

Similar to GDPR’s “data portability

- Entitled to receive: **person-specific details** about PI collected, sold or disclosed & specific pieces of PI collected

- Consumers may request access to PI & obtain in a **“readily usable format”** that allows porting to another entity “without hindrance”

- **Upon verification** of consumer identity, business **must respond** but not required to retain info obtained in a one-time transaction or re-identify/link info not in identifiable form *(unclear if applies to pseudonymized or de-identified data)*

- Consumers may request **no more than twice in 12 mos.**
Deletion Rights - not a part of ballot initiative

Upon valid request, must delete any collected PI & require service providers delete PI - similar to GDPR’s “right to be forgotten”

- Must be disclosed in “reasonably accessible” form to consumers, e.g. via website, privacy notice, etc.

- 9 exceptions - construed to be fairly broad in nature:
  - complete transaction for which PI collected to provide good/service requested by consumer or otherwise perform contract between business/consumer
  - detect & maintain data security & preventing fraud
  - debug to identify & fix repair errors
  - engage in public/peer-reviewed scientific, historical, or statistical research in public interest when deletion would render it impossible or seriously impair achievement of such research
  - enable solely internal uses aligned with consumer expectations based on relationship with business
  - otherwise use consumer’s PI internally in a lawful manner compatible with the context in which PI was provided
  - see slide notes for 3 other less commonly used exceptions
Limits on Liability for Violating Act

- **Businesses** sharing PI with service providers violating Act
  - Must establish at time of disclosing PI, did “not have actual knowledge, or reason to believe, service provider intends to commit” such violation (due diligence)

- **Service providers** when business for which it provides services violates Act

- **Businesses** sharing PI with 3rd parties violating Act
  - Must only disclose PI pursuant to a contract including specific provisions
  - Must contractually require a certification that 3rd party understands Act’s requirements & provisions prohibiting 3rd party from reselling PI, retaining or using PI for any purpose other than that enumerated in contract, & retaining or using PI outside of direct business relationship
Comparison
California Consumer Privacy Act (CCPA) to EU’s GDPR
### CCPA vs EU’s GDPR

#### Personal Information (PI)

- Listed data elements are PI to extent identify, relate to, describe, are capable of being associated with, or could reasonably be linked, directly or indirectly, to particular consumer or household
- Identifiers, e.g. real name/alias, postal/email address, IP address, account name, SSN, driver’s license#, passport#, or other similar identifiers
- Commercial information
- Biometric identifiers
- Internet or other electronic activity information
- Unique persistent identifiers that recognize a consumer, family or device over time & across different services
- Geolocation data
- Audio, electronic, visual, thermal, olfactory or similar information
- Professional or employment-related information
- Inferences drawn
- Does not identify sensitive PI
- Excludes aggregate consumer info & deidentified data

#### Personal Data (PD)

- PD generally means any information or data which relates to a living individual who can be directly or indirectly identified by it
- **Special Categories** of (Sensitive) PD - consists of political opinions, religious or philosophical beliefs, racial or ethnic origin, or trade union membership, genetic data, biometric data, data regarding health or data concerning a natural person’s sex life or sexual orientation
  - Excludes anonymous data

(e-Privacy Act will expand definition of PD beyond GDPR & in most cases require explicit opt-in consent for electronic communications)

---

HIPAA – not comparing PHI as this relates strictly to health information
## Differences

<table>
<thead>
<tr>
<th>Subject</th>
<th>CCPA</th>
<th>EU GDPR</th>
</tr>
</thead>
</table>
| **Scope** | • Applies to for-profit “business” that meets revenue / volume thresholds for CA resident PI  
• Business similar to data controller, except doing business in CA  
• Service provider similar to data processor is directly liable  
• 3rd parties (not recognized in EU)  
• Protects CA residents  
• Excludes HIPAA/GLBA/DLPPA/etc | • Applies to businesses, public bodies / institutions & not-for-profit entities  
• Established in EU or outside of EU & either:  
  • offering goods/services to EU or  
  • monitoring behavior in EU  
• Protects “data subjects”  
• Omnibus in nature covering all industries |
| **Notice requirements** | • Must disclose certain information about collection, sale & disclosure of PI in privacy notice on website  
• Must provide just-in-time disclosures at or before collection of PI  
• “Do Not Sell My Personal Information” button/link | • Must provide data subjects with detailed notice about collection, use & disclosure of PD, & retention period, individual rights, information about lawful bases for processing, identity of controller, DPO, local representative, etc. |

PD = Personal Data (EU)  
DPO = Data Protection Officer (EU)
### Differences

<table>
<thead>
<tr>
<th>Subject</th>
<th>CCPA</th>
<th>EU GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lawful processing requirements</strong></td>
<td>• N/A, but “business purposes” are specified as <em>presumptively valid</em> (rulemaking &amp; time will tell)&lt;br&gt;• Focuses on transparency &amp; limiting selling of PI</td>
<td>• Must have <strong>valid legal basis</strong> for all processing of personal data (PD)</td>
</tr>
<tr>
<td><strong>Consent</strong></td>
<td>• <strong>Consent</strong> via informed, transparent privacy notice &amp; just-in-time disclosures <em>is the operating model</em></td>
<td>• Consent is one of <strong>many legitimate interests &amp; least desirable</strong> as it can be withdrawn &amp; affords right to deletion&lt;br&gt;  • <em>consent rules are tighter</em>&lt;br&gt;• Other legitimate interests include:&lt;br&gt;  • <strong>performance of a contract</strong> with data subject&lt;br&gt;  • <strong>vital interests</strong> of data subject/other person&lt;br&gt;  • public interest&lt;br&gt;  • legal obligation&lt;br&gt;  • <strong>legitimate interests pursued by controller, except where overridden</strong> by interests or fundamental rights &amp; freedoms of data subject requiring protection of PD</td>
</tr>
</tbody>
</table>
## Differences

<table>
<thead>
<tr>
<th>Rights</th>
<th>CCPA</th>
<th>EU GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Children</strong></td>
<td>• Ages 13-16, minor must opt-in for selling PI</td>
<td>• Under age 16, must have parent’s or guardian’s consent – with member states permitted to lower age to 13</td>
</tr>
<tr>
<td></td>
<td>• <strong>Under 13</strong>, parent/guardian must opt-in</td>
<td>• GDPR allows other lawful grounds than consent for processing</td>
</tr>
<tr>
<td></td>
<td>• Children’s PI can be “sold” only on basis of consent</td>
<td></td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
<td>• <strong>No explicit record-keeping requirements</strong></td>
<td>• Requires a DPO</td>
</tr>
<tr>
<td></td>
<td>• Must <strong>train</strong> staff dealing with rights requests from consumers</td>
<td>• Requires <strong>local representative</strong> under certain conditions</td>
</tr>
<tr>
<td></td>
<td>• However requires <strong>tracking infrastructure of data collection &amp; processing streams</strong> to identify CA residents &amp; flag PI to honor disclosure requests &amp; opt-in/out choices</td>
<td>• Requires <strong>data &amp; processing inventory justified by legitimate interest</strong> for collection, use, sharing &amp; retention</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Requires <strong>demonstrable proof of compliance</strong> that can be requested by a DPA at any time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• some relief for controllers with less than 250 employees</td>
</tr>
<tr>
<td><strong>Anti-discrimination</strong></td>
<td>• Consumers <strong>must not be discriminated against because of exercise of rights</strong></td>
<td>• Not explicitly included as a right – however is implicit in GDPR principles</td>
</tr>
</tbody>
</table>
## Differences

<table>
<thead>
<tr>
<th>Rights</th>
<th>CCPA</th>
<th>EU GDPR</th>
</tr>
</thead>
</table>
| Service providers / data processors | • While *no explicit contractual requirements*, it is *advisable to include similar requirements*, e.g. honor deletion requests, etc.  
• **Requires disclosures of 3rd parties** receiving PI which are not businesses or service providers | • *Explicit contractual requirements*                                                                      |
| PbD & use of PIAs              | • **Not expressly required, but advisable**                           | • Mandatory **Privacy-By-Design & use of Data Privacy Impact Assessments (DPIAs)** for high risk projects  
• **Data Minimization required**                                        |
| Data Retention requirements    | • Data can **be retained for business purposes**                      | • Data can only **be retained for valid legal/legitimate purposes**                |
## Differences

<table>
<thead>
<tr>
<th>Subject</th>
<th>CCPA</th>
<th>EU GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cross-border transfer requirement</strong></td>
<td>• No adequacy determinations for transfer to other states/countries</td>
<td>• Transfers of PD data outside of EU must be to an “Adequate” country or must use X-border data transfer mechanism (Privacy Shield, SCCs, BCRs, Codes of Conduct, Seals, Certifications)</td>
</tr>
<tr>
<td></td>
<td>• No X-border transfer mechanisms</td>
<td>• Local representative required under certain conditions</td>
</tr>
<tr>
<td><strong>Enforcement</strong></td>
<td>• CA AG may impose civil penalties of up to $7,500 per intentional violation - no cap on total amount of penalty</td>
<td>• Tiered penalty system – violations may result in fines up to €20M or 4% of total worldwide annual turnover, whichever is greater</td>
</tr>
<tr>
<td></td>
<td>• Private right of action for breaches with $100-$750 statutory or actual damages</td>
<td>• Private right of action for actual damages</td>
</tr>
<tr>
<td></td>
<td>• 30 day cure period (for statutory damages under private actions)</td>
<td></td>
</tr>
</tbody>
</table>

SCCs = Standard Contractual Clauses, aka Model Clauses (EU)
<table>
<thead>
<tr>
<th>Rights</th>
<th>CCPA</th>
<th>EU GDPR</th>
</tr>
</thead>
</table>
| **Right to access**    | • Must provide consumers with details about collection, sale & disclosure of PI (e.g., categories of PI sold to different categories of 3rd parties) & “specific pieces of PI”  
• Applies to PI collected in *last 12 mos*  
• Exceptions: (a) can verify identity, (b) manifestly unfounded or excessive requests | • Must provide data subjects with access to PD & specific details about processing (purposes of processing, sources of information, etc.)  
• Applies to *all* data  
• Exceptions: (a) can verify identity, (b) manifestly unfounded or excessive requests, (c) adversely affects rights & freedoms of others |
| **Right to object**    | • Consumers have right to **opt out of “sale”** of their PI (M&A exception, except opt-out required if materially inconsistent use with original promises); greater control over data-sharing | • Data subjects have **right to object to broader processing** of PD in certain circumstances |
| **Response time to rights request** | • **Within 45 days** of receiving verifiable request  
• Can be extended by 45 days “when reasonably necessary” – or “up to 90 additional days where necessary” | • “**Without undue delay**” & in any event **within 1 mo.**  
• Can be extended by 2 mos. “where necessary” |
<table>
<thead>
<tr>
<th>Rights</th>
<th>CCPA</th>
<th>EU GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Right to portability</strong></td>
<td>If business responds to request to access PI via electronic means, “the information shall be in portable &amp; to extent technically feasible, in readily useable format that allows consumer to transmit it to another entity without hindrance”</td>
<td>Where basis for processing is consent or legitimate interests, data subjects have right to receive PD they provided to controller “in structured, commonly used &amp; machine-readable format &amp; have right to transmit data to another controller without hindrance”</td>
</tr>
<tr>
<td><strong>Right to delete PI</strong></td>
<td>Consumers <strong>have right</strong> to request PI deletion (rulemaking may provide more guidance)</td>
<td>Data subjects have right to have PD deleted <strong>where</strong> (a) “no longer necessary,” (b) they withdraw consent, (c) processing is unlawful, or (d) if processing is based on legitimate interests, there are no “overriding legitimate grounds”</td>
</tr>
<tr>
<td></td>
<td><strong>Exceptions</strong>: (i) complete transaction / perform a contract, (ii) detect / protect against / prosecute security incidents or illegal activity, (iii) debug &amp; fix errors, (iv) exercise free speech or other legal rights, (v) research exception, (vi) “solely internal uses that are reasonably aligned” with consumer expectations, (vii) compliance with law</td>
<td><strong>Exceptions</strong>: (i) continued lawful basis for processing, (ii) exercising right of expression, (iii) compliance with EU law, (iv) establishment / exercise / defense of legal claims, (v) public health exception, (vi) archiving / research exception</td>
</tr>
<tr>
<td></td>
<td>Business must direct service provider to delete consumers’ PI</td>
<td></td>
</tr>
</tbody>
</table>

Differences
Additional sources: differences between CCPA & GDPR


About Us
SoCal Privacy Consultants
Why SoCal Privacy?
Operationalizing Privacy and Security Programs

- **Practical** – we arm you with the knowledge, tools & confidence to establish a workable & functional program

- **Sustainable** – operationalize through governance with clear roles, responsibilities & practices (NIST’s Repeatable RM Tier)
  - You get our tools, so you can perform future self-assessments (sustainability)

- **Defensible** – establish risk management program & educate you on how to defend actions to a regulator & plaintiff judge or jury
  - Empower newly designated privacy & security officials re: how to effectively communicate importance of privacy & security to c-levels & board members to overcome any resistance & gain their support & commitment - regulators evaluate “the tone at the top” when the worse happens

- **Trustworthy** – a well-founded privacy & security program establishes & maintains trust relationship with consumers & other stakeholders as well as mitigates risk of costly & disruptive breaches
Why SoCal Privacy?
Key aspects of who we are at the core

**Experience** – major law firms still recommend the Big Four, but choose us when education and practical operational experience is called for

- **We’re not recent college graduates using a checklist – we’re experienced professionals**
  - Michael has testified before three FTC lawyers for two hours on behalf of a client
  - Michael served as part-time Chief Privacy Officer of an international company for 8 years
  - Neil has audit & e-discovery experience & understands FTC expectations having worked there

- **Understand client’s business and how to operationalize practices/processes**
  - Conducting data mapping first allows us to get our arms around your business to better advise you during the gap & risk assessment
  - Michael’s previous operations executive experience allows him to provide practical advice on how to operationalize practices as repeatable processes

- **Understand IT technical systems and controls**
  - Neil’s experience allows him to offer deep dive technical advice
Typical Phase I: Gap Assessment SCOPE of WORK

- **Perform Data Mapping** (data flow, inventory & locations)

- **Privacy Impacts Assessment (PIA)** - based on data mapping interviews to ensure accuracy with privacy notice and laws/regulations/standards

- **Conduct Controls Evaluations** - based on NIST Cybersecurity Framework evaluation methodology
  - HIPAA + *Top 20 Critical Security Controls*
  - ISO 27002:2013 + *Top 20 Critical Security Controls*
  - U.S. Sentencing Guidelines for Effective Compliance Programs

- **Perform Security Risk Assessment**
Phase I: Work Tools & Deliverables
Provided in Box to counsel first for release to review

- **Work tools** – Also delivered for your reuse
  - **Data mapping: SIPOC & resource map** (Excel) with example interview questions
  - **Controls evaluations workbooks** (Excel)
  - **Risk assessment workbook** (Excel) & placemat (valuation methodology)
    - Documents entire process and provides instructions for repeatability
  - **Requested documents list** (Word)

- **Deliverables**
  - **Data Flow Diagram(s)** (Vizio)
  - **Privacy Impact Assessment (PIA) Report** of recommendations (Word)
  - **Security Summary Report** (Word)
  - **Gap & Risk Register** of Prioritized Recommendations (Excel)

Recommend setting up a shared, but restricted repository for all compliance documentation to facilitate governance and help readily respond to information requests
<table>
<thead>
<tr>
<th>#</th>
<th>Service Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Requested Documents Review</td>
<td>Assure readiness to quickly and fully produce requested documents within 10 days to demonstrate compliance as part of an inquiry, audit, or investigation</td>
</tr>
<tr>
<td>2</td>
<td>RBAC Assessment and Training</td>
<td>Assess adequacy and scalability of RBAC tiers, individual/role RBAC rights assignments, and RBAC authorization and periodic review process for each Resource (containing PII) and make recommendations to assure proper governance and controls for minimum necessary defensibility; can provide roles-based training to appropriate Resource Owners/Custodians and other stakeholders (data mapping is very helpful)</td>
</tr>
<tr>
<td>3</td>
<td>Organizational Governance and Training</td>
<td>Assess organizational governance and recommend clear roles and responsibilities customized to organization, culture, risk profile and unique needs; can provide roles-based training with various stakeholders on their roles and responsibilities and how these integrate to assure a compliant and legally defensible program</td>
</tr>
<tr>
<td>4</td>
<td>Privacy/Security-by-Design (P/SbD) Governance and Training</td>
<td>Assess organizational needs and recommend clear, customized roles and responsibilities to operationalize P/SbD; can provide roles-based training with appropriate stakeholders on how P/SbD should be operationally conducted using a risk assessment, data minimization strategy, logging, and kill chain awareness and OWASP top 10 training</td>
</tr>
<tr>
<td>5</td>
<td>Monitoring and Evaluation/Auditing Program Governance and Training</td>
<td>Assess and recommend how to formally assign and govern the mechanisms for periodic monitoring and evaluations/auditing, including identifying owners for each activity, frequency (calendarize these activities), scope of each activity, where findings and corrective actions/mitigation plans should be reported, and who is responsible for developing a comprehensive “risk management and control implementation” plan for progress tracking and reporting; can provide roles-based training with various stakeholders on their roles and responsibilities (one of 7 elements of U.S. Sentencing Guidelines for Effective Compliance Programs and a major weakness in most programs)</td>
</tr>
</tbody>
</table>
### Additional Possible Future Scope of Consulting Services

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td><strong>Real Time Incident Detection and Response Evaluation</strong></td>
<td>Evaluate intrusion detection/prevention and insider theft detection processes and recommend foundational changes to strengthen internal processes or outsourcing to a Managed Security Services Provider (MSSP)</td>
</tr>
<tr>
<td>7.</td>
<td><strong>Incident/Event Management Governance</strong></td>
<td>Evaluate event reporting, logging of events/incident, and investigation and closure process and recommend improvements; can provide roles based training on roles and responsibilities, process, etc.; can also assess breach notification policy</td>
</tr>
<tr>
<td>8.</td>
<td><strong>Third Party Management Governance</strong></td>
<td>For each third party with access to PII, review due diligence Company has on file for adequacy of information security program; review governance process and third party agreement’s standard security requirements; recommend improvements; ensure due diligence reviews are documented in a Third Party Management Database or develop same for Company use; note data sensitivity involved and frequency of required periodic reviews based on data sensitivity; can provide roles-based training to appropriate stakeholders (data mapping or list of third parties)</td>
</tr>
<tr>
<td>9.</td>
<td><strong>Privacy, Breach Notification and Security Policies</strong></td>
<td>Policies may be available for licensing fee to include a defined number of hours of review hours of Company redlines to customize policies to organization, operations, culture, risk profile and unique needs (list of policies and samples available for review); policies can also be developed from scratch or existing policies reviewed</td>
</tr>
<tr>
<td>10.</td>
<td><strong>Monthly Status Report Conference Call</strong></td>
<td>Schedule monthly 30 or 60-minute call with appropriate stakeholders; prepare/provide progress tracking report of all activities in advance of call for review during call</td>
</tr>
<tr>
<td>11.</td>
<td><strong>Implementation</strong></td>
<td>For any recommendation made by Consultant, Company may desire Consultant’s help with implementation</td>
</tr>
<tr>
<td>12.</td>
<td><strong>Retainer</strong></td>
<td>On demand privacy and security consulting advice generally by phone or email that is documented in a monthly tracking log to be provided with the monthly invoice; rates vary based on the monthly book of hours selected; hours can be used in a variety of ways, e.g. provide guidance, such as Privacy/Security-by-Design guidance on new or enhanced projects, conduct due diligence of a new prospective Third Party, etc.</td>
</tr>
</tbody>
</table>
Certified, experienced privacy and security professionals arm you with the knowledge, tools and confidence to build and establish a practical, sustainable, and legally defensible Privacy and Security Program with our 2-phased process:

Phase 1 - Gap Assessment
- Create data flow, inventory, and locations map which the first step towards governance
- Conduct controls evaluation of your current program against applicable regulations and standards
- Perform risk assessment to identify foreseeable risks and acceptably mitigate these risks
- Provide reports: security prioritized recommendations and privacy impacts assessment to help you establish or strengthen your program

Phase 2 - Implementation
- Assist with custom implementation of Phase 1 recommendations, including policies and processes

Our experience and expertise allows us to serve a wide range of industries, such as high tech, Internet, financial services, and biotech/life sciences/healthcare firms.

Michael Cox, CI PP  mcox@socalprivacy.com
President and Founder  619.318.1263
www.SoCalPrivacy.com

Also privacy and security consulting for mobile apps and due diligence of third parties and M&A