Breaking Down Privacy -
The Landmark California Consumer Privacy Act of 2018 and How it Compares to HIPAA and EU’s GDPR (3 CPE)

IIA/ISACA Joint San Diego Chapters’ IT Full Day Seminar
Wednesday, November 14 | 10am – 12:30pm
Marina Village Conference Center, Starboard Room
1936 Quivira Way, San Diego 92109

Michael Cox, CIPP/US
President and Founder
Chief Privacy Consultant

Neil R Packard, CISA
Chief Security Consultant
## Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:30 – 8:00</td>
<td>Registration/Check-In/Breakfast</td>
</tr>
<tr>
<td>8:00 – 8:10</td>
<td>Announcements</td>
</tr>
<tr>
<td>8:10 – 9:50</td>
<td>Building a Successful Audit Plan for Cloud Services (2 CPE) – Matt Stamper</td>
</tr>
<tr>
<td>9:50 – 10:00</td>
<td>Break</td>
</tr>
<tr>
<td>10:00 – 12:30</td>
<td>Breaking Down Privacy – The Landmark California Consumer Privacy Act of 2018 and How it Compares to HIPAA and EU’s GDPR (3 CPE) - Michael Cox and Neil Packard</td>
</tr>
<tr>
<td>12:30 – 1:15</td>
<td>Lunch</td>
</tr>
<tr>
<td>1:15 – 2:55</td>
<td>Cyber Security Incident Response Best Practices (2 CPE) – Emily O’Carroll and Rebecca Hanovice</td>
</tr>
<tr>
<td>2:55 – 3:10</td>
<td>Break</td>
</tr>
<tr>
<td>3:10 – 4:00</td>
<td>Robotic Process Automation (1 CPE) – David Matthews and Lester Sussman</td>
</tr>
</tbody>
</table>
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
How many –
- are aware of CaCPA?
- already complied with GDPR?
- in Financial Services?
- in Healthcare industry?
- in SMB?
- in Publicly-traded?
Agenda

- Privacy introduction
  - Risk management, Privacy-by-Design and defensibility
  - Privacy accountability model
  - Data privacy & its relationship with information security

- California Consumer Privacy Act of 2018 (CaCPA) & Amendments
  - History & Amendment
  - The law
  - Roadmap for compliance

- CaCPA similarities & differences with EU’s GDPR
  - Taking advantage of HIPAA & GLBA exemption

- Roadmap to compliance

- Sustainable governance & data mapping

- In sum

Note: Amendment changes marked in burnt red
Introduction

Privacy
<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DPLC</strong></td>
<td><strong>Data Privacy Lifecycle</strong> – notice, collection, purpose, access, 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 (&quot;inputs&quot;) and to (&quot;outputs&quot;) during the DPLC (&quot;process steps&quot;) – and only capture process steps where personal data is involved <em>(used during my ERM experience)</em></td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td><strong>Products/services, processes, software/apps, databases, technologies, systems &amp; service providers / 3rd parties</strong> <em>(ext. resources)</em> containing/involving PI</td>
</tr>
<tr>
<td><strong>PbD / PIAs</strong></td>
<td><strong>Privacy-by-Design / Privacy Impact Assessments</strong> <em>(DPIA or Data Protection Impact Assessment)</em></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>
Privacy & security fundamentals

- More than compliance risks: financial, regulatory, legal, operational-disruption & brand/reputation risks
- Breaches are inevitable despite reasonable efforts
- Requires defensible & sustainable program of policies, governance & embedded practices
- Must be prepared to properly respond to:
  - Partner due diligence
  - Breaches
  - Ensuing regulatory investigations & lawsuits
- Part of Trust equation - a Privacy/Security-by-Design functional requirement of products, processes, etc.
Compliance vs. defensible strategy
Many compliant organizations continue to suffer breaches

- **Check-the-box compliance is not defensible**
  - Standards establish **min.** baseline, but are not enough
  - Laws, regs & standards cannot keep up with emerging threats & technologies

- Principles for building & preserving long-term value
  - **When, not if** – presumption:
    - breach will occur; and
    - will be investigated & subject to legal proceedings
  - Able to make **legally sound, compelling arguments** from view of a plaintiff’s judge/jury or regulator that you’ve done **everything reasonable**
Privacy-by-Design enables defensibility

- Establish **Risk Management System** (RM)
  - **Institutionalizes** risk ownership & accountability
    - ERM is a sustainable model
- Define **clear roles & responsibilities**
- Bake **Privacy-by-Design** into policy & training
  - Anticipate foreseeable risks
  - Design & document reasonable controls
    - Incorporate **Privacy-by-Default**
  - Develop & test controls, prior to roll-out
NIST Risk Management (‘‘RM’’) Implementation Tiers

Tiers consider organization’s current RM
- Practices
- Threat environment
- Legal & regulatory requirements
- Business objectives & organizational constraints.

Determine desired Tier:
- Meets organizational goals
- Cost-effective
- Reduces risk to acceptable levels
<table>
<thead>
<tr>
<th>Tier</th>
<th>Risk Level</th>
<th>Risk Management Process</th>
<th>Integrated RM Program</th>
<th>External Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PARTIAL</td>
<td>Informal, ad-hoc, reactive</td>
<td>Limited awareness</td>
<td>No processes in place</td>
</tr>
<tr>
<td>2</td>
<td>RISK INFORMED</td>
<td>Management approved RM practices are not established policy</td>
<td>Risk awareness but informal RM</td>
<td>Awareness, but no formalized</td>
</tr>
<tr>
<td>3</td>
<td>REPEATABLE</td>
<td>Sustainable, Formal RM practices in policy</td>
<td>Formal policies/procedures are implemented/reviewed</td>
<td>Understand dependencies collaborate with other entities</td>
</tr>
<tr>
<td>4</td>
<td>ADAPTIVE</td>
<td>Lessons learned &amp; predictive indicators inform RM practices</td>
<td>RM is part of the culture</td>
<td>Collaboration ensures accurate, current information shared</td>
</tr>
</tbody>
</table>
## CaCPA: 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>Data owner</td>
<td>Exercise rights (control) thru notice/consent</td>
</tr>
<tr>
<td>- Individual –</td>
<td></td>
<td></td>
</tr>
<tr>
<td>state laws</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Patient - HIPAA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Data subject –</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business</strong></td>
<td>Trusted organization</td>
<td>Defines data collected &amp; purposes &amp; means of processing - <em>responsible</em> 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 –</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Service provider</strong></td>
<td>Subcontractor</td>
<td>Processes strictly on behalf of data controller - responsible for own security practices - but also with direct liability</td>
</tr>
<tr>
<td>- Bus. associate - HIPAA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Data processor –</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3rd parties</strong></td>
<td>Advertisers, data brokers</td>
<td>Any other person/business receiving PI from a business pursuant to certain contractual limitations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Back to Slide 42
Question...

What are some implications of this accountability model relative to how business is often being conducted today?  
(re: slide 14)
## 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></td>
</tr>
<tr>
<td><strong>Consumer rights &amp; choices</strong></td>
<td><strong>Data protection</strong></td>
</tr>
<tr>
<td><strong>Notice / transparency</strong> <em>(informed)</em></td>
<td><strong>IP, network &amp; asset protection</strong></td>
</tr>
<tr>
<td><strong>Legitimate purpose / consent for collection, use, access, sharing &amp; retention</strong> <em>(DPLC management)</em></td>
<td><strong>Confidentiality, integrity &amp; availability</strong></td>
</tr>
<tr>
<td>- Authorized access governance</td>
<td>- Unauthorized access</td>
</tr>
<tr>
<td><strong>Laws, context, social norms, principles &amp; risk oriented</strong></td>
<td><strong>Standards &amp; controls oriented</strong></td>
</tr>
<tr>
<td><strong>Includes security</strong></td>
<td><strong>Does not include privacy</strong></td>
</tr>
<tr>
<td><strong>Accountability / governance / trust</strong></td>
<td><strong>Often not included in standards</strong></td>
</tr>
</tbody>
</table>
Question...

What does this tell you about the different nature of privacy & security?
(re: slide16)
Answer

- **Security** standards generally *strengthen over time* as a means to trying to stay ahead of threats.

- **Privacy** as a concept is *ever evolving* due to new technologies, new contexts, new social norms, etc.

  - **Question**: What are some examples of?
    - What may be *creepy in one context* that *may not be creepy in another context*?
    - What may be *acceptable today* that was *not acceptable in the past*?
## Privacy principles

Other frameworks: FTC’s FIPP, APEC, OECD, Privacy Shield, ISACA, etc.

<table>
<thead>
<tr>
<th>10 Generally Accepted Privacy Principles (GAAP) – AICPA/CICA</th>
<th>EU’s GDPR – 6 principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Management</strong> (assigns accountability)</td>
<td><strong>1. Lawfulness, fairness &amp; transparency</strong> (consent is one option)</td>
</tr>
<tr>
<td><strong>2. Notice</strong></td>
<td><strong>2. Purpose limitation</strong></td>
</tr>
<tr>
<td><strong>3. Choice &amp; consent</strong></td>
<td><strong>3. Storage limitation</strong></td>
</tr>
<tr>
<td><strong>4. Collection</strong> (re: purpose)</td>
<td><strong>4. Accuracy</strong></td>
</tr>
<tr>
<td><strong>5. Use, retention &amp; disposal</strong> (re: purpose)</td>
<td><strong>Purpose limitation</strong></td>
</tr>
<tr>
<td><strong>6. Access</strong> (consumer review/update)</td>
<td><strong>5. Integrity &amp; confidentiality</strong></td>
</tr>
<tr>
<td><strong>7. Disclosure to 3rd parties</strong></td>
<td><strong>Accuracy</strong></td>
</tr>
<tr>
<td><strong>8. Security for privacy</strong> (unauthorized access)</td>
<td><strong>6. Data minimization</strong></td>
</tr>
<tr>
<td><strong>9. Quality</strong> (accurate, complete &amp; relevant)</td>
<td></td>
</tr>
<tr>
<td><strong>10. Monitoring &amp; enforcement</strong></td>
<td></td>
</tr>
</tbody>
</table>

Other: Onward transfer

Legend: FIPP = Fair Information Practice Principles; APEC = Asia-Pacific Economic Cooperation; OECD = Organization for Economic Co-operation and Development.
Privacy requires information governance

- Notice/consent-choice

- Data processing governance
  - Data collection - purpose
  - Data access/use - purpose (internal)
  - Data access/availability/correction/quality (consumer)
  - Data disclosure/sharing/transmit - purpose
  - Data storage/retention - purpose & secure disposal

- Data minimization

- Data security (CIA)

- Cross border data transfer rules
Data minimization via Privacy-by-Design

- **Anonymized**: low risk of identification due to *singling out, link-ability or inference*
  - EU threshold: *irreversible* to prevent identification

- **PI**: do not disclose as anonymous in notice/consent/marketing
  - **De-identified** – remove all direct identifiers
  - **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
  - **Aggregate data**
  - **Minimum necessary**

https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm
Minimum necessary applies across DPLC

- **Minimum necessary** to accomplish legitimate purpose
  - Data *collection*
  - RBAC *access* to perform *regular job duties*
  - Data *use*
  - Data *sharing/disclosures*
  - Data *retention* to mitigate company liability
    - *Justify data retention based on facts* (not speculation)

- **Dispose** of data *timely & securely*
Like EU’s GDPR

- CaCPA has extra-territorial reach, major operational impacts & potential for huge fines

- Many organizations will be underprepared & not ready to comply when it comes into force
  - Compliance organizations create competitive advantage with prospective business partners through due diligence

- There is a reason it was published well in advance
  - Very complex and disruptive & is not a “box-ticking” compliance exercise
  - Requires substantial development & implementation
  - Has enforcement teeth & right to sue
CA has led U.S. & often the world in codifying privacy protections

- **1972** CA Constitution amended to include right of privacy among “inalienable” rights of all people

- **2002** CA Legislature amends law defining “personal information” (“PI”)

- **2002 - 2017** CA legislature enacts privacy laws including:
  - CA Breach Notification Act (2002) – 1st
  - Online Privacy Protection Act (2004) – 1st
  - Shine the Light Law (2005)
Previously, focus has been on EU’s GDPR

Focus shifts to a bold new law passed by California

**The Consumer Privacy Act of 2018**

Most comprehensive & complex data privacy regulation in the U.S.

*Organizations around the world will have to comply with the Act*

*GDPR compliance does not satisfy CaCPA*
This all started as a result of …

- Alastair Mactaggart & his wife having dinner with friends, including a Google software engineer

- Asked his friend if he should be worried about everything Google knew about him. “I expected one of those answers you get from airline pilots about plane crashes. You know — ‘Oh, there’s nothing to worry about.’”

- Instead, his friend told him … “If people really knew what we had on them, they would flip out.”

- Mactaggart studied this issue for 2 years & ultimately became perhaps most important U.S. privacy activist

https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html
Citizens force legislature’s hand

To fast track this law thru its process to avoid CA’s unique ballot initiative process, however it suffers from redundancy, drafting errors & lack of clarity

2017: Californians for Consumer Privacy (CCP) started Consumer Privacy Act ballot initiative for Nov. election (allowing plaintiffs to sue for $1000 per “technical” violation)

2018:
- **May - CCP**
  - Obtained 625K signatures within weeks & submitted for ballot measure approval
  - Agrees to withdraw initiative if CA legislature passes law
- **June 25**
  - CCP’s initiative qualifies for the Nov. statewide ballot
- **June 28**
  - AB 375 text 1st published on June 21 after only 2 days of drafting
  - CA Consumer Privacy Act of 2018 signed into law, after only a week of debate
Almost immediately, resistance & changes begin

- Coalition of 30+ **industry associations/groups**, including CA Chamber of Commerce, advocated for: (see slide in Appendix)
  - **Modifications to** definitions of “consumer” & “PI”
  - Increased operational flexibility to create/use de-identified data
  - Removal of **data portability** provision
  - Clarification of **non-discrimination** provision

- 64 days later, late Fri. night, 8/31, before 2018 adjournment, **CA legislature approved SB 1121**, sending a package of amendments to Governor for review by 9/30, 2018
  - Corrects many **typographical/drafting errors** (technical clean-up)
  - Provides far **more limited relief than many had hoped**
  - Includes several business-friendly amendments - small, but substantive
On 9/23, CA Governor signed into law SB-1121 Amendment to CaCPA

- SB 862 allocates $700K & 5 new staff members to support AG to promulgate regulations to implement CaCPA & provide compliance advice upon request

Amendment puts deadline of July 1, 2020 on AG to publish implementing regulations

- AG cannot enforce until 6 mos. thereafter or July 1, 2020, whichever comes 1st
  - May buy businesses up to additional 6 mos. depending on how long it takes to promulgate regulations
  - But CA AG expects to issue final rules in June 2019 enabling enforcement to begin Jan. 1, 2020
Could CA legislature *water down* CaCPA?

What is likelihood of & **implications for**:

- **Other states** passing similar laws?
- **Federal omnibus privacy law**?
- **EU Adequacy**?
Imagine 50 versions of CaCPA!

- Expect additional amendments
- Ballot initiative’s sponsors pledged to revive initiative if CaCPA is watered down
  - Appears new law’s core requirements & approach will stay intact
- Other states considering new rules likely with material differences leading to patchwork similar to breach notification laws
- Tech giants pushing for U.S. omnibus privacy law preempting state laws
  - Consumer advocates want federal law to simply be a floor
  - Executive branch developed proposed privacy framework
  - Congress not likely acting until after Nov. elections, if then
  - Not likely going to achieve EU’s “adequacy” standard
But, just as with GDPR don’t wait ...

*begin now to work towards compliance*

Businesses should **budget** for CaCPA compliance **early**

Start data mapping & tracking data & data practices as of Jan. 1, 2019

to comply with **1-year look-back re: consumer data disclosure requests** - enforcement delay serves as a delay for this obligation
CaCPA highlights

- Extraterritorial effect
- General applicability, independent of industry sector with certain exceptions
- New consumer rights
- Need to implement new data tracking, disclosure & management practices
- Regulatory enforcement by State AG
- Private right of action in certain circumstances
- No express duty regarding data security - but rather is a remedy for certain security incidents defined in Section 1798.150(a)
Who is protected?

- **Consumers** – natural persons who are residents of CA (customer business relationship not necessary) including:
  - Employees & independent contractors
  - Visitors to company premises, tenants, students, parents, children, etc.
  - Individuals associated with commercial customers / 3rd party relationships

- **Resident** includes every individual who is:
  - In CA for other than a temporary/transitory purpose &
  - Domiciled in CA who is outside State for temporary or transitory purpose

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

- Number of businesses
  - U.S.: 500,000+ companies
  - California: 135,000+ companies

- Vast majority are small- to medium-sized businesses

- But, underestimated as based on revenue & number of customers, not for example website visitors

Figures derived by an IAPP examination of the language of the law as applied to U.S. census data about American businesses. Link not provided as article only available to IAPP members.
Who must comply?

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

- Every “for profit” business
- Service providers processing PI on behalf of such business - use of PI must be limited by contract
- 3rd parties - any other person/business receiving PI from a business pursuant to certain contractual limitations
Who must comply?

- Every “for profit” business that:
  - Collects PI for a business purpose
  - Determines purposes & means of processing
  - Does business in CA & meets one of following criteria
    - Annual gross revenue $25M (not clear if CA or global rev.)
    - Annually buys, receives, sells or shares PI of > 50,000 consumers, households or devices for commercial purposes
      - Note: almost 40M people live in CA
    - Derives > 50% of annual rev. from selling consumers’ PI
How many CA residents’ PI would have to be collected daily to come under CaCPA?

- To sharing unique website visitors with Google Analytics for analysis
- To share credit card shipping information with vendor

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

- Examples?
SMB impact examples

- Even **SMBs** with less than $25M in revenues could still be **subject to the Act if it**: (BakerHostetler)
  - Has **50,000+ unique CA visitors annually to its website & makes money by** or otherwise engages in **interest-based advertising**
    - That’s avg. of **138** unique website visits daily or combination thereof
    - Same logic: simply processing avg. of 138 credit cards daily
    - And other data collection practices you can think of
  - It derives 50% of its revenue from interest based advertising

- So **all but smallest businesses will need to comply**
CaCPA exempts

- Non-profits

- Federal privacy laws - *Amendment clarifications*
  - **HIPAA/CMIA** cov. entities (CEs)/bus. assoc. (BAs)
    - Also 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 exempted
    - *Excludes research for commercial purpose*
  - **GLBA** entities are exempted
    - But are subject to CaCPA provisions & requirements if engage in activities outside of GLBA
  - **FCRA & DPPA**
Limits on liability for violating Act

- Businesses sharing PI to service providers violating Act
  - To qualify, must establish that at the time of disclosing PI, it did “not have actual knowledge, or reason to believe, that service provider intends to commit” such violation.

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

- Businesses sharing PI with 3rd parties violating Act
  - To qualify for this limit, must:
    - Only disclose PI pursuant to a contract including specific provisions
    - 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.

See Accountability Matrix
### Incredibly broad definition of PI

11 categories of data elements listed are PI, not automatically, but 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></th>
<th><strong>Identifiers</strong></th>
<th>such as real name/alias, postal/email address, IP address, account name, SSN, driver’s license#, passport#, or other similar identifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Categories of PI described in CA’s customer records destruction law: 1798.90e</td>
<td>categories of public records, e.g. cities, that are PI subject to records retention schedule</td>
</tr>
<tr>
<td>3</td>
<td>Characteristics of protected classifications under CA or federal law, e.g. Education info</td>
<td>PI not considered publicly available under Family Educational Rights and Privacy Act (FERPA), &amp; “characteristics of protected classifications under CA or federal law”</td>
</tr>
<tr>
<td>4</td>
<td><strong>Commercial information</strong></td>
<td>including records of personal property &amp; products/services purchased, obtained or considered, or other purchasing &amp; consuming histories &amp; tendencies</td>
</tr>
<tr>
<td>5</td>
<td><strong>Biometric identifiers</strong></td>
<td>e.g., sleep, health &amp; exercise data</td>
</tr>
</tbody>
</table>
Question...

What commercial information might your organization currently collect that might be within CaCPA’s scope?

(re: slide 43)
### Incredibly broad definition of PI

11 categories of data elements listed are PI, not automatically, but 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>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Internet or other electronic activity information</td>
</tr>
<tr>
<td>7</td>
<td>Unique persistent identifiers that recognize a consumer, family or device over time &amp; across different services</td>
</tr>
<tr>
<td>8</td>
<td>Geolocation data</td>
</tr>
<tr>
<td>9</td>
<td>Audio, electronic, visual, thermal, olfactory or similar information</td>
</tr>
<tr>
<td>10</td>
<td>Professional or employment-related information</td>
</tr>
<tr>
<td>11</td>
<td>Inferences drawn</td>
</tr>
</tbody>
</table>
Question...

- Can you have PI without a name of a consumer?
- What data elements stand out as surprising, perhaps in terms of what your organization currently collects?

(re: slide 45)
## 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><em>buying, renting, gathering, obtaining, receiving, or accessing</em> any personal information (PI) pertaining to a consumer by any means</td>
</tr>
</tbody>
</table>
| **Sale**    | 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 *to another business or a 3rd party for monetary or other valuable consideration* (almost always “contractual consideration”)
| **Disclosure** | providing PI to another person for *operational* purposes, or other *notified purposes*, provided use of PI shall be reasonably necessary & 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 |

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?

(re: slide 47)
CaCPA: aggregate & de-identified info is not PI

<table>
<thead>
<tr>
<th>Information</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate</td>
<td>information that relates to a <strong>group or category</strong> of consumers, from which individual consumer identities have been removed and is “<strong>not reasonably linkable</strong>” to a consumer or <strong>device</strong></td>
</tr>
<tr>
<td>De-identified</td>
<td>information that <strong>cannot reasonably</strong> identify, relate to, describe, be capable of being associated with, <strong>or be linked</strong>, directly or <strong>indirectly</strong>, to a particular consumer (eliminates “key-coded” data sets which are linkable)</td>
</tr>
</tbody>
</table>
How does this definition of de-identified differ with HIPAA’s?
(re: slide 49)
Exception: aggregate & de-identified information

- **Does not restrict** ability to collect, use, retain, sell or disclose **de-identified or aggregate** consumer PI

  - **But stronger de-identified definition:** “information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer”
    - Thus, *information that used to be thought of as de-identified may be PI under CaCPA*, e.g. hashed email addresses used in multi-party marketing transactions

- To qualify for exception, must implement **4 safeguards** & processes to **prevent reidentification** (see slide notes)

- Given technology is increasingly capable of reidentifying data by combining various sources, **be careful when pursuing anonymization or de-identification** strategies
Basic consumer rights

Extends right to privacy in CA constitution by establishing 1st-in-kind U.S. consumer rights over data ownership & control (EU-like but not as extensive)

- Right to know
  - PI collected
  - If PI sold/shared & to whom
- Right to (request) deletion
- Right to opt-out of “sale”
- Right of access & data portability
- Right to equal service & price (anti-discrimination)
Notice & choice rights prior to or at time of PI collection

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 prior to or at time of PI collection

- **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)
    - Does not include service providers – but includes sharing PI for online advertising purposes
    - After 12 months, may request reauthorization
  - 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 that receive PI through a sale cannot sell that information unless consumer has received notice & had an opportunity to opt out of sale
Notice & choice rights prior to or at time of PI collection

- To sell or disclose children’s PI to 3rd party requires:
  - Express opt-in by parent/guardian for ages 13-16
    - Consistent with COPPA
  - Opt-out for age 16 & older

Cannot disregard knowledge of age

This requires further age verifications & restrictions beyond the Children’s Online Privacy Protection Act (COPPA)
<table>
<thead>
<tr>
<th><strong>WHAT MUST BE DISCLOSED</strong></th>
<th><strong>WHO MUST DISCLOSE</strong></th>
<th><strong>WHERE TO DISCLOSE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector of personal information</td>
<td>Seller of personal information</td>
<td>Online privacy notice or website's &quot;California Rights&quot; section</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></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>X</td>
</tr>
<tr>
<td>Categories of personal information disclosed for a business purpose</td>
<td>X</td>
<td>X</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>X</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>X</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</td>
<td>Seller of</td>
</tr>
<tr>
<td>Consumers’ rights</td>
<td>of personal</td>
<td>personal</td>
</tr>
<tr>
<td></td>
<td>information</td>
<td>information</td>
</tr>
<tr>
<td>To request access to</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>their personal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>information, along with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>one or more designated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>methods for submitting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>such requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To request deletion of</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>their personal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To opt out of the sale</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>of their business</td>
<td></td>
<td></td>
</tr>
<tr>
<td>information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not to be discriminated</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>against for exercising</td>
<td></td>
<td></td>
</tr>
<tr>
<td>any of their other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CaCPA rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notice of any financial</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>incentives pursuant to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section 1798.125(b)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear description of</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>material terms of any</td>
<td></td>
<td></td>
</tr>
<tr>
<td>financial incentive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>program</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*See discussion of: Section 1798.110(c)*
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

- Right to request deletion of 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
Anti-discrimination rights
A dense, vague portion of the Act - obtain privacy counsel advice

Right to equal service/price, even if exercise rights

- Conversely, prohibits discrimination by charging different rates/services or denying goods/services for exercising rights
  - Includes offering different prices, qualities of goods, or levels of service (or even suggesting such will occur if rights are exercised)

- Permitted to offer different prices or levels of service if difference is “reasonably related to the value provided to consumer by consumer’s data”

- Permitted to offer “financial incentives” reasonably related to value provided to consumer, with notice & prior opt-in consent, for PI collection, sale or deletion
  - Consider creative incentives for consumers to opt-in
  - Could pay for PI use or privilege of remaining anonymous
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 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
  - Must identify all pieces of consumer PI, including across 3rd parties, to fulfill disclosure requests & opt-ins/outs & record date, timestamp & authentication
  - When electing not to substantively respond, inform of reasons for not taking action & any rights to appeal, recognizing desire to avoid an action

- Requires training of staff responsible for handling:
  - Consumer inquiries about rights & privacy practices
  - Handling rights requests
Enforcement with large civil penalties

- Exclusively enforced by CA Attorney General
  - Businesses failing to cure within 30-day cure period face penalties:
    - Up to $2,500 for each violation (likely per consumer), or
    - Up to $7,500 for each intentional violation – Amendment clarified not just negligent
  - Also subject to an injunction
  - 20% of penalties collected to fund enforcement

- To avoid statutory damages, must provide substantive evidence of compliance
  - CA AG estimates it needs 57 full-time staff to enforce law and secure over $57.5M in civil penalties to cover cost, suggesting enforcement may be robust (Baker Hostetler)
CA AG has rule-making authority

- Specific implementing rules:
  - **June 28, 2019**: opt-out, notice, access/portability & exception provisions
  - **January 1, 2020**: 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: (can be aggregated into class action)
  - Greater of statutory damages of $100-$750 or actual damages per consumer per incident
  - Amendment: applies only to “data breach” violations & not technical violations of Act as a whole – thus definition of breached PI is narrower than CaCPA’s PI definition
  - If consumer has provided 30-day written notice & bus. has not cured violation & provided “express written statement” that violation has been cured & “no further violations (will) occur”
    - Can sue if business continues to violate CaCPA in breach of its written statement
  - For pecuniary damages (of quantifiable monetary value), no notice required
Private right of action’s PI definition is much *more limited than the broader CaCPA definition*

- Private right of action **only applies to a breach of** the following data elements, which are:
  - Individual’s 1st name/initial & last name *in combination with* any one or more of following, when either name or data elements are 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**
Apply CaCPA 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
Other CaCPA internal business impacts

- **Marketing PI** (see detail slide in appendix for more info)
  - No distinction between PI held in **B2B** vs. B2C relationship
  - Reconsider use of 3rd-party PI requiring disclosure
  - Identify, locate & delete improper PI used for marketing purposes (revise forms/profiles) due to disclosures
  - Think carefully before selling PI about customers/users

- **Employee PI** (see detailed slide in appendix for more info)
  - Map employee PI & establish governance over data
  - Employee privacy notices, handbooks & posters
  - Honor employee rights (same as consumer rights)

[Learn more at Lexology](https://www.lexology.com/library/detail.aspx?g=fe141600-2456-4e70-901d-484366dcfe81)
Comparing CaCPA to EU’s GDPR
And qualifying for HIPAA & GLBA exemptions
<table>
<thead>
<tr>
<th>Privacy Rights</th>
<th>GDPR</th>
<th>CaCPA</th>
<th>HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to Notice &amp; Choice: (provide notice &amp; inform of rights): CaCPA – Notice/Disclosures; HIPAA - NOPP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Right to Access (quality; correction / amendment)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Right to Notifying External Resources re: Corrections, Erasure or Restriction (opt-in/out)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Right to Data Portability</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Right to Object to Processing: 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 Erasure (“right to be forgotten”): 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 Restrict Processing (opt-in/out of sale)</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Right to Not Be Evaluated via Automated Profiling</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Right to Complain (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>
CaCPA impact on health & life sciences entities

1. Determine if any data is covered by CaCPA
   a. Exceptions: **HIPAA, CMIA, Common Rule clinical trials** & non-profit not part of HIPAA/CMIA entity, subject to 3rd party requirements
   b. Determine if any collected patient info is not PHI under HIPAA or medical info under CMIA - if treated in same manner as under HIPAA/CMIA, such PI is an **CaCPA exception** for CE, however BA is not expressly exempted
   c. Determine if clinical trial is for human subjects’ research conducted/supported by federal department/agency - commercial research does not qualify as an exception

Question...

Does a company with a direct-to-consumer health care mobile app that voluntarily chooses to adhere to HIPAA standards also have to comply with CaCPA?

How many people by a show of hands think? (could have them stand for yes and sit for no for engagement)
- Yes
- No

(re: slide 72)
CaCPA impact on health & life sciences entities

2. Identify & evaluate de-identification methods & map data to CaCPA’s definitions & requirements
   a. CaCPA **does not apply to “de-identified” data** that cannot reasonably identify, relate to, describe, capable of being associated with, or be linked, directly or indirectly, to particular consumer, provided a company uses de-identified information and has implemented proper processes & safeguards.
   b. CA AG may clarify if de-identified data under HIPAA (no longer PHI) falls into CaCPA if not de-identified under CaCPA

CaCPA impact on health & life sciences entities

3. Determine if company’s disclosures could now be considered “sales” of data.
   a. Especially when monetary or other valuable consideration involved - if so, a number of individual rights will be in play

4. Assess whether company needs to develop/update policies/ procedures for individual rights requests.
   a. CaCPA grants additional rights (CEs/BAs should have more mature rights polices & practices required by HIPAA)
      i. Request deletion/disclosure, opt-out/in to sales, anti-discrimination if exercise rights, private right of action
   b. CEs/BAs may maintain data not subject to HIPAA that may be subject to new CaCPA rights requirements

Comparison
California Consumer Privacy Act (CaCPA) to EU’s GDPR
Background: CaCPA & GDPR

- **GDPR**
  - negotiated over 4 years
  - published 2 years in advance

- **CaCPA**
  - negotiated virtually overnight
  - published 1.5 years in advance of enforcement with a 12 mo. look back at data collected for disclosure requests
Commonalities: CaCPA & GDPR

- Protect residents & thus have extra-territorial reach
- Can include HR/employment data in scope
- Applicability thresholds cover many SMBs
- Create new consumer rights
- De-identification definition is very similar
- Must track & document compliance, but in a very different manner
- Create new service provider/data processor obligations which must be expressed in agreements
- Compliance with GDPR can be leveraged, but will not fulfill CaCPA requirements
<table>
<thead>
<tr>
<th>CaCPA</th>
<th>EU’s GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Information (PI)</strong></td>
<td><strong>Personal Data (PD)</strong></td>
</tr>
<tr>
<td>▪ 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</td>
<td>▪ PD generally means any information or data which relates to a living individual who can be directly or indirectly identified by it</td>
</tr>
<tr>
<td>▪ <em>Identifiers</em>, <em>e.g.</em> real name/alias, postal/email address, IP address, account name, SSN, driver’s license#, passport#, or other similar identifiers</td>
<td>▪ <strong>Special Categories</strong> 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</td>
</tr>
<tr>
<td>▪ Commercial information</td>
<td>(e-Privacy Act will expand definition of PD beyond GDPR &amp; in most cases require explicit opt-in consent for electronic communications)</td>
</tr>
<tr>
<td>▪ Biometric identifiers</td>
<td></td>
</tr>
<tr>
<td>▪ Internet or other electronic activity information</td>
<td></td>
</tr>
<tr>
<td>▪ Unique persistent identifiers that recognize a consumer, family or device over time &amp; across different services</td>
<td></td>
</tr>
<tr>
<td>▪ Geolocation data</td>
<td></td>
</tr>
<tr>
<td>▪ Audio, electronic, visual, thermal, olfactory or similar information</td>
<td></td>
</tr>
<tr>
<td>▪ Professional or employment-related information</td>
<td></td>
</tr>
<tr>
<td>▪ Inferences drawn</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Subject</th>
<th>CaCPA</th>
<th>EU GDPR</th>
</tr>
</thead>
</table>
| **Scope**   | • Applies to for-profit “business” that meets **revenue / volume thresholds** for CA resident PI  
• Business defined similarly to EU “controller”  
• Service providers/processors are directly liable  
• **3rd parties** | • Applies to controller & processor  
• Established in EU or outside of EU & either:  
  • **offering goods/services to EU** or  
  • **monitoring behavior in EU** |
| **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)

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

PD = Personal Data (EU)

### Differences

<table>
<thead>
<tr>
<th>Rights</th>
<th>CaCPA</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>Rights</th>
<th>CaCPA</th>
<th>EU GDPR</th>
</tr>
</thead>
</table>
| Accountability | • No explicit record-keeping requirements  
• However requires **tracking infrastructure of data collection & processing streams** to identify CA residents & flag PI to honor disclosure requests & opt-in/out choices | ▪ Requires a **DPO**  
▪ Requires **local representative** under certain conditions  
▪ Requires **data & processing inventory justified by legitimate interest** for collection, use, sharing & retention  
▪ Requires **demonstrable proof of compliance** that can be requested by a DPA at any time  
  ▪ some relief for controllers with less than 250 employees |

DPO (Data Protection Officer, a GDPR SME)

### Differences

<table>
<thead>
<tr>
<th>Subject</th>
<th>CaCPA</th>
<th>EU GDPR</th>
</tr>
</thead>
</table>
| **Cross-border transfer requirements** | • No adequacy determinations for transfer to other states/countries  
• No X-border transfer mechanisms | • 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)  
• Local representative required under certain conditions |
| **Fines**                     | • CA AG may impose civil penalties of up to $7,500 per intentional violation - no cap on total amount of penalty  
• Private right of action for breaches with $100-$750 statutory or actual damages  
• 30 day cure period (for statutory damages under private actions) | • Tiered penalty system – violations may result in fines up to €20M or 4% of total worldwide annual turnover, whichever is greater  
• Private right of action for actual damages |

SCCs = Standard Contractual Clauses, aka Model Clauses (EU)

### Differences

<table>
<thead>
<tr>
<th>Rights</th>
<th>CaCPA</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”  
• 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.)  
• 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; 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” |

### Rights

<table>
<thead>
<tr>
<th>Rights</th>
<th>CaCPA</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 have generally applicable right to have PI deleted (rulemaking may provide more guidance) • Exceptions: (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>• Data subjects have right to have PD deleted where (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” • Exceptions: (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>
</tbody>
</table>

Roadmap to CaCPA Compliance
GDPR Lessons Learned
Apply lessons learned from GDPR

- Analyze whether the CaCPA applies to you

- Prepare to comply prior to enforcement
  - 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
Apply lessons learned from GDPR

- **Data inventory, mapping & tracking infrastructure** are essential

- **Start service provider & 3rd party inventory & management early**
  - Vendors, marketing partnerships & co-branded relationships, data brokers & others
  - Assess & **update agreements** to address compliance requirements, e.g. to avoid “sale” of PI to provide liability safe harbor
Apply lessons learned from GDPR

- Understand *compliance will take longer than you believe*, e.g. tagging & tracking data elements, fulfilling data subject rights

- Expect **uncertainty** until common understanding evolves

- Significant **fines & class action lawsuits** await the non-compliant

- Leverage *counsel & operational-oriented consultants & 3rd party compliance tools* to gain needed expertise, avoid re-inventing the wheel & save time
Action plan

1. Prepare/maintain **data maps, data inventories or other records** of CA residents’ PI re: households, devices, data sources, storage locations, usage & recipients

2. Develop & implement **data tracking infrastructure** to fulfill data disclosure requests.

3. **Inventory** & maintain all **external resources & update agreements** re: compliance with CaCPA
   
   a. Start due diligence process early - some 3rd parties may need to be replaced for noncompliance or raising pricing

4. Update **privacy notices** to add newly required disclosures re: consumer rights & update **at least semi-annually**
   a. Provide **clear, conspicuous “Do Not Sell My Personal Information” link** on business’ Internet homepage, directing users to web page & toll-free phone# enabling them, or someone they authorize, to opt out of sale of resident’s PI
      i. CA’s Shine the Light Law also requires website homepage link to “Your California Privacy Rights”

5. Update **privacy policies** re: data access, deletion & portability rights fulfillment & other CaCPA obligations
   a. Develop **play-book for standard communications** to be sent to individuals requesting to exercise their rights

6. Establish **tracking infrastructure of data collection & processing streams** to identify CA residents & flag PI to honor disclosure requests & opt-in/out choices

   a. Tag & classify every existing data element in 11 PI categories
      
      i. When & how collected in last 12 months; with whom shared; where located & how long
      
      ii. Identify consumer data may sell, segregate into categories & ensure no data of CA residents who opted out is sold

   b. Record opt-in/out, date/time stamp & authentication

   c. Analyze **legal basis for collecting & processing PI** to explain rationale for exemptions to consumer’s right to deletion
      
      i. E.g., big data analytics & artificial intelligence algorithms that leverage PI

Action plan

7. Make available **designated methods** for submitting requests for data disclosure & deletion requests, including a toll-free phone# & website
   a. **Train workforce members** re: rights & rights requests/opt-outs, proper authentication, etc.

8. Provide **data access & portability** capabilities to consumers (portal?)

Action plan

9. **Fund & implement new systems & processes** to comply with new requirements:
   a. **Verify identity & authorization** of persons who make requests for data access, deletion or portability
   b. **Standardize** process for **handling & responding** free of charge to consumer requests for PI
      i. **Respond to rights requests** for data access, deletion & portability within 45 days
   c. **Avoid requesting opt-in consent for 12 months** after CA resident opts out

Action plan

10. Comply with **opt-out** requests to data sharing

11. **Determine age of CA residents** to avoid charges of "willfully disregard(ing) CA resident’s age"
   
   a. Implement processes to secure consent of parental or guardian for minors under 13 years & affirmative consent of minors between 13 & 16 years prior to data sharing for business purposes
   
   b. Can provide consent form to be signed by parent/guardian & returned via U.S. mail, fax, or electronic scan

Action plan

12. Establish **policy & training**, and **evaluate** existing practices:
   a. **Marketing**
   b. **Sale of PI**
   c. **Discriminatory pricing & services**
   d. **De-identification rules** and 4 safeguards

Establish Governance for Program Sustainability and Defensibility Including Data Mapping of DPLC
Privacy Risk Management & Control Framework
Modeled after DOJ, OIG, U.S. Sentencing Guidelines for Compliance & COSO for Risk Mgmt

Leadership:
Organizational Governance & Accountability

Risk Management:
Continuous Privacy-by-Design & Periodic Risk Assessment

Standards & Controls Governance:
Policies, Data & Resources, HR, External Resources Management

Monitoring, Detecting & Response

Training, Awareness & Communications

This lifecycle management process facilitates continually strengthening the program. The framework should drive the organization of internal privacy policies – details follow.
## Privacy Risk Management & Control Framework

<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  
• 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 |
| **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

### Privacy Program

- Data & resource mapping
- Governance structure
- PI sensitivity classification
  - drives strength of controls
- **Risk management**: P/SbD, periodic
- Sanctions & complaints
- External resource management
- Monitoring, auditing & oversight
- Incident & breach management & response

### Privacy Practices

- Data privacy lifecycle controls
  - notice, data collection, use, sharing & retention controls
- Data subject rights & choices
  - data infrastructure & management
- Data minimization (avoid re-identification)
  - e.g. min. necessary, key coding, de-identification, pseudonymization
- Verification & authentication

### Security Practices

- Administrative safeguards
  - e.g., RBAC design, authorization & periodic review
- Physical controls
  - e.g., review of facility’s physical controls
- Technical controls
  - e.g. use of encryption
- Engineering controls
  - e.g. implementation of Privacy/Security-by-Design/SDLC

### 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**
Can someone briefly define information governance?
Governance is a system of policies & processes whereby company activities are directed & controlled to assure sustainability & defensibility (NIST “Repeatable”)

How do you direct & control?

- Clear roles & responsibilities defined in policies & training
  - When someone terminates & leaves such a role, a responsible executive/governance committee must immediately identify a replacement to avoid loss of operational continuity
External Resource Management means governance of service providers & 3rd parties under CaCPA
Other related governance scopes include M&A, system architecture, change management, project management, etc.
Organizational Governance

“Tone at the top” (regulators look for evidence of organizational commitment, support & resources) & an organizational structure w/ clear roles & responsibilities

- **Board of Directors** – periodic oversight reporting to fulfill fiduciary duty

- **Governance Committee/Responsible Executive** - guidance, commitment & support

- **Privacy & Security Officials** - high enough level with authority to independently act without interference, e.g. CPO/CISO or direct/dotted line report to Responsible Executive
  - Mitigate any inherent conflict of interest (multiple hats) & “fox guarding the hen-house” reporting

- **Implementation Working Group** - follow up on prioritization & implementation of corrective actions/mitigation plans & report on behind-projects to Committee

- **Domain Owners** - responsible under oversight of Officials via direct/dotted line reporting
  - **Security**: physical security, technical security, engineering security & HR security
  - **Privacy**: operational privacy practices (e.g. administration of patient rights) & legal privacy (e.g. notices, consents, government requests)

- **Functional liaisons** – assist with PbD in larger organizations
Governance through Policy
Ensure policies clearly enable all the other governance components

Clearly define in policy:

- Risk management & control framework
- Applicable standards (HIPAA, HITRUST, ISO 27001/2:2013, Top 20 CSCs)
- All roles/responsibilities [Steering Committee, Responsible Executive, Privacy / Security Officials, Domain Owners, Implementation Working Group, management, customer contact personnel, IT, engineering, Resource Owners / Custodians, product/project managers, workforce members (with access to PI) & users (others without access to PI but who can compromise network)]
- Who is responsible for executing what processes, when or frequency, & what oversight (approvals, separation of duties, & monitoring) is required (major weakness in many company policies)
- Document revision, approval & versioning control, & annual review
HR Governance

Ensure policy & practices clearly enable HR’s role in all 4 stages

Operational recommendations

☐ Pre-onboarding – Question: Why this state?
  - Conduct criminal background checks
  - Signed attestation of having read, understood & agreed to AUP/confidentiality agreement

☐ Onboarding
  - New hire privacy/security awareness (workforce members) & cybersecurity training (users)
  - On-the-job specific (management checklist) & roles-based privacy/security training
HR Governance

Ensure policy & practices clearly enable HR’s role in all 4 stages (continued)

- **Employed**
  - Annual privacy/security (workforce members) & cybersecurity training (all users)
  - Annual policy/procedure review/attestations (might be handled by doc control function)
  - Properly handle RBAC rights during role changes
  - Consistent sanctions enforcement & documentation re: events, incidents and breaches

- **Termination**
  - Proper termination of access, including cloud-based services & equipment return
  - Tightly manage terminated employees converted to temporary consulting roles
Data Privacy Lifecycle (DPLC) & Resource Governance

Map DPLC processes & data locations for proper governance & PbD of processes & resources

- **Data map each unique end-to-end DPLC identifying**
  - Data inventory
  - Resources (data locations)
  - Resource Owners/Custodians

- **Ensure DPLC practices are consistent with privacy notice** to avoid a deceptive trade practice & reputation/brand damage
Data Privacy Lifecycle (DPLC) & Resource Governance

- Designate Data Map Owners responsible for:
  - Ensuring accuracy of data diagrams & related resource maps
  - Identify planned changes:
    - DPLC practices - Notify Privacy Official & Legal
    - External Resources - coordinate with Privacy/Security Officials:
      - Privacy/Security-by-Design of all Resources, e.g. RBAC, encryption, etc.
      - Proper due diligence, contracting & periodic monitoring of external resources
Data Privacy Lifecycle (DPLC) & Resource Governance

- Inventory/document all DPLC sub-processes

- Validate/record legitimate/business purpose for all DPLC sub-processes in risk register
  - Data collection
  - Data access
  - Data use
  - Data sharing
  - Data retention
  - X-border data transfers

- Stop non-compliant processes
- Remove non-compliant data
Problem: A Forrester report of 150 data security professionals published in January 2017 reveals

- 76% believe their organization has a “mature or very mature” data security strategy, yet “most companies struggle to encrypt data, audit it for abuse, enforce a strict least privilege model, classify it, and even understand where it’s (data is) located” be it on premises, at third parties or in the cloud.

*If you don’t know where your data is, how can you protect it?*

Source: The Data Security Money Pit: Expense In Depth Hinders Maturity
- https://info.varonis.com/hubfs/docs/research_reports/Varonis_TLP.pdf
Data Mapping

- Develop data flow, inventory & resource map every unique data privacy lifecycle (DPLC)

- Should be a formalized, repeatable process
  - Designate who is responsible for ensuring this is done
  - Identify & inventory what PI is collected, used, shared, stored & disposed
  - Classify highest level of data sensitivity (based on data inventory) in each resource
  - Identify what data is transferred
  - Inventory all resources
  - Assign resource owner & custodian to each resource for governance purposes (segregation of duties)
Data Mapping Process

- Identify & interview process/functional SMEs re: core end-to-end DPLC process & practices
  - Focus interview questions on “following the data flow”
  - Conduct deeper-dive analysis in PIA/DPIA report

- Interview sessions require 4-6 hours
  - Discussions often “breakdown communication silos” between SMEs resulting in:
    - better understanding of end-to-end DPLC process & resources
    - identifying process improvements & control strengthening
**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>Notice</td>
<td>Data Collected</td>
<td>Data Used / Processed / Accessed</td>
<td>Data Used / Processed / Accessed</td>
<td>Data Used / Processed / Accessed</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
## Privacy Data Mapping SIPOC

**Process Name:** PHI/PII/PIE Processing Sample

**Process Owner:** [Privacy Official or delegate]

**Revision Date:** 13 Mar 2016

### Process Steps

<table>
<thead>
<tr>
<th>S</th>
<th>Data Suppliers / Sources</th>
<th>Location From / Data State</th>
<th>I</th>
<th>Data Inputs</th>
<th>P</th>
<th>Data Flow Steps</th>
<th>O</th>
<th>Data Outputs</th>
<th>C</th>
<th>Location To / Data State</th>
<th>Data Customers / Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Clinic / Practice</td>
<td>US / INTL</td>
<td>I</td>
<td>Signed Consent</td>
<td>P</td>
<td>Notice</td>
<td>O</td>
<td>Signed Consent</td>
<td>C</td>
<td>Locked File cabinet, Scanned to:/Shared Folder:/consents/month-Year</td>
<td>Legal</td>
</tr>
<tr>
<td></td>
<td>Clinic / Practice</td>
<td>FedEx / UPS</td>
<td></td>
<td></td>
<td></td>
<td>Receive Sealed Sample Kit</td>
<td></td>
<td></td>
<td></td>
<td>Receiving Area</td>
<td>Accessioning</td>
</tr>
<tr>
<td></td>
<td>Accessioning</td>
<td>Receiving Area</td>
<td>I</td>
<td>sample kit w/Patient name, activation code</td>
<td>P</td>
<td>Open Kit: Assign barcode to sample</td>
<td>O</td>
<td>sample kit w/Patient name, activation code, barcode (accessionNo)</td>
<td>C</td>
<td>Lab Work Bench</td>
<td>Lab</td>
</tr>
<tr>
<td></td>
<td>Lab</td>
<td>Lab Work Bench</td>
<td>I</td>
<td>sample w/Patient name, barcode, activation code</td>
<td>P</td>
<td>Lab Processing</td>
<td>O</td>
<td>sample w/Patient name, barcode, activation code; raw output</td>
<td>C</td>
<td>Sample into freezer, SAN storage Array</td>
<td>Data Processing</td>
</tr>
</tbody>
</table>
Sample Data Flow Diagram

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

PHI/PII Processing Sample Data Flow Diagram

Legend:
- Green path is the "happy path" of report delivery.
- Dark Red is 3rd parties that receive PHI/PII
Data Resource Map

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

<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><strong>Resource owner</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resource custodian</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data inventory</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Data identifiers</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Highly sensitive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Sensitive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Slightly sensitive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Non-sensitive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 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.
Privacy Rights Governance

- **Designate:** (accountability)
  - Privacy rights’ **process owner** responsible for proper compliance execution
  - Appropriate **roles & responsibilities for fulfilling** privacy rights in policy

- Establish **data tracking infrastructure** & disclosure/deletion processes
  - Identify **all pieces of consumer PI, including across 3rd parties**, to fulfill disclosure/deletion requests & ensure accurate privacy notice
  - Identify reasons for not taking action & any rights to appeal

- Establish privacy **rights fulfillment processes** in policy: access, deletion
  - **Map** privacy rights fulfillment processes
  - Establish **methods** for submitting requests: toll-free PH#, Web portal
  - Define methodology for **verifying** requesting consumers **without undue hindrance**
  - Identify reasons for not taking action & any rights to appeal
  - Define readily useable **format** for data portability **without hindrance**

- Establish review of **potential discriminatory** pricing/services practices

- **Train** appropriate staff responsible for handling rights inquiries, requests & fulfillment
Privacy-by-Design Governance (incorporates Security-by-Design)

Purpose: Establish a system whereby foreseeable risks are identified & acceptably mitigated as a part of day-to-day decision-making (ERM model)

- Designate for each resource identified during data mapping
  - Resource Owners responsible for RBAC design, authorization of RBAC rights to individuals, & periodic review of all RBAC rights
  - Resource Custodians responsible for implementation of authorized RBAC rights & providing reports of all users & their respective RBAC rights for periodic review by Resource Owner

resource = data location
Privacy-by-Design Governance (incorporates Security-by-Design)

- **Designate individuals** (in policies/training) responsible for anticipating privacy & security **risks** related to new/enhanced **resources** & working with Officials to properly design, develop & test controls to acceptably mitigate risk prior to roll-out (use a PIA tool)
  - **Resource Owners** in collaboration with engineering/SQA management
  - **Project/product managers**/business/systems analysts in collaboration with engineering/SQA management
    - Educate engineering/SQA re: **OWASP Top 10 & other security vulnerabilities**
Privacy-by-Design Governance
Operational recommendations – incorporates Security-by-Design

- Incorporate Privacy-by-Design strategies into new / enhanced resources prior to release
  - Privacy-by-Default
  - DPLC & resource management
  - Maintain data tracking infrastructure & management
  - Data minimization
  - Security-by-Design
The PIA
Pre-CaCPA

Privacy Impact Assessment

Tool to be used during the (design phase) of a new:
- Resource
- Process
- Vendor relationship
- Application
- Service
- Business Model

<table>
<thead>
<tr>
<th>Check Y or N</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. What specific types of PHI / PII (PII) are collected? Please describe:</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>a. Is this PII not currently being collected? If so, notify Chief Privacy Officer (CPO). Identify if data crosses international borders to CPO.</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>b. Any change to where / how PII is collected? If PII is not collected from individual directly, identify collection source.</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>c. If PII will be collected on a new resource, has log data been sufficiently enabled to identify logon info, and who and what specific PII were accessed in the event of a compromise?</td>
</tr>
<tr>
<td></td>
<td>2. Describe the purpose / use for which the PII is being collected.</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>a. Is this use consistent with consent / Notice of Privacy Practices / mobile or web privacy notice? If this is a change, notify CPO to update same or create a specific consent or authorization.</td>
</tr>
<tr>
<td></td>
<td>3. Where is the PII going to be held / stored (resource)?</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>a. Does this represent a change to where PII is currently stored? If so, notify Information Security Officer (ISO).</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>b. Did the resource owner design RBAC roles and authorize who shall be granted RBAC rights? Identify the responsible resource owner.</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>c. Identify if any currently unauthorized individuals will need to have access to this PII?</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>d. Did the resource custodian develop privacy / security-by-design requirements for this resource? Identify the resource custodian.</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>e. Was either the CPO or ISO consulted re: the privacy / security-by-design requirements?</td>
</tr>
<tr>
<td></td>
<td>4. How long will this PII need to be stored to fulfill its business purpose? Identify when it will be destroyed and what triggers this process?</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>5. Will this PII be shared with / transmitted to a 3rd party? Please describe:</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>a. If this is a service provider / Business Associate (BA), did CPO conduct Information Security due diligence and approve the BA? If not, notify CPO.</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>b. If the data is PII, can it be de-identified or encrypted? Describe.</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>c. How will PII be protected, including preventing leakage in 4 data states?</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>i. Data-at-rest - describe:</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>ii. Data-in-motion - describe:</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>iii. Data-at-endpoints - describe:</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>iv. Data-at-disposal - describe:</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>c. Will Privacy/Security-by-Design be documented as a part of the design requirements and implementation, and properly tested for prior to roll-out?</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>d. Will SQA develop appropriate use cases to properly test this functionality?</td>
</tr>
<tr>
<td>□ Yes □ No</td>
<td>e. Will test data be anonymized or masked? If not, discuss with CPO.</td>
</tr>
</tbody>
</table>
Governance: Risk Ownership

- **Risk owners own risks inherent in their people, process & technology**
  - Identified in data flow, inventory & resource/locations mapping

- **Executives should assign owners to resources w/in organizational control** (or by default become owner for such resources) & **inform** PO/SO, so resources & owners can be **recorded in resource map**

- **Product/project managers** in collaboration with **engineering** are primarily **responsible for Privacy-by-Design of resources**
Governance: Risk Ownership

- **Resources:**
  - Products/services, processes, apps/software, databases, internal/external systems, technologies
  - External resources: service providers & 3rd parties

- **Resource Owners** are responsible for ensuring **RBAC design**, *authorizing* RBAC **rights**, & *periodically reviewing* RBAC **rights** for accuracy

- **Resource Custodians** are responsible for implementing *authorized* RBAC **rights** & providing **reports** of all rights for periodic review by resource owner
External Resource Management Governance

Purpose: Develop system for properly qualifying & managing service providers & 3rd parties with access to customer/employee PI

- Designate **External Resource Mgmt Coordinator** responsible to:
  - Approve **Data Minimization** strategy for intended purpose
  - Ensure proper **due diligence** assuring satisfactory security program in place
  - **Proper contracting** utilizing standard agreement customized to add: security official; necessary safeguards re: business arrangement; incident notification timeframe & responsibilities; right to audit; BC/DR plans; how data handled at termination of agreement; & indemnification
  - **Periodic review** based on data sensitivity & observed poor patterns of practice
  - **Document in a “external resource database”** the rationale behind: (documentary evidence)
    - Whether external resource has PI & level of data sensitivity
    - What due diligence was performed
    - How frequently the periodic review should be performed
Privacy/Security Officials should:

- Define in policy **acceptable security due diligence requirements** based on data sensitivity
- Agree on standard **external resource agreement template** re: privacy/security obligations/requirements & **establish governance over changes to template**

Note:
- Privacy Official or General Counsel may serve as external resource mgmt. coordinator for SMBs
- In larger firms, this is supply chain/procurement manager
Event, Incident & Breach Response Governance

Requires Privacy & Security Official collaboration

Purpose: Establish in policy/practice a response plan for events, incidents & breaches, including Sanctions

- Communicate what events should be reported to whom in policy/training
  - Use anonymous compliance hotline poster/exit interviews

- Have clear incident response plan with defined roles & duties BEFORE an event occurs
  - Who to call (e.g. law enforcement, data breach vendors) with contact information
  - Understand when to bring in expert privacy counsel (prior to forensics)
  - Use table-top/simulation exercises to ensure everyone understands their role
Event, Incident & Breach Response Governance

Requires Privacy & Security Official collaboration

- **Documentation** requirements
  - Use **standardized log of all events** (trend analysis) & investigation report
  - Thoroughly investigate & address immediate/long-term mitigations, including any sanctions, with a sense of urgency (Yahoo is the poster child of what not to do)
  - Properly document & centrally archive
  - Expect documentation to be reviewed by external parties

- **Review incidents for lessons learned**
  - Understand trends, make changes as necessary (change in policy, risk mitigation &/or training)
Question...

Can someone describe the difference between a privacy & security incident?

- What are examples of each?
## Event vs. Incident vs. Breach

<table>
<thead>
<tr>
<th>1. <strong>EVENT</strong></th>
<th>2. <strong>INCIDENT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy:</strong> <strong>Observable</strong> privacy / Infosec <strong>issue</strong>, e.g., a <strong>violation of policy</strong>, must be reported to Privacy/Security Officials</td>
<td><strong>Policy:</strong> <strong>Attempted or successful unauthorized access, use, disclosure, modification, or destruction</strong> of information <strong>or interference with system operations</strong> in an information system</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. <strong>Reportable BREACH</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>California:</strong> <strong>Non-encrypted/non-redacted</strong> PI subject to unauthorized access, exfiltration, theft or disclosure” due to a <strong>failure</strong> to implement &amp; maintain reasonable security procedures</td>
</tr>
<tr>
<td><strong>HIPAA:</strong> Acquisition, access, use, or disclosure of <strong>unsecured PHI</strong> not permitted by Privacy Rule <strong>which compromises</strong> security or privacy of PHI – based on 4 risk factors</td>
</tr>
<tr>
<td><strong>CMIA:</strong> <strong>Unauthorized</strong> access, use or disclosure of PHI [Confidentiality of Medical Information Act]</td>
</tr>
</tbody>
</table>
Monitoring & Evaluation/Auditing Governance

Purpose: Establish in policy mechanisms for periodic evaluations/monitoring, reporting of findings & overseeing timely implementation of corrective actions/mitigation plans

- Define activities in policy, assign ownership & calendarize
  1. Regular, timely patching
  2. Periodic risk assessment & controls evaluation
  3. Periodic vulnerability scans & penetration tests
  4. Periodic code reviews
  5. Periodic RBAC rights review
  6. Periodic hardware/software inventory reconciliation
  7. Periodic review of access points & wireless
  8. Periodic external resource due diligence based on data sensitivity
  9. Periodic incident response desktop exercise &/or simulation
  10. Periodic testing of Business Continuity & Disaster Recovery plans
Develop & implement **near real-time 24/7 incident detection** of internal & external threats

Develop “**risk management & control implementation plan**” that prioritizes & tracks implementation of tasks identified during periodic monitoring & evaluations
- Working Group should use a **risk & gap register**

Define in policy provision of & ownership for **periodic accountability** reporting to Board of Directors, Responsible Executive/Governance Committee
Documentation Evidence of Governance
Facilitates oversight & demonstrates compliance / legal defensibility

- All governance practices & processes should be documented in a standardized manner that facilitates easy oversight review by Officials.

- All identified risks & gaps should be recorded in a risk & gap register & actively prioritized & managed to timely & complete implementation.

- Maintain evidentiary documentation of compliance for 7 years (class action lawsuits) after later of the date of their creation or last effective date, unless a longer timeframe is required by law or regulation.

- Establish restricted “centralized privacy/security repository”, so all related information is housed in the same place (oversight / investigation preparedness).
  - Appropriate sub-folder examples include: event & incident reporting; sanctions; periodic RBAC reviews; training participation sign-up sheets & presentations); Privacy-by-Design/PIA; Steering Committee minutes & reports; Implementation Working Group reports; risk assessments; controls evaluations; vulnerability scans & pen tests; etc.
In sum: Governance & Maturity Tips

- Establish **budget** for foreseeable 2019 costs

- Assemble a **collaborative, cross-disciplinary team** to work across the enterprise

- Integrate **Privacy/Security-by-Design** with engineering/development

- Integrate new required operational practices **into existing policies/SOPs**

- **Train** all appropriate staff

- Ensure ownership, **governance & roles/responsibilities** are well defined & communicated for sustainability (NIST’s repeatability) - beware of “**conflicts of interests**” & “**separation of duties**”

- Establish **monitoring/oversight of key activities** for repeatability

- Implement **periodic self-assessment or audit** to evaluate compliance gaps & ensure sustainability & maturity

- **Document** decision-making, monitoring, evaluations/assessments in a compliance repository demonstrate accountability - ensure **investigational preparedness** to timely & comprehensively respond

- **Consulting & Legal** - seek SME advice & support

  Modify **data monetization business models**

  Brace for **additional penalties & liquidated damages**
General Privacy Takeaways

- Privacy is customer expectation & thus functional requirement (PbD)

- Privacy professionals provide important role in operationalizing privacy to achieve repeatability & aspire for legal defensibility
  - Generally privacy counsel provides guidance & support

- Privacy governance can be effectively coordinated with security governance

- Privacy professionals serve as customer advocate with a lot of autonomy

- Technology explosion & GDPR/CaCPA will spur dramatic growth of privacy professionals

- If your organization does not have a privacy function, consider learning & filling the gap – if it does, learn & offer to assist privacy official (mentor)
IAPP Certifications
https://iapp.org/certify/programs/

- **CIPP/US**
- **CIPP/E** – EU (GDPR)
- **CIPP/C** – Canada
- **CIPP/A** - Asia
- **CIPP/G** - Government
- **CIPT** – Privacy Technologist (PbD)
- **CIPM** – Privacy Management (program management)
In Sum
Summary

- California is on *bleeding edge* of Privacy in U.S.
- CaCPA re-enforces Californians’ right to privacy
  - Provides consumers an effective way to control their PI
  - Right to know, delete, opt-out, access/portability & anti-discrimination
  - *Don’t Wait* – There is less time than you think to become compliant as anyone who has worked on GDPR compliance knows full well
ANY FINAL QUESTIONS?

If you would like to have any of our whitepapers or other documents, please note which ones on your business card and provide it to us or let us know

- Data Mapping
- PIA
- Requested Documents List
- Legally Defensible
- RBAC

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

Neil R Packard, CISA
npackard@socalprivacy.com
619.208.2529

www.socalprivacy.com
Appendix
Supplemental Analysis
About Us
# NIST Risk Management ("RM") Implementation Tiers

<table>
<thead>
<tr>
<th>Tier</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>PARTIAL</strong></td>
</tr>
<tr>
<td>Risk Management Process</td>
<td>Informal, ad-hoc (and sometimes reactive) RM practices. Prioritization of RM may not be directly informed by organizational risk objectives, the threat environment, or business requirements.</td>
</tr>
<tr>
<td>Integrated RM Program</td>
<td>Limited RM awareness. RM implemented on an irregular, case-by-case basis. Processes do not enable risk information to be shared within the organization.</td>
</tr>
<tr>
<td>External Actions</td>
<td>No processes in place to share information with other entities.</td>
</tr>
<tr>
<td>2</td>
<td><strong>RISK INFORMED</strong></td>
</tr>
<tr>
<td>Risk Management Process</td>
<td>Management approved RM practices are not established policy. Prioritization of RM is directly informed by organizational risk objectives, threat environment, or business/mission requirements.</td>
</tr>
<tr>
<td>Integrated RM Program</td>
<td>Risk awareness but informal RM. RM procedures are implemented. Staff has adequate resources to perform their RM duties. Risk information is informally shared within the organization.</td>
</tr>
<tr>
<td>External Actions</td>
<td>Awareness, but no formalized capabilities to interact and share information externally.</td>
</tr>
<tr>
<td>3</td>
<td><strong>REPEATABLE</strong></td>
</tr>
<tr>
<td>Risk Management Process</td>
<td>Formal RM practices in policy. RM practices are regularly updated based on changes in business requirements and a changing threat and technology landscape.</td>
</tr>
<tr>
<td>Integrated RM Program</td>
<td>Formal RM and policies/procedures are implemented/reviewed and respond effectively to changes in risk. Personnel possess knowledge/skills to perform appointed roles/responsibilities.</td>
</tr>
<tr>
<td>External Actions</td>
<td>Understanding of dependencies and collaborates and receives information with other entities.</td>
</tr>
<tr>
<td>4</td>
<td><strong>ADAPTIVE</strong></td>
</tr>
<tr>
<td>Risk Management Process</td>
<td>Lessons learned and predictive indicators inform RM practices. Actively adapts to a changing risk landscape and responds to evolving/sophisticated threats in a timely manner.</td>
</tr>
<tr>
<td>Integrated RM Program</td>
<td>RM is part of the culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on systems/networks.</td>
</tr>
<tr>
<td>External Actions</td>
<td>Collaborate to ensure accurate, current information to improve RM actions before events occur.</td>
</tr>
</tbody>
</table>
Key amendments – integrated into this deck

Does not address all of the ambiguities & uncertainties of the law

- Exempts data regulated by HIPAA/CMIA, GLBA & DPPA, including service providers & ecosystem partners that handle regulated data
  - However these regulated industries remain subject to data breach class action provisions of CaCPA
    - Makes more complex: data breach risk mitigation planning & service provider agreement negotiations
    - Distinguish carefully between federally regulated data & other types of PI
  - Added new exemption: clinical research subject to Federal Common Rule

- Limits broad 1st Amendment exception to apply only to “non-commercial” activities
  - Says nothing about whether news reporting by media company is non-commercial activity
    - Future clarification may include “newsgathering”
  - Attempt to avoid interpretations of entities having 1st Amendment rights to communicate PI to other entities
    - May be more vulnerable to 1st Amendment challenges re: commercial speech and fully protected speech theories
Key amendments – integrated into this deck

*Does not address all of the ambiguities & uncertainties of the law*

- Clarifies fines for violations: $7,500/intentional & $2,500/unintentional (previously $7,500 could be sought for a violation)

- Enforcement & right to sue (2 of most controversial elements)
  - Removes requirement for consumer to notify AG prior to suing (so called “gatekeeping” function)
  - Clarifies right to sue exists only for data security breaches

- Grant 6-mos. grace period before enforcement when AG issues rulemaking or July 1, 2020 whichever is earlier. Extension only applies to privacy requirements of the law & does not pertain to breach class action provisions (including availability of statutory damages), which will go into effect on Jan. 1, 2020
  - If regulations are issued on or before July 1, 2019, an unlikely occurrence since AG has been given an extension to develop those regulations until July 1, 2020, there will be no 6-mos. grace period
### 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 |
| Right to (request) deletion | right to request **deletion of PI collected** from business servers & service providers upon receipt of a verified request with some exceptions |
| Right to opt-out of “sale” | right to **say “no” to sale** of PI (or for children under 16, right to no have PI sold absent parent/guardian opt-in) |
| Right of access & data portability | right to access to **specific pieces** of PI in format allowing transfer to another entity |
| Right to equal service & price (anti-discrimination) | right to receive **equal service & pricing, even if exercise rights**, but does permit offering financial incentives if reasonably related to value provided by consumer’s data |

**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)
CaCPA impacts for marketers & marketing
No distinction between PI held in B2B relationship vs. B2C (unlike CAN-SPAM)

- Reconsider use of 3rd-party PI that must be revealed via right’s request
  - PI beyond what is publicly available & not published online by consumer
  - 3rd-party recipients can not sell PI sold to 3rd party unless consumer received explicit notice & opportunity to opt out (affects data brokers)

- Reevaluate data fields on forms & profiles due to transparency disclosures

- Utilize data-minimization principles to mitigate private right-of-action risk

- Figure out how to identify, locate & delete PI

- Think carefully before selling information about customers or users
  - Must maintain record of sales for 12 mos. & provide clear & conspicuous link on website labeled Do Not Sell My Personal Information to opt-out
  - Selling PI of children 16 years old & younger has more requirements
  - Failing to honor such requests can result in significant penalties from CA AG

Employee data compliance activities

Amendments/rulemaking may modify/clarify, but start planning compliance activities

- Map employee PI: job applicant, benefits, prof. & employment-related info (e.g., comp., perf. reviews)
- Disclosures in employee privacy notices, handbooks, posters in common areas/breakrooms
- Opt-out notices for sale or sharing of PI for valuable consideration
  - Exception: PI transfers to 3rd party re: corporate transactions/bankruptcy
- Honor employee rights to: information re: PI collection & disclosure; access to PI; request deletion of PI
- Avoid discriminatory employment practices re: termination, declining promotion opportunities, offering different terms of employment
- Establish governance over employee PI (policy, training, etc.)
  - Create/update record retention policy & practices explaining legal obligation (e.g. 3 years under Fair Labor Standards Act, 4 years IRS tax record regulations)
  - Inventory/update service provider contracts (e.g. prohibit “retaining, using, or disclosing PI for any purpose other than for the specific purpose of performing the services”; require cooperation with actionable employee access and deletion requests)
  - No breach exception for good faith acquisition of PI by employee or agent, e.g. mishandling

Key changes proposed by industry associations/lobbyists

Some of these proposed changes are addressed in the Amendment, many others are not

- Delay implementation to 12 months after AG’s rulemaking
- Remove employees/contractors and commercial/non-residential customers of a business from definition of consumer
- Clarify: PI is limited to information “linked or reasonably linkable” to a particular consumer, not information that relates to or could be associated with a consumer; and explicitly exclude de-identified, aggregate, pseudonymized consumer information to permit a business to collect, retain, sell or disclose such consumer information (also clarify definition of de-identified information)
  - Remove references to: household, devices and family; “probabilistic identifiers”; inferences and tendencies; Professional or Employment-Related Information; thermal, olfactory
  - Strike “specific pieces of PI” and refer only categories of PI regarding right to request
- Clarify should not “unreasonably” discriminate against consumer; add may incentivize “retention” of PI
- Clarify scope of GLBA, FCRA and DPPA exemptions by removing “if it is in conflict with that law”
- Clarify that covered entities and business associates are exempted, not simply PHI, under HIPAA, CaCMA (Confidentiality of Medical Information Act) and “Common Rule” (Federal Policy for Protection of Human Subjects)
- Permit 45 days to implement opt-out request for sale of PI
- Provide method flexibility for facilitating portability (remove toll-free phone#; add online portal/Web page)
- Remove “business shall not require consumer to create an account to make a verifiable request”
- Removes willful disregard of consumer’s age as deemed as actual knowledge
- Clarify private right of action relates only to a data breach and that CA AG is exclusive enforcer
- Safe harbor to data breach liability encouraging strong security

https://regmedia.co.uk/2018/08/21/ca-privacy-act-big-tech.pdf
CA AG Xavier Becerra’s 5 primary concerns

Expressed in 8/22 letter to CA State Assembly & Senate leaders

1. CaCPA requires AGO to provide (legal) opinions to any business or third-party as well as warnings and opportunity to cure before enforcement
   a. States is a potential conflict of interest; wants this corrected - however, EU DPAs provide such advice

2. Civil penalty provisions are potentially unconstitutional
   a. States cannot be amended through legislation (was created by voters via Prop 64); has offered corrective language

3. Unnecessary requirement for private plaintiff’s to give notice to AGO before filing suit
   a. States courts (not AG) determine merits of private lawsuit and imposes unnecessary personnel and administrative costs on AGO; thus should be eliminated

4. AGO has one year to provide rulemaking
   a. States AGO asked to become a regulator (rather than simply an enforcer) and no resources are provided and timeline is simply unattainable; wants increased resources and realistic timeline

5. CaCPA does not include a private right of action to seek legal remedies, but rather a limited right to sue if a victim of a data breach
   a. Argues the lack of a private right of action substantially increased need for new AGO enforcement resources; urges consumers be provide a private of action under CaCPA

GDPR - Brexit planning scenarios

Negotiations may necessitate: a) **data transfer mechanism** (SCC, BCR, approved Code of Conduct/Certification mechanism, Privacy Shield) if no adequacy finding for UK; and b) **alternative lead authority** for purposes of “one stop shop” and new BCRs

- **Brexit planning scenarios** – Eduardo Ustaran (see source below)
  - **Soft Brexit** – leaving EU with minimum possible impact – **20% odds**
    - Continued unhindered exchange of personal data between UK and EU
    - Ability of UK’s ICO (DPA) to participate in “one stop shop” mechanism
  - **Semi-soft Brexit** – adequacy fast-tracked, but no “one stop shop” – **40%**
    - In practical terms, ensures free flow of personal data between EU and UK
    - Probably allows ICO to be in involved in BCR authorization process
  - **Semi-hard Brexit** – UK would need to seek “adequacy”, knowing level of scrutiny would be meticulous (without regard to “special relationship”) – **30%**
    - As typical adequacy finding process takes several years, would require standard contractual clauses, BCRs or similar legal tool to fill this gap
  - **Hard Brexit** (“No deal Brexit”) – **10%**
    - Firmly closes door on adequacy finding and for a ICO role among fellow DPAs

- **Negotiations may necessitate:**
  - **data transfer mechanism** if no adequacy finding for UK, e.g. SCC, BCR, approved Code of Conduct/certification mechanism, Privacy Shield
  - **alternative lead authority** for purposes of “one stop shop” and new BCRs

Compliance vs. Risk Management

*Short-lived, myopic compliance vs. sustainable, long-term value ERM approach*

- Compliance is generally viewed as a cost, at best a necessary evil, and often involves using checklists and templates.

- ERM is about embedding risk management into strategy, culture, capabilities, and practices to create value and improve performance.
  - E.g., operational risk management is about improving operational performance to achieve stable, predictable outcomes.
  - Using the ERM framework and principles can help less mature organizations learn how to create sustainable privacy and security operational processes which can lead to applying the same ERM principles to managing their other risks over time.
  - COSO’s ERM Framework of 5 components and 20 principles seems simple. However embedding these into the DNA of an organization is hard and requires persistence over several years to reach a reasonably mature state.

- For more information:
  - [https://www.coso.org/Pages/erm.aspx](https://www.coso.org/Pages/erm.aspx)
**LEAN: Data sensitivity drives a risk-based approach**

*Determine strength of controls based on data sensitivity levels*

<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></td>
<td>1st name/initial &amp; last name plus any of following: gov't issued ID # (SSN, passport ID#, state ID#, driver’s license#, tax ID#, birth/marriage certificate), W-2, health insurance ID#, genetic info (defined by GINA), medical/health info (medical history, physical/mental condition, test results, diagnosis, treatment/medications), background check info, biometric data/record or identifiers, digital signature, precise geo-location data user name/D or email address w/ password or common security question answers (mother’s maiden name, DOB, place of birth) financial acct # or payment card info plus any required security/access code or password</td>
</tr>
<tr>
<td>3</td>
<td><strong>Sensitive</strong></td>
<td>PII that does not fall into highly or less sensitive PII groups, such as other personally identifiable dates, vehicle ID/serial #, other unique ID#/characteristic/code, non-precise geo-location data, other personnel file info</td>
</tr>
<tr>
<td>2</td>
<td><strong>Slightly Sensitive</strong></td>
<td>published contact info: name plus address, phone#; email address, fax#, instant message user ID, URL address, IP address, photo/video/audio file, persistent device/processor/serial ID; any other PII used for marketing purposes (see CA’s “Shine the Light Law”)</td>
</tr>
<tr>
<td>1</td>
<td><strong>Non-Sensitive</strong></td>
<td>non-personal information, such as session identifiers/cookies</td>
</tr>
</tbody>
</table>

Examples – adjust processes based on data sensitivity levels, e.g. pre-contract due diligence and periodic monitoring of BAs, roles-based access controls (RBAC)
**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, <strong>real-time</strong> 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, <strong>periodic</strong> 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, and trained on.
- For lower risks, detective controls are adequate. Higher risks should have preventive and 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

Inherent Risk

Preventive Controls

Risk Event

Detective Controls

Net / Residual Risk
### Typical Standards & Controls

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CA Consumer Privacy Act of 2018, Amendments &amp; Rulemaking</td>
<td>• HIPAA/HITECH Security Rule</td>
</tr>
<tr>
<td>• HIPAA/HITECH Privacy &amp; Breach Notification Rules</td>
<td>• ISO/IEC 27001-2:2013</td>
</tr>
<tr>
<td>• Generally Accepted Privacy Principles (GAPP)</td>
<td>• Top 20 Critical Security Controls (CA AG requires)</td>
</tr>
<tr>
<td>• EU’s General Data Protection Regulation (GDPR)</td>
<td>• SEC OCIE Cybersecurity Initiative</td>
</tr>
<tr>
<td></td>
<td>• NIST Cybersecurity Framework methodology</td>
</tr>
</tbody>
</table>

**Privacy Program** (sustainable foundation)

- U.S. Sentencing, DOJ & OIG Guidelines for Effective Compliance (used to meet out penalties)
- COSO Risk Management Program Management
### Top 20 Critical Security Controls v.7 (3/19/18)
Brings more focus on authentication, encryption and application whitelisting

<table>
<thead>
<tr>
<th>Basic CIS Controls</th>
<th>Foundational CIS Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inventory &amp; Control of Hardware Assets</td>
<td>7. Email &amp; Web Browser Protections</td>
</tr>
<tr>
<td>2. Inventory &amp; Control of Software Assets</td>
<td>8. Malware Defense</td>
</tr>
<tr>
<td>3. Continuous Vulnerability Assessment &amp; Remediation</td>
<td>9. Limitation &amp; Control of Network Ports, Protocols &amp; Services</td>
</tr>
<tr>
<td></td>
<td>10. Data Recovery Capabilities</td>
</tr>
<tr>
<td></td>
<td>11. Secure Configuration for Network Devices, such as Firewalls, Routers &amp; Switches</td>
</tr>
<tr>
<td>5. Secure Configuration for Hardware &amp; Software on Mobile Device, Laptops, Workstations &amp; Servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14. Controlled Access Based on Need to Know</td>
</tr>
<tr>
<td></td>
<td>15. Wireless Access Control</td>
</tr>
<tr>
<td></td>
<td>16. Account Monitoring &amp; Control</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organizational CIS Controls</strong></td>
<td></td>
</tr>
<tr>
<td>17. Implement a Security Awareness &amp; Training Program</td>
<td>19. Incident Response &amp; Management</td>
</tr>
</tbody>
</table>

[https://www.cisecurity.org/controls/](https://www.cisecurity.org/controls/)
Systems Acquisition, Development & Maintenance
For more information about SDLC & Privacy/Security-by-Design

- **Privacy Impact Assessment** – Consultants previously provided an issue-spotting PIA

- **Kill Chain**
  - Describes the phases/stages of a targeted attack (created by Lockheed Martin)
  - Each stage presents an opportunity to detect and react to the attack

- **OWASP Top 10** Most Critical Web Application Security Risks

- **Application Security Guide for CISOs**

- **Cloud Security Alliance’s Cloud Security Controls Matrix**
  - [https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview](https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview)

- **AWS Shared Responsibility Model**
Public Accountability for “Tone at the Top”

CEOs accountable for providing access to Boards

- Sony compromise (destroyed 3000 computers & 800 servers; critical systems out 3 mos)
  - Vice chairman resigned (exposure of “sensitive” emails)

- Target breach
  - CIO fired
  - CEO fired after 25 years with company
  - Board of directors survived proxy fight (lack of oversight/fiduciary duty)

- Yahoo breaches
  - Yahoo lost $350 million in Verizon purchase acquisition with more money reserved for additional losses
  - General Counsel resigned with no severance (poor investigation)
  - CEO personally lost $14 million - annual bonus and equity award
Impacts of lack of Privacy-by-Design

- 20 year FTC Consent Orders for P-b-D violations re: mobile apps (2014)
  - Fandango Movies app assured customers during checkout that credit card data was stored and transmitted securely
  - CreditKarma app disclosed use of “industry-leading security precautions” and privacy policy represented use of SSL encryption
  - Both disabled SSL certificates for testing that were not re-enabled prior to being placed in production
    - Fandango’s app was left vulnerable almost 4 years
  - Apps were vulnerable to man-in-the-middle attacks, especially dangerous on public wi-fi networks
  - Should have been tested for this prior to release and scanned for this vulnerability
  - FTC did not allege actual data breach or identity theft occurred
  - App developers must properly manage design, testing and implementation
Privacy is an asset for **gaining Competitive Edge**

*By building and maintaining *stakeholder trust and loyalty*

- **Privacy Builds and Sustains** **Brand Integrity and Customer Loyalty**

- **Privacy Enables** **Achievement of Business Objectives**
  - **Gain sales** via customer referrals to family, friends and associates (67% rely on this)
  - **Win partner business**
  - **Secure investor confidence**
  - **Secure acquiring company bid**
  - **Protects company value** by mitigating financial, legal, regulatory, operational and reputational risks
    - **Facilitates obtaining cyber risk insurance** (no absolute security)

*Ponemon Institute survey*
# State data breach laws – updated July 2018

50 states plus D.C., Guam, Puerto Rico & Virgin Islands = 54

<table>
<thead>
<tr>
<th># States</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>“Personal Information” definition <strong>is broader</strong> than general definition: # is on the rise</td>
</tr>
<tr>
<td>4</td>
<td>Trigger notification by <strong>access</strong>: CT, NJ, Puerto Rico (NY &amp; CA have no peeking laws)</td>
</tr>
<tr>
<td>43</td>
<td>Require a <strong>risk-of-harm analysis</strong></td>
</tr>
<tr>
<td>37</td>
<td>Require notice to the <strong>attorney general or state agency</strong>: # is on the rise</td>
</tr>
<tr>
<td></td>
<td>Days: AL (45), AK, AZ, CA (15/PHI), CO (30), CT, DE, FL (30), HI, ID, IL (45), IN, IA, LA, ME, MD, MA, MO, MT, NE, NH, NJ, NM (45), NY, NC, ND, OH, OR, Puerto Rico, RI, SC, SD, TX, VT, VA, WA (45), WI</td>
</tr>
<tr>
<td>18</td>
<td>Require notification within a specific timeframe <strong>less than 60 days</strong> (HIPAA)</td>
</tr>
<tr>
<td></td>
<td>Days: 7: ME; 15: CA (clinics, health facilities, home health agencies &amp; hospices); 30: CO, FL; 45: AL, AZ, MD, NM, OH, OR, RI, TN, TX, VT, VA, WA, WI; 60: DE, LA, SD 90: CT</td>
</tr>
<tr>
<td>18</td>
<td>Permit a <strong>private right of action</strong> (courts using HIPAA to define negligence) – includes CA</td>
</tr>
<tr>
<td>54</td>
<td>An <strong>encryption safe harbor</strong> (all)</td>
</tr>
<tr>
<td>8</td>
<td>Triggered by compromise of electronic &amp;/or <strong>paper</strong> records - AK, HI, IN, IA, MA, NC, WA, WI</td>
</tr>
</tbody>
</table>

*Do you have a breach notification policy and breach response resources to comply with this complexity?*

Refer to BakerHostetler or other law firm resource for the latest information:
State law defines PII
California added logon credentials & answers to security questions in 2014

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Persistent identifiers</strong>&lt;br&gt;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 - <em>also cannot override browser privacy settings</em></td>
</tr>
<tr>
<td>2.</td>
<td><strong>Medical / health Information</strong>&lt;br&gt;conditions, treatments, therapies, prescriptions, drugs, medications, dosage, medical products or equipment used; prescribing physician name, address, &amp; contact info; health insurer’s name, insurance account #, or insurance policy #</td>
</tr>
<tr>
<td>3.</td>
<td><strong>Geo-location information</strong>&lt;br&gt;street name/town – does not have to be precise</td>
</tr>
<tr>
<td>4.</td>
<td><strong>Online logon information</strong>&lt;br&gt;user ID/password, <em>answers to common security questions</em>**</td>
</tr>
<tr>
<td>5.</td>
<td><strong>PII used for marketing purposes</strong>&lt;br&gt;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>6.</td>
<td><strong>Security questions</strong>&lt;br&gt;place of birth, mother’s maiden name, etc.</td>
</tr>
<tr>
<td>7.</td>
<td><strong>PCI data</strong>&lt;br&gt;credit/debit/payment card information <em>(PCI-DSS)</em></td>
</tr>
<tr>
<td>8.</td>
<td><strong>Other</strong>&lt;br&gt;biometrics, W-2s, personnel files; video / audio file</td>
</tr>
</tbody>
</table>

EU data privacy laws identify other types of PII
5 ways program can be under scrutiny

*Can lead to loss of business/opportunity and/or enforcement action*

1. **Complaint** to regulatory authority or law enforcement
   - Referred cases from other agencies / direct complaints from customers / whistle-blowers

2. **Breach** – entire program scrutinized, not just cause of breach, by HHS/FTC/state AGs
   - Reported by compromised organization or service provider, customer, FBI, etc.
   - Media firestorm

3. **Business partner due diligence** prior to contracting and periodically thereafter
   - Requests information if no independent audit
   - The higher up the Fortune 500 ladder, the greater the scrutiny

4. **Acquiring company** (M&A) / investor due diligence to mitigate “successor liability”

5. **Cyber risk insurance applications** requiring a due diligence assessment
Calculating breach risk

\[
\text{risk} = \text{probability} \times (\text{threat} \times \text{vulnerability}) \times \text{impact} \times \text{consequence}
\]

Note: even a low probability with a serious impact equals a high risk

<table>
<thead>
<tr>
<th>Probability of Occurrence</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Significant</th>
<th>Damaging</th>
<th>Serious</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligible</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td>Very Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Very High</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Extreme</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
</tbody>
</table>

But the probability of a breach is usually underestimated – *Businesses in last 12 months had: 90% one or more breaches; 59% multiple breaches* (Ponemon Institute)
Breach impacts can be catastrophic


Privacy is more than a compliance risk, it is a component of Trust and reputation risk

Avg. breach cost/compromised record = $225 U.S. / $380 healthcare
(Ponemon Inst.)

- Regulatory risk
- Legal risk

- Financial risk
  - Lost sales and business opportunities
  - 12-22% avg. loss in brand value

- Reputation/brand risk is uninsurable and can be catastrophic

- Operational risk
  - CEOs lost 1-1.5 years of productivity (interviews)

- Officer liability risk
  - Target: CEO & CIO fired; and 2 proxy firms recommended 2 & 7 directors be fired
  - D&O class actions – 10K and IPO cyber security risk claims
  - Also Sony, Yahoo, etc.
Yet, cost to protect is low
You don’t have to be low-hanging fruit!

- Avg. protection cost ($16) is about 10% of avg. global breach costs ($158) per compromised record (Gartner) - less than 7% of U.S. cost & 4.5% of U.S. healthcare cost

- Avg. breach cost reductions per record (Ponemon Institute’s 2016 Cost of Data Breach Study)
  - Governance improvements and DLP technology reduce breach costs
  - $16 for incident response plan & team – 10% off global avg. breach cost of $158
  - $13 for extensive use of encryption – 8%
  - $9 for employee training – 5.7%
  - $9 for participation in threat sharing – 5.7%
  - $9 for business continuity involvement - 5.7%
  - $8 for extensive data leak protection (DLP) – 5%
  - $7 for CPO / CISO appointed – 4.4%

- 97-99% of breaches are avoidable with reasonable controls (simple/intermediate) (Verizon Business Data Breach Investigation Reports)

- Legal defensibility is getting to 97-99% avoid-ability, not “absolute security”, as there is no such thing
5 risk responses

Most responses should be *mitigate* – *document rationale* for any other response

1. **Accept** – Business decides to accept the current level of risk because: a) the mitigation costs outweigh the benefits; or b) the key causes are out of its control (inescapable part of doing business) – *must be defensible*

2. **Avoid** - *Eliminate a process or product* to avoid the risk or condition as the risks outweigh the rewards  
   a. E.g., eliminate installing a faulty slide that could hurt children from the project plan

3. **Transfer/Share** - *Contractually shift* or share the consequences of a risk to a third party or *insure* the risk

4. **Monitor** – *Temporarily delay* selecting another response until more information, usually research, is obtained  
   a. *Timeframe should be agreed upon*, usually no more than 30-60 days, and tracked

5. **Mitigate** – *Strengthen controls* (improve controls effectiveness) to reduce the risk to an acceptable/defendable threshold (reducing likelihood &/or impact)

**Document approving authorities** for all risks & where appropriate rationales
FTC Consent Order client impacts

- **20 year consent order**
  - CEO will likely want another executive to sign the order, e.g. GC, CFO, CRO or CPO/CISO
  - A copy of the order must be delivered to / receipt acknowledged by all current / future: subsidiaries, principals, officers, directors, managers, employees, agents, and representatives having responsibilities relating to the order

- **Increased cost of compliance**
  - Provide 30 days notice of change to corporation, e.g., dissolution, assignment, sale, merger or like action
  - Within 90 days of order, provide a report of compliance to the order
    - Respond within 10 days to additional information requests
  - Expensive independent biennial audits by CISSP, CISA, or GIAC (not a CPA)
    - Demonstrate compliance on any given day during 20 year period
  - Retain specified compliance documentation for a period of 5 years
    - Any documents that “contradict, qualify, or call into question compliance with” the order; risk assessments; consumer complaints; plans, reports, studies, reviews, audits, audit trails, training materials, and assessments; statements disseminated to consumers re: privacy/security
  - Compliance is elevated due to:
    - FTC expectations, e.g. privacy/security training occurs prior to providing new hires access to PII
    - Being on the FTC’s radar screen and wanting to avoid another breach
COSO ERM
20 key principles within five components

<table>
<thead>
<tr>
<th>Governance and Culture</th>
<th>Strategy and Objective Setting</th>
<th>Execution (Performance)</th>
<th>Review and Revision (Monitor what really matters)</th>
<th>Information, Communication, &amp; Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lay strong foundation of risk governance and culture - governance sets tone reinforcing importance of and establishing oversight responsibilities for ERM.</td>
<td>ERM and strategy work together to align objective-setting with risk appetite.</td>
<td>Identify risks that may impact achievement of strategy and business objectives. Assess and prioritize risks. Select risk responses. Report results to key risk stakeholders.</td>
<td>Maximize value of risk information and reports. Review entity performance to consider how well ERM components are functioning over time and in light of substantial changes and what revisions are needed.</td>
<td>ERM requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.</td>
</tr>
</tbody>
</table>

1. Exercises Board Risk Oversight
2. Establishes Governance and Operating Structures
3. Defines Desired Culture (Organizational Behaviors)
4. Demonstrates Commitment to Core Values (Integrity/Ethics)
5. Enforces Accountability
6. Attracts, Develops and Retains Capable Individuals

1. Considers Risk and Business Context
2. Defines Risk Appetite
3. Evaluates Alternative Strategies
4. Considers Risk When Formulating Business Objectives
5. Defines Acceptable Variation in Performance

1. Identifies Risk
2. Assesses and Values Risk
3. Prioritizes Risks
4. Selects and Implements Risk Responses
5. Develops Portfolio View

1. Assesses Substantial Change
2. Reviews Risk and Performance
3. Pursues Improvement in Enterprise Risk Management

1. Leverages Information and Technology
2. Communicates Risk Information
3. Reports on Risk, Culture, and Performance
California passes 1st IoT cybersecurity law

Effective Jan. 1, 2020

- Regulates manufacturers of (likely consumer) devices that can directly or indirectly connect to Internet and are assigned an IP or Bluetooth address, although language is quite broad

- Exemptions include:
  - unaffiliated 3rd-party software/applications that user adds to connected device
  - providers of means of purchasing/downloading software/applications, such as provider of an electronic store or marketplace
  - connected devices already subject to federal law/regulation promulgated by federal agency
  - entities or persons subject to HIPAA or CMIA with respect to activity regulated by those laws

- “Reasonable security” feature, it specifies that any such feature must be:
  - appropriate to nature and function of device
  - appropriate to information the device may collect, contain, or transmit
  - designed to protect device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure

- If regulated connected device is capable of authentication outside a local area network, it will be deemed to be equipped with a “reasonable security feature” if:
  - preprogrammed password is unique to each device
  - user is required to generate a new password before accessing device for the first time
UK’s Code of Practice for Consumer IoT Security

Three quick wins

- **unique passwords**: avoid use of IoT device default passwords (e.g., avoid universal default usernames and passwords, or leaving it up to the consumer to change them)
- **vulnerability disclosure**: all IoT device/services suppliers should implement a vulnerability disclosure policy (e.g., provide a public point of contact so security researchers/others can report issues, which should be acted upon in a timely manner)
- **secure, updated software**: keep software up to date in IoT devices (e.g., regularly issue or install software patches)

<table>
<thead>
<tr>
<th>#</th>
<th>13 Guidelines</th>
<th>Primarily Applies to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Device Manufacturers</td>
</tr>
<tr>
<td>1</td>
<td>No default passwords</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>Implement a vulnerability disclosure policy</td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>Keep software updated</td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td>Securely store credentials &amp; security-sensitive data</td>
<td>X</td>
</tr>
<tr>
<td>5</td>
<td>Communicate securely</td>
<td>X</td>
</tr>
<tr>
<td>6</td>
<td>Minimize exposed attack surfaces</td>
<td>X</td>
</tr>
<tr>
<td>7</td>
<td>Ensure software integrity</td>
<td>X</td>
</tr>
<tr>
<td>8</td>
<td>Ensure personal data is protected</td>
<td>X</td>
</tr>
<tr>
<td>9</td>
<td>Make systems resilient to outages</td>
<td>X</td>
</tr>
<tr>
<td>10</td>
<td>Monitor system telemetry data</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Make it easy for consumers to delete personal data</td>
<td>X</td>
</tr>
<tr>
<td>12</td>
<td>Make installation &amp; maintenance of devices easy</td>
<td>X</td>
</tr>
<tr>
<td>13</td>
<td>Validate input data</td>
<td>X</td>
</tr>
</tbody>
</table>

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 re: 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
## Additional Possible Future Scope of Consulting Services

<table>
<thead>
<tr>
<th></th>
<th>Requested Documents Review</th>
<th>Assure readiness to quickly and fully produce requested documents within 10 days to demonstrate compliance as part of an inquiry, audit, or investigation</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td></td>
<td>Additional Possible Future Scope of Consulting Services</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>-------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| 6. | **Real Time Incident Detection and Response Evaluation**  
   | 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) |
| 7. | **Incident/Event Management Governance**  
   | 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 |
| 8. | **Third Party Management Governance**  
   | 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) |
| 9. | **Privacy, Breach Notification and Security Policies**  
   | 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 |
| 10. | **Monthly Status Report Conference Call**  
    | 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 |
| 11. | **Implementation**  
    | For any recommendation made by Consultant, Company may desire Consultant’s help with implementation |
| 12. | **Retainer**  
    | 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. |
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 is the first step toward 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, CIPP  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